Chief Executive Officer
Louis Ward, MHA

Mayers Memorial Hospital District

Board of Directors
Jeanne Utterback, President
Beatriz Vasquez, PhD, Vice President
Tom Guyn, MD, Secretary
Abe Hathaway, Treasurer
Tami Vestal-Humphry, Director

Finance Committee

Meeting Agenda

August 25th, 2021– 9:30 AM
Mayers Memorial Hospital District
Burney Boardroom
20647 Commerce Way
Burney, CA 96013
Zoom Meeting Information
CLICK HERE TO ENTER
Call In Number: 1-253-215-8782   Meeting ID: 821 2366 4191

In observance of the Americans with Disabilities Act, please notify us at 530-336-5511, ext 1264 at least 48 hours in advance of the meeting so that we may provide the agenda in alternative formats or make disability-related modifications and accommodations. The District will make every attempt to accommodate your request.

Attendees

Abe Hathaway, Chair, Board Member
Tami Vestal-Humphry, Board Member
Louis Ward, CEO
Travis Lakey, CFO

1	**CALL MEETING TO ORDER**				
2	**CALL FOR REQUEST FROM THE AUDIENCE - PUBLIC COMMENTS OR TO SPEAK TO AGENDA ITEMS**				**Approx. Time Allotted**
3	**APPROVAL OF MINUTES**				
3.1	Regular Meeting – July 28th, 2021		***Attachment A***	**Action Item**	2 min.
4	**DEPARTMENT REPORTS:**				
4.2	Lab – Ulysses Pelew		***Attachment B***	Report	2 min.
4.3	Radiology – Alan Northington		***Attachment C***	Report	2 min.
4.4	Cardiac Rehab – Trudi Burns		***Attachment D***	Report	2 min.
5	**FINANCIAL REVIEWS/BUSINESS**				
5.1	July 2021 Financials		***Attachment E***	**Action Item**	5 min.
5.2	Accounts Payable (AP)/Accounts Receivable (AR)			**Action Item**	5 min.
5.3	Managed Security Services (IT) Agreement/Proposal		***Attachment F***	**Action Item**	10 min.
5.4	401 K Annual Report			Report	10 min.
6	**ADMINISTRATIVE REPORT**			Report	5 min.
7	**OTHER INFORMATION/ANNOUNCEMENTS**			Information	

8 **ADJOURNMENT:** Next Regular Meeting –September 22, 2021

Posted 8/20/2021

Public records which relate to any of the matters on this agenda (except Closed Session items), and which have been distributed to the members of the Board, are available for public inspection at the office of the Clerk to the Board of Directors, 43563 Highway 299 East, Fall River Mills CA 96028. This document and other Board of Directors documents are available online at www.mayersmemorial.com.

Chief Executive Officer
Louis Ward, MHA

Mayers Memorial Hospital District

Board of Directors
Finance Committee
Minutes

July 28, 2021 – 9:00 am
MMHD FR Boardroom

These minutes are not intended to be a verbatim transcription of the proceedings and discussions associated with the business of the board's agenda; rather, what follows is a summary of the order of business and general nature of testimony, deliberations and action taken.

1	**CALL MEETING TO ORDER:** Abe Hathaway called the meeting to order at 9:34 am on the above date.			
	BOARD MEMBERS PRESENT:	**STAFF PRESENT:**		
	Abe Hathaway, Committee Chair Tami Vestal-Humphry, Director **ABSENT**:	Louis Ward, CEO Travis Lakey, CFO Ryan Harris, COO Candy Detchon, CNO Susan Garcia, Food & Nutrition Services Manager Jessica DeCoito, Board Clerk		
2	**CALL FOR REQUEST FROM THE AUDIENCE – PUBLIC COMMENTS OR TO SPEAK TO AGENDA ITEMS - None**			
3	**APPROVAL OF MINUTES**			
	3.1	A motion/seconded carried; committee members accepted the minutes of June 23, 2021	***Humphry, Hathaway***	**Approved by All**
4	**DEPARTMENT REPORTS: NONE**			
	4.1	**Dietary:** Revenue from kitchen sales has hit us hard with COVID and not being open to the public. Our menu is limited with the hope to decrease waste but still provide the staff with options for their lunches. We hope to open in the middle of the August to collect your meals in the cafeteria, but still ordering meals online. An update of the menu will also take place. Bringing the salad bar back will be a huge hit because it is our most ordered item pre-COVID. Losses we have incurred from the equipment going down is approximately $1230 each time. In the past two months (June and July) we have had 5 equipment failures. We lose a lot more product in Burney than Fall River because we have more freezers/refrigerators in FR. Our refrigerator and freezer units are old and exposed to the elements which has made their functionality worse.		
5	**FINANCIAL REVIEWS**			
	5.1	**June 2021 Financials:** Assessing the statistics with NPH (Registry staff company) – offering housing but they are not taking it which costs us more in mileage in the end. So we've looked at housing options in both Burney and Fall River. We will continue to discuss the housing thoughts and options when we get into Strategic Planning. Inventory issues have been brought up with Retail Pharmacy. We will be meeting up and walking through the processes to understand what is going on. 340B conversation taking place tomorrow with MVHC. Auditors will be here on August 16th. Cost Report conference in Reno in September that both CFO and CEO will be attending. COO will also be there for the Rural Health Clinic portion. Provider Relief funding available and we are working on gathering more information and will share when it's available.	***Hathaway, Humphry***	**Approved by All**
	5.2	**Accounts Payable (AP) & Accounts Receivable (AR)**: 58.29 AR Days, AP 1,044,461		
6	**ADMINISTRATIVE REPORT –** Will report in Regular Board Meeting.			
7	**OTHER INFORMATION/ANNOUNCEMENTS: None**			
8	**ADJOURNMENT – 10:23 AM**			
	Next Finance Committee Meeting: August 25, 2021 – Burney Boardroom			

Rad Comparison FY 20 to 21	FY 20	FY 21
Revenue		
4500-0100 (Clinical Lab - Semi-Prvt Acute)	$199,619	$253,658.00
4500-0200 (Clinical Lab - Swing Bed)	$65,845.00	$68,156.00
4500-0800 (Clinical Lab - Semi Private SNF)	$1,283.00	$3,649.00
4500-1100 (Clinical Lab - OP/Referral)	$2,872,989	$2,608,277.00
4500-1200 (Clinical Lab - OP/Surgery)	$39,266.00	$28,342.00
4500-1300 (Clinical Lab - OP Services)	$84,130.00	$62,793.00
4500-1500 (Clinical Lab - MOO)	$132,503.00	$124,914.00
4500-1600 (Clinical Lab - OP/ED)	$1,008,393.00	$1,159,354.00
4500-1900 (Clinical Lab - Hospice)	$0	$544
Total Revenue	**$4,404,038**	**$ 4,309,687.00**
Expenses		
7500-0000 (Lab - Mamagement)	$144,926	$90,399.88
7500-0100 (Lab - Tech Spec)	$113,513	$ 198,642.04
7500-0500 (Lab - Clerical/ Ward Clerk)	$150,162.12	$ 150,789.15
7500-0800 (Lab - Medicare)	$7,498.23	$ 7,966.83
7500-0900 (Lab - Callback - STBY)	$70,957.09	$ 79,615.81
7500-1000 (Lab - FICA)	$28,958.37	$ 30,745.47
7500-1200 (Lab - Sick Pay)	$3,271.87	$ 1,196.11
7500-1600 (Lab - WRKM'S COMP INS.)	$16,543.32	$ 17,417.76
7500-1800 (Lab - VAC & HOL PAY)	$53,604.82	$ 48,116.53
7500-2000 (Lab Physician Fee)	$23,400.00	$ 21,600.00
7500-4100 (Lab - Medical Supplies)	$4,908.32	$ 22,561.50
7500-4120 (Lab - Med Sup Covid 19)	$0.00	$ 606.00
7500-4600 (Lab - Office Supplies)	$1,947.53	$ 3,790.02
7500-4800 (Lab - Instrments/Minor Equipment)		$ 12,197.50
7500-4820 (Lab - Instr/Minor Equip C19)		$ 9,055.84
7500-4900 (Lab - Minor Equipment)	$2,073.33	$ 16,454.81
7500-5000 (Lab - Non-Med Supplies)	$313,612.02	$ 428,222.21
7500-5020 (Lab - NonMed Supp C19)	$8,669.00	$ 139,707.00
7500-6200 (Lab - Repairs & Maintence)	$11,969.00	$ 6,455.77
7500-6800 (Lab - Freight)	$11,514.68	$ 10,918.42
7500-6820 (Lab - F/H Covid 19)	$140.29	$ 2,112.42
7500-6900 (Lab - Other Purchase Services)	$146,145.14	$ 654,690.89
7500-6921 (Lab - Other Purchase Services Travel)	$281,601.55	$ 318,782.96
7500-7400 (Lab - Depreciation Expenses)	$14,631.79	$ 40,512.75
7500-7600 (Lab - Rent/Lease Equipment)	$422.58	$ 4,651.70
7500-8100 (Lab - Liability Insurance)	$18,487.68	$ 19,666.68
7500-8300 (Lab - Licenses & Taxes)	$34,963.62	$ 38,068.87
7500-8320 (Lab - Tax Covid 19)	$587.25	$ 10,661.55
7650-8700 (Lab- Outside Training)	$77.00	$ -
7500-8800 (Lab - Travel)	$0.00	$ 3,644.10
7500-8801 (Lab - Milage)	$1,491.88	$ 631.40
Total Expenses	**$1,466,078.02**	**$ 2,394,881.97**
Net Income	**$2,937,959.58**	**$ 1,914,805.03**

Mayers Memorial Hospital District Financial Report FY 2021

Matthews Imaging Department

Conclusion

Over the past year, expenses were in line with exam volumes and operations. There was a 4% decrease in Ultrasound volume, CT volume increased by 12.8% and general diagnostic X-Ray gained 5.56% in volume year over year.

Staffing

Staffing continues to be a challenge with the use of travelers and increases costs. We have been unsuccessful in our efforts to retain permanent technologists.

Computed Tomography CT

CT volumes increased over last year’s level by 121 exams to a total of 944, which remains under the numbers Mayers should be completing based on area demographics. CT exams continue to travel outside our service area to competing facilities.

Referral patterns play a significant role in where outpatient CTs are done. However, out of pocket costs will be a more dominant determining factor.

Ultrasound

Ultrasound exam numbers decreased by 30 exams to 739 from 769 exams representing a 4.06% decrease year over year.

General Diagnostic X-ray

Genral X-ray exam numbers increased by 5.56 percent to 3,328 exams, year over year. These numbers are manageable and consistent with current demographic trends and allow opportunities and capacity for higher revenue modalities such as CT

Respectfully Submitted By: Alan Northington, MHA/MBA, R.T., Imaging Manager

Rad Comparison FY 20 to 21	FY 20	FY 21
Revenue		
4560-0100 (Radiology - Semi-Prvt Acute)	$32,097	$38,871.00
4560-0200 (Radiology - Swing Bed)	$5,808.00	$8,429.00
4560-1100 (Radiology - OP/Referral)	$490,677	$571,828.00
4560-1200 (Radiology - OP/Surgery)	$2,234.00	$6,826.00
4560-1300 (Radiology - OP Services)	$747.00	$0.00
4560-1500 (Radiology - MOO)	$23,033.00	$17,106.00
4560-1600 (Radiology - OP/ED)	$392,900	$430,715
4560-0100 (CT/MRI - Semi-Prvt Acute)	$113,803	$181,231.00
4560-0200 (CT/MRI - Swing Bed)	$14,702	$19,171.00
4560-1100 (CT/MRI - OP/Referral)	$684,274	$841,305.00
4560-1300 (CT/MRI - OP Services)	$0	$6,038.00
4560-1500 (CT/MRI - MOO)	$149,588	$150,958.00
4560-1600 (CT/MRI - OP/ED)	$1,205,330	$ 1,371,385.00
4670-0100 (Ultrasound - Semi-Prvt Acute)	$20,247	$ 18,084.00
4670-0200 (Ultrasound - Swing Bed)	$4,579	$ 5,665.00
4670-1100 (Ultrasound - OP/Referral)	$604,176	$ 588,755.00
4670-1200 (Ultrasound - OP/Surgery	$0	$ 179.00
4670-1300 (Ultrasound - OP Services)	$3,808	$ 2,906.00
4670-1500 (Ultrasound - MOO)	$12,757	$ 11,721.00
4670-1600 (Ultrasound - OP/ED	$84,838	$ 90,103.00
Total Revenue	**$3,845,598**	**$ 4,361,296.00**
Expenses		
7630-0000 (Radiology - Mamagement)	$123,235	$122,524.24
7630-0100 (Radiology - Tech Spec)	$134,634	$ 178,012.81
7630-0500 (Radiology - Clerical/ Ward Clerk)	$61,743.85	$ 66,176.55
7630-0800 (Radiology - Medicare)	$6,961.61	$ 7,334.37
7630-0900 (Radiology - Callback - STBY)	$145,577.59	$ 125,755.73
7630-1000 (Raidology - FICA)	$26,252.60	$ 25,649.91
7630-1200 (Raidology - Sick Pay)	$1,971.62	$ 2,024.56
7630-1600 (Raidology - WRKM'S COMP INS.)	$10,942.08	$ 16,851.96
7630-1800 (Raidology - VAC & HOL PAY)	$29,055.83	$ 33,254.69
7630-1802(Radiology - COVID Sick Pay)	$0.00	$ 1,372.80
7630-4100 (Raidology - Medical Supplies)	$16,612.14	$ 28,068.33
7630-4500 (Raidology - Cleaning Supplies)	$206.56	$ 207.91
7630-4600 (Raidology - Office Supplies)	$476.43	$ 2,440.09
7630-4900 (Raidology - Minor Equipment)	$3,903.87	$ 5,756.60
7630-5000 (Raidology - Non-Med Supplies)	$4,613.84	$ 4,150.97
7630-6200 (Raidology - Repairs & Maintence)	$56,199.84	$ 54,645.01
7630-6800 (Raidology - Freight)	$472.72	$ 1,202.86
7630-6900 (Raidology - Other Purchase Services)	$39,193.58	$ 48,237.60
7630-6921 (Raidology - Other Purchase Services Travel)	$274,097.25	$ 254,165.00
7630-7400 (Raidology - Depreciation Expenses)	$125,224.68	$ 232,475.48
7630-7600 (Raidology - Rent/Lease Equipment)	$3,760.45	$ 5,854.41
7630-8100 (Raidology - Liability Insurance)	$9,265.56	$ 9,690.00

7630-8300 (Raidology - Licenses & Taxes)	$13,897.26	$ 2,536.71
7650-8700 (CT/MRI - Other Purchase Services)	$7,500.00	$ 3,243.66
7630-8800 (Raidology - Travel)	$2,275.12	$ 82.14
7630-8801 (Radiology - Milage)	$0.00	$ -
Total Expenses	$1,098,044.32	$ 1,231,714.39
Net Income	$2,747,553.68	$ 3,129,581.61

CARDIAC REHAB FINANCIAL REPORT 2021

This year has been a very stressful year for almost everyone throughout the world. We absolutely know that stress is very hard on the body and especially contributes to heart issues. This fact alone makes Cardiac Rehab even more vital for the people in our community. It is a safe place to regain health after a heart event. We want to meet the needs of the people in our community (Big Valley, Burney and Fall River) without increasing their stress load by driving to Redding. We also strive to provide a place to maintain strength by exercise, enjoy socializing with others (with similar problems), and decrease stress. Cardiac Rehab is a terrific place to decrease blood pressure, tone muscles and help to change those genetic predispositions for heart disease.

SERVICE PROVIDED: We provide each patient with an outlined exercise plan that is specific for that patient's current needs. For example: a recent, post-op, open heart, surgical patient cannot exercise their arms for 8 weeks after surgery (to keep added stress off of the incision). Then they must slowly introduce arm exercises to regain upper body strength. (That's where we come in) A patient that has back issues (along with heart concerns) will need to have extra back support as they exercise. As people age they sometimes have multiple ailments to consider as their exercise regimen is outlined. There is a RN here 3 days a week to assist with medication questions, dietary concerns, and to encourage visits to the physician if needed. We also have a CR Assistant here on Tuesdays. She is proficient in exercise techniques, safe weight machine use and dietary concerns. I am in the process of figuring out some ways to utilize her talents even more than we do now.

PATIENT VISITS FOR THE FISCAL YEAR: There were 2,192 patient visits. 145 of those were monitored patients. We also placed 26 Holter monitors. (A Holter is a Cardiac monitors that a patient wears at home for 24-48 hours.) We were blessed to receive grant money for 3 new Holters to assist with our community's growing needs. EKGs were at 604 this year which is in keeping with our average.

Compared to last year we decreased Monitored patients -46, increased maintenance patients +15, and increased our Holter monitors +5.

- Maintenance patients are charged $35.00/month. This price has been maintained for many years which is a great community benefit.
- Monitored patients are charged $235.00/Visit! They come in 2-3 days a week for 36 total visits. (No increase in cost this year.)
- Holter patients are charged $429.00 each. (No increase in cost this year.)
- EKG patients are charged $246.00 each. (An increase of $14.00 this year.)

Of course we know that not all charges are recovered 100% through the insurance. Maintenance patients pay their fee out of pocket so the recovery rate is 100%. Monitored patients, Holters, and EKGs recover an average of $.60 on the dollar. It depends on the insurance. The only way that Cardiac Rehab survives is because of the EKG revenue. That brings revenue/expenses to an even ground.

NUMBERS: Currently we have 4 monitored patients (one just started, two are midway, and the fourth will be starting as soon her blood pressure is under control. We are working with the doctor and medication now.) We also had one monitored patient graduate (a couple weeks ago) into the maintenance program.   Right now our numbers are low primarily due to COVID. We have been open this entire year but have definitely felt the loss of some of our patients. Some stay home due to concern about being around others. We take extra precautions with disinfecting the equipment after each use, hand washing, social distancing, and mask wearing to enter and leave the gym.   While exercising the patients are not required to wear their mask over their nose and mouth due to the increased respiratory effort needed. These patients are all here with a cardiac or respiratory deficiency and need more airflow. We have fans moving the air, fresh air coming in and encourage water consumption. If ANY of the patients are sick they are told not to come in at all.   These restrictions have enabled us to keep our doors open as safely as possible.

Extra Monies were received from Mayers Healthcare Foundation to purchase three Holter monitors. This totaled $3,300.00 and was desperately needed.

I am exploring ways to reach out to our community to meet their cardiac needs. I have made posters for our new clinic and made current flyers about Cardiac Rehab so our new physicians, PAs and NPs know what we have to offer. There are a few other ideas that I'm working on that will unfold as the year progresses that will help our Intermountain Area and bring revenue into Cardiac Rehab.

Cardiac Rehab operates in the negative.   It is a vital community service but doesn't make money.   With the revenue from the EKGs we are able to either break even or stay in the positive. This allows us to continue to serve our community more efficiently.

Please feel free to come in and see our gym anytime.

CYGILANT RESPONSE TO RFP

Mayers Memorial Hospital District

Managed Security Services/Security Operations Center (SOC) Provider
Technical Proposal

Submitted by:

Cygilant
2400 District Avenue
Burlington, MA 01803
POC: Cooper Mooney
cmooney@cygilant.com
617.337.4839

Submitted August 6th, 2021

Table of Contents

1. Introductory Letter

Subject: Mayers Memorial Hospital District Request for Proposal (RFP) 2021

Dear Ryan,

Cygilant is very pleased and excited to submit our response to the Mayers Memorial Hospital District Managed Security Services Provider/SOC RFP.

Cybersecurity is hard work. Resource constraints – not enough time or limited resources – and ever-increasing threats coupled with compliance requirements are leaving many businesses at a disadvantage and causing stress. Cygilant exists to help you. We partner to extend your team with cybersecurity-as-a-service that overcomes resource constraints, reduces threats and helps achieves compliance. Our main goal is to help you reduce the stress of cybersecurity.

We are excited to work with Mayers Memorial Hospital District who has taken a major initiative to complete, not only 24x7x365 network coverage and visibility, but map towards and improve their security objectives. With this initiative, a partnership with Cygilant can transform the Hospital District from a potential victim to a proactive, cyber stronghold. With Cygilant, we demand excellence, and we will protect Mayers Memorial Hospital District 24x7x365 to ensure you can rest easy knowing you are secure. We are more than a cybersecurity vendor – we are a partnership, and we look forward to working with the District in the near future.

If you need any additional information, please reach out to me at cmooney@cygilant.com.

All the best,

Cooper Mooney

Senior Account Executive – West Coast at Cygilant

(203) 695-4918 – Cell

https://www.linkedin.com/in/cooper-mooney-bb151a107/

2. Cygilant Cost Proposal – Mayers Memorial Hospital District RFP

	1 Yr Agreement
Cygilant 24x7 SOCVue Security-as-a-Service	**Cost Per/Year**
SOCVue Security Monitoring Service – AlienVault USM Anywhere 1.5 TB/Month, 15 Days Hot Storage and Cold Archival Storage	$76,800
SOCVue Endpoint Management Service – SentinelOne Control 370 Endpoints (135 Servers & 235 Workstations)	$26,418
SOCVue Qualys Vulnerability Management Service – Qualys Vulnerability Scanner and 500 IPs (external and internal)	$18,690
Cygilant 24x7 SOCVue Security-as-a-Service	**$119,652.60**

This price is the 1-year annual agreement for Cygilant's 24x7 SOCVue Security-as-a-Service covering Tasks: 1.1 24x7 SOCVue Security & Threat Monitoring, 1.2 Endpoint Management (Detection + Response), and 1.3 Unlimited Vulnerability Management. This price also includes everything discussed in the attached RFP, with no additional costs involved.

Cygilant 24x7 SOCVue Security & Threat Monitoring – This is covered by Cygilant's SOCVue Security Monitoring service as described in the RFP and Cygilant's Service Level Agreements (SLA), included in the price above. The pricing includes a subscription license to AlienVault USM Anywhere SIEM, which includes 1.5 TB/Month of data consumption, 15 Days Hot Storage of Log Data, Cold Archival Storage of Log Data for the entire duration of the agreement. The installation, configuration, and management of the AlienVault USM Anywhere SIEM is done by Cygilant's SOC team and the Cybersecurity Advisor, included in the price of the service. The 1.5 TB/Month of data consumption includes every device listed in the Hospital District's RFP. This is included in Cygilant's cost proposal above.

Cygilant Endpoint Management (Detection + Response) – This is covered by Cygilant's Endpoint Management service as described in the RFP and Cygilant's Service Level Agreements (SLA), included in the price above. The pricing includes a subscription license to SentinelOne Control, which includes x endpoint, for the Hospital District's x servers and x workstations. The installation, configuration, and management of the SentinelOne software is done by Cygilant's SOC team and the Cybersecurity Advisor, included in the price above.

Cygilant Unlimited Vulnerability Management – This is covered by Cygilant's Endpoint Management service as described in the RFP and Cygilant's Service Level Agreements (SLA), included in the price above. The pricing includes a subscription license to Qualys' vulnerability scanner, which includes x IPs (both external and internal) for unlimited scanning. The installation, configuration and management of the Qualys Vulnerability Scanner is done by Cygilant's Cybersecurity Advisor, included in the price above.

Cygilant offers a discounted bundle percentage of 5% for its services, which is included in the proposed cost proposal.

Cygilant offers three-year contract agreements that are additional cost-savings to the Hospital District.

3. Estimated Implementation Timeline

The following contains our anticipated project schedule for Mayer Memorial Hospital services:

Activity	**Anticipated Timeline in Calendar Days**
Complete onboarding	6-8 weeks
Establish change control procedures	
Deploy all required tools and appliances	10-15 days
Train staff in use of all services	No formal training provided
Integrate with and ingest content from existing tools	10-15 days
Required project meetings	Monthly meetings with the Hospital's Cybersecurity Advisor

Activity	**Anticipated Timeline**
Define success criteria for solution and deployment	Within three Days of Signing Agreement
Build your tailored installation and deployment plan	First week of Service
Install sensor	Partners schedule
Import Nodes or IPs	Five days after install
Performance baselining	Within the first four to six weeks of Service
SOCVue Walkthrough (Review Incidents, Scan Results, Patches and Reporting)	Within the first month of Service
Alert and report customization	Within the second month of Service
Monthly meeting and review with Dedicated Cybersecurity Advisor	Every month of service

The Cygilant onboarding process is described in more detail below and will be performed in three stages:

1. Service Orientation Call

Your Cygilant Account Executive Cooper Mooney will contact you to schedule a Service Orientation Call with your Cygilant Cybersecurity Advisor. The goals of the call will be:

- Introduce the Hospital to the SOCVue Security Monitoring service People, Processes, and Technology
- Identify points of contact
- Define requirements for toolset deployment
- Identify devices on which to monitor

- Provide connectivity requirements for toolset communication

2. Installation Call

After your Service Orientation Call has been performed, you will be contacted to schedule the installation of security monitoring solution. The goals of the installation call will be:

- Install the AlienVault USM Anywhere SIEM solution SentinelOne, and Qualys tool (will need multiple calls, if necessary)
- Test and validate toolset connectivity
- Perform a discovery scan to detect nodes on the network (Qualys)
- Integrate nodes to be monitored (AlienVault)
- Transition to service deployment

3. Service Deployment

Further deployment actions will be performed by your Cybersecurity Advisor and the Cygilant Security Operations Center. The subsequent steps will include:

- Review the status of the onboarding project plan
- Validate contacts to receive notifications
- Set up access to the SOCVue platform
- Discuss reporting needs
- Conduct internal operation readiness review
- Commence with security monitoring deliverables as outlined in Section 4: Service Features

4. Accurately Completed Questionnaire (Attachment A)

4.a Company

1. **How long has your company been in business?**

   Cygilant has been in business for 20 years, previously as EiQ Networks, Inc. (2001-2017). Cygilant specializes in 24x7 SIEM and threat monitoring and created one of the first Top 5 SIEM technologies, its legacy solution SecureVue, which is still used in the Department of Defense and U.S. Government. Led by a seasoned team of cybersecurity executives and technologists, Cygilant has over 20 years of cybersecurity experience and over 7 years managing a Global Security Operations Center. Cygilant combines security expertise with its best of breed SIEM technology and cybersecurity dashboard, the SOCVue Platform.

2. **How many Security Operation Centers do you maintain? Where are they located?**

   Cygilant operates a 24x7 global Security Operation Center (SOC) located in Belfast, Northern Ireland.

3. **How many total employees do you have?**

   Cygilant currently has 65 employees and is actively hiring.

4. **How many of these employees are part of your SOC(s)?**

   Cygilant has over 35 security professionals in SOC & Security Services, backed up by about 20 engineers in Development, Product Support, DevOps, and Infrastructure Support roles. Over two-thirds of Cygilant staff are exclusively engaged in delivering managed security & SOC services.

5. **How long have you offered MSSP/SOC services to your clients?**

   Cygilant has offered MSSP services since 2001 (formerly EiQ Networks). Cygilant has offered SOC services since 2014.

6. **Are clients homed out of a specific monitoring center or is activity shared across all your centers?**

   There is one centralized 24x7x365 SOC, located in Belfast, Northern Ireland, that monitors the Hospital’s complete environment. Cygilant’s SOC processes allow for scalable, repeatable, and effective operations. Cygilant’s SOC Director, Dr. Ben Harrison, has created a complex, comprehensive alerting system that analyzes numerous factors to determine alert severity. Cygilant achieves this through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. Through these processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. Cygilant also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. Furthermore, every workflow follows these rules and is documented and recorded for compliance purposes.

Furthermore, as part of the SOC monitoring activity, you will be assigned a Cybersecurity Advisor. The Cybersecurity Advisor is a one-on-one point of contact that is assigned directly to the Hospital's IT team, to utilize as a true cybersecurity resource. The goal of this Advisor is to understand Mayer Memorial Hospital's security objectives and work to meet them. To do so, the Cygilant Cybersecurity Advisor will schedule monthly one-on-one review sessions to review open tickets and incidents, analyze alert trends, configure and maintain the SIEM technology, discuss needed improvements for SOC monitoring, define and finetune reporting needs and future deployment plans, and schedule follow-up calls as needed. During these meetings, the Cybersecurity Advisor can answer any questions the Hospital may have about how to improve and mature their cybersecurity posture.

7. Approximately how many clients do you have fully implemented in your MSSP/SOC offering?

Cygilant has over 150 partners fully implemented in our MSSP/SOC offering.

8. How many of these clients are in healthcare?

~25 percent of Cygilant clients are in healthcare.

9. Are you willing to demonstrate your services in a proof of concept implementation?

Yes, Cygilant encourages a complimentary proof of concept for Mayer Memorial Hospital District.

10. What is your client retention rate?

Cygilant's client retention rate is over 90%, with most customers purchasing additional services over the duration of the partnership.

11. Please describe what you feel differentiates your offering from your competitors.

Cygilant's Security Monitoring service exists to help Mayer Memorial Hospital proactively identify, respond to, and remediate security threats in their environment. With over 15 years of cybersecurity experience and over 7 years in managing a Global Security Operations Center (SOC), our cybersecurity experts guarantee that if the Hospital chooses Cygilant, they will build, mature, and grow their proactive cybersecurity program. Cygilant has achieved this for our clients in the past by combining our people, process, and technology.

Trust in your Security-as-a-Service (SaaS) provider and their personnel is paramount. In May 2020, Cygilant opened a new Global SOC in Belfast, Northern Ireland, a known cybersecurity hub. Cygilant's SOC operates four tiers of human support on a 24x7 basis. Cygilant tapped into Belfast's cyber skill pool to staff its SOC with team members holding master's and Doctor of Philosophy (PhD) degrees in cybersecurity and who come from SOC, Network Operating Center (NOC), software engineering, and information technology (IT) backgrounds. Cygilant's SOC team members hold certifications such as CompTIA Security Plus, CEH (Certified Ethical Hacker), Global Information Assurance Certification (GIAC), Cisco, and SANS. The Hospital will have direct access to these experts via phone/email and who will work one-on-one with them as an extension of their team and aid with any threats.

A tried and proven process is also a major component in selecting a SaaS partner. Cygilant's SOC processes allow for scalable, repeatable, and effective operations. Cygilant's SOC Director, Dr. Ben Harrison, has created a complex, comprehensive alerting system that analyzes numerous factors to determine alert severity. Cygilant achieves this through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. Through these processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. Cygilant also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. We want to give you the best actionable alerting in the industry – and we will do so. Furthermore, every workflow follows these rules and is documented and recorded for compliance purposes.

To further this point, being fully secure on a 24x7 basis goes further than just managing your endpoints. A SOC needs visibility into a variety of data sources, not just endpoint events. A well-rounded security monitoring program includes network traffic analysis, security device events (firewall, gateway, etc.), endpoint data, and cloud sources like Office 365 login activity. By combining all this data with a modern SIEM, Cygilant has more information not only for threat detection, but also for tracing the threat across your environment after a suspicious incident occurs. Therefore, we have implemented proven processes that are both entirely customizable to your security needs and customer-centric so that the Hospital can know they are secure and get the most out of your cybersecurity program with Cygilant being your Security-as-a-Service partner.

A third component of choosing a SaaS provider is technology. Cygilant will help Mayer Memorial navigate the messy cybersecurity market by partnering with and providing best-of-breed technologies like AT&T Cybersecurity, SentinelOne, Qualys, etc. All our technologies are Gartner certified and Fortune 500 tried and proven technology, as compared to the other options in the market. In addition to the partnerships we have created, Cygilant has also created and developed its own proprietary technology, our SOCVue Platform. SOCVue simplifies and consolidates multiple streams of security data to help detect and respond to threats faster and effortlessly collaborate. Also, the Hospital will have a centralized platform to see all of the real-time SOC incident response and compliance activities to provide full network visibility. The goal of SOCVue is to make your environment easier to manage, eliminating the need to engage multiple vendors or technologies. Cygilant will manage all that best-of-breed technology for the Hospital and ease deployment, management, and response through our innovative SOCVue platform.

Cygilant is the most affordable boutique Cybersecurity-as-a-service for all-sized organizations and is a true partner in cybersecurity. We want to see you and your team succeed and grow your cybersecurity program as much as you do. That is why we combine our security experts with best of breed technology and a cybersecurity dashboard in a repeatable process-driven service. We want to give you access to everyone at Cygilant, from the Director of our SOC Operations to our CEO – because we value your security objectives and want to ensure we help you achieve them. In partnering with us, not only will you get a boutique, enterprise-level Security-as-a-Service, but you will get the best customer security value in the industry because we put Customer Security Value at the center of our services, where it belongs.

12. Do you have a dedicated internal threat team? How will you notify MMHD of an internal threat to your environment?

Yes, Cygilant has an internal threat team that is constantly evaluating and researching known or unexpected threats.

Dependent on the severity of the threat, a Cygilant SOC member will either call your phone directly or ensure we notify you of and remediate the threat. If the threat is less critical, your Cybersecurity Advisor will reach out to you via email with information and a Threat Advisory that details the severity of the threat, its impact on business', actionable remediation guidance, etc.

13. Please provide any industry certifications your MSSP/SOC hold, such as SOC, ISO, etc.

Cygilant's SOC team members hold certifications such as CompTIA Security Plus, CEH (Certified Ethical Hacker), Global Information Assurance Certification (GIAC), Cisco, and SANS.

Cygilant holds SOC2 and PCI certification. We are actively working on translating our compliance from SOC2 into parallel ISO 27001 certification.

4.b Compliance

14. Is your solution able to assist us in identifying systems that store, transmit(send/receive), and access ePHI?

Cygilant will use the Qualys network scanner to discover systems on your network. You Cygilant Cybersecurity Advisor will work with you to identify which of these systems process ePHI and can create a separate asset inventory group for tracking these systems.

15. How do you anticipate assisting us in protecting and monitoring access to PHI?

Cygilant will deploy Qualys vulnerability scanning to detect weaknesses in ePHI systems that could be exploited by attackers. Cygilant will also deploy SentinelOne agents on your servers, workstations, and laptops to detect and block malware. The SentinelOne agent will also use advanced machine learning to detect anomalous behavior on the endpoint that might indicate that someone is trying to gain unauthorized access. Lastly, Cygilant will deploy the AlienVault USM Anywhere solution to collect audit logs and alerts from your network infrastructure. These logs will be monitored by the Cygilant SOC around the clock to identify potential security incidents, which could include outside attacks or misuse by insiders.

16. **How do you intend to secure logs or other telemetry data containing PHI? How long will they be stored?**

    Logs and other data collected by Cygilant is encrypted in transit to our systems and encrypted at rest in the products that process and store the information. Logs collected by Cygilant typically contain data like IP addresses, usernames, domains, and file hashes, and do not typically contain any health records. Logs will be stored in "cold storage" in the AlienVault solution for the duration of the contract unless you request it to be purged sooner.

17. **Are you willing to engage in a BAA? Please send a copy.**

    Yes, we have engaged in a BAA with other clients and would be willing to do so. If the District would like us to sign a BAA, please send it over for our review and consideration.

18. **Do you use sub-processors to support your environment? If yes, how do you ensure the sub-processors operate securely and effectively?**

    Cygilant uses several sub-processors including Amazon Web Services, Zendesk, and the products named above. Cygilant sub-processors are SOC 2 compliant and regularly recertified by third-party auditors. Cygilant reviews sub-processor security controls to ensure Cygilant customer data is being protected by the highest industry standards.

19. **Have you suffered a breach, either from an internal or external actor, in any of the preceding 60 months? Please describe and indicate what was learned from this event?**

Cygilant experienced a cybersecurity event in August 2020. The Cygilant Security Operations Center (SOC) discovered a security threat and immediately reported it for investigation. Cygilant was decommissioning a system housing legacy software when an unknown actor gained access to the environment. The system since has been decommissioned. Cygilant engaged a third-party forensic investigation firm to assist in further understanding the nature and scope of the event. Cygilant also conducted a full review of its cybersecurity policies, procedures, processes, and security measures to ensure that they remain appropriate. Cygilant segregates customer transactional data from other company data housed within its environment. This security measure prevented customer transactional data from being impacted by the event. Cygilant hopes this summary addresses any questions you might have about the now-resolved event. Cygilant remains a trusted advisor and partner in delivering premium and uncompromised Cyber Security as a Service. However, should you have additional questions, please do not hesitate to contact Christina Lattuca at CLattuca@cygilant.com or (617) 337-4802.

20. **Has a customer ever been breached due another customer's breach?**

    No.

4.c Technology

21. Describe your implementation and tuning process for a new customer. How long does this usually take?

The following contains our anticipated project schedule for Mayer Memorial Hospital services:

Activity	**Anticipated Timeline in Calendar Days**
Complete onboarding	6-8 weeks
Establish change control procedures	
Deploy all required tools and appliances	10-15 days
Train staff in use of all services	No formal training provided
Integrate with and ingest content from existing tools	10-15 days
Required project meetings	Monthly meetings with the Hospital’s Cybersecurity Advisor

Activity	**Anticipated Timeline**
Define success criteria for solution and deployment	Within three Days of Signing Agreement
Build your tailored installation and deployment plan	First week of Service
Install sensor	Partners schedule
Import Nodes or IPs	Five days after install
Performance baselining	Within the first four to six weeks of Service
SOCVue Walkthrough (Review Incidents, Scan Results, Patches and Reporting)	Within the first month of Service
Alert and report customization	Within the second month of Service
Monthly meeting and review with Dedicated Cybersecurity Advisor	Every month of service

The Cygilant onboarding process is described in more detail below and will be performed in three stages:

5. Service Orientation Call

Your Cygilant Account Executive Cooper Mooney will contact you to schedule a Service Orientation Call with your Cygilant Cybersecurity Advisor. The goals of the call will be:

- Introduce the Hospital to the SOCVue Security Monitoring service People, Processes, and Technology
- Identify points of contact

- Define requirements for toolset deployment
- Identify devices on which to monitor
- Provide connectivity requirements for toolset communication

6. Installation Call

After your Service Orientation Call has been performed, you will be contacted to schedule the installation of security monitoring solution. The goals of the installation call will be:

- Install the AlienVault USM Anywhere SIEM solution and SentinelOne tool
- Test and validate toolset connectivity
- Integrate nodes to be monitored
- Transition to service deployment

7. Service Deployment and Security Monitoring

Further deployment actions will be performed by your Cybersecurity Advisor and the Cygilant Security Operations Center. The subsequent steps will include:

- Review the status of the onboarding project plan
- Validate contacts to receive notifications
- Set up access to the SOCVue platform
- Discuss reporting needs
- Conduct internal operation readiness review
- Commence with security monitoring deliverables as outlined in Section 4: Service Features

During the on-boarding process, Cygilant will work with the Mayer Memorial Hospital IT team to customize the alerts to meet the Hospital needs. Cygilant will work to define what the Hospital considers an Urgent, High, Medium, and Low alert. Each company defines “alerts” differently, so during the onboarding process your dedicated Cybersecurity Advisor will document how you define each severity of alerts. This documentation will act as knowledge base (KB) articles for the account – allowing your dedicated Cybersecurity Advisor and SOC to cross reference and use a baseline. This allows Cygilant to provide the Hospital their desired level of service. This personalization to the alerts and account are included in our services and the Hospital will not be charged extra for this customization.

After the on-boarding process, the Hospital will work directly with both the Cybersecurity Advisor and the SOC to continuously finetune and configure alert rulesets, their playbook, the AlienVault USM Anywhere SIEM technology, etc. – as mentioned above. During these normal operations, if SOC analysis of alerts determines a need for tuning is present or suspected, a ticket will be created to modify customer security content. This is a process of continual improvement in line with the lifecycle of security content management. This continual finetuning allows Cygilant to provide the Hospital District their desired level of service for the entirety of the partnership.

22. Describe the overall level of effort and engagement of our internal team to assist in the POC and implementation of your MDR Services. Please include descriptions of all software and hardware installations as well as configuration that the MMHD team will need to assist with.

Cygilant and the Hospital will maintain a constant ongoing relationship throughout the entire duration of the service agreement, whether through the SOC, Cybersecurity Advisor, Account Manager, or Executive Sponsor. Implementation is handled directly by the SOC and your Cybersecurity Advisor, which is included as part of the service cost. During implementation, the Hospital will join scheduled calls and answer outreach (via phone/email) from the Cybersecurity Advisor or SOC to assist with questions/troubleshooting needed to complete the implementation for the Hospital (i.e. credentials, access to servers for installation, etc.).

With the help of both Cygilant and AlienVault USM Anywhere, the Hospital will configure and set up a server via VMWare for the AlienVault installation. The server requirements for configuring the VMware server are provided by Cygilant prior to our installation call. The requirements provide a step-by-step process including network bandwidth, necessary open ports (only for installation), etc. (https://cybersecurity.att.com/documentation/usm-anywhere/deployment-guide/aws/about-usm-aws-sensor-deployment.htm) See link for server requirements. Once that server is configured, the rest of the implementation is done by Cygilant. After implementation, the responsibilities/resources for both Cygilant and the Hospital can be found below.

The Hospital's Responsibilities Include:

- Customer shall cooperate with and assist the SOCVue Services Team in the performance of the services, and will provide the following resources necessary for the SOCVue Services Team's performance hereunder as specified.
- Customer is responsible for maintaining port/protocols required for communication between managed nodes and the security monitoring components (on-premises or cloud-based).
- If remote VPN access is required, Customer shall grant and provide the SOCVue Services Team with secure remote VPN access to the system running the security monitoring platform at all times during the term including all required access credentials (e.g. IP Address, URL, login account, password, etc.).
- Customer shall provide a list of authorized contact information (including name, phone, email, etc.) for both business hours and after hours.
- Customer shall appoint a contact designated to work with the SOCVue Services Team for all aspects, including escalations, related to the service(s) that will have authority to act on behalf of Customer.
- Customer will promptly communicate to the SOCVue Services Team any questions or concerns relating to the proper delivery of the services provided.
- Customer is responsible for remediation of any incidents about which they are notified.
- Customer will be responsible for providing the SOCVue Services Team with a complete listing of devices, servers, and applications to be monitored.
- Customer is responsible for procuring the necessary data quota to cover the monthly event volumes transmitted to AlienVault USM. In the event of an overage, Customer is responsible for taking action to reduce data volume or procure additional data in a timely manner.
- Customer is responsible for the cost of storing data beyond the standard 12-month retention period that comes with the purchased subscription level.
- Customer will be responsible for configuring the devices, servers and applications that will be monitored per the SOCVue Services Team instructions.

- Customer must provide and maintain a suitable system, meeting minimum system specifications, in a networked environment, with properly installed and patched Operating System (OS) software for operating any security monitoring components installed in the customer's environment.
- Customer must provide the appropriate prerequisite hardware and software necessary for the security monitoring components to be installed and operate properly.
- For on-premises components, Customer is responsible for backups and restore of the solution and all data needed.

Cygilant Responsibilities Include:

- Cygilant will ensure that Cygilant analysts and engineers assigned to the service are knowledgeable about the Cygilant and AlienVault toolsets.
- Cygilant will deliver the service as detailed in Section 4: Service Features.
- Cygilant analysts are responsible for meeting the SLAs in Section 7: Target Service Levels
- Cygilant is responsible for notifying Customer about data overages in a timely manner and giving Customer the option to purchase additional data.
- Cygilant shall retain the collected event log data for 12 months. (Additional storage is available for a fee.)
- Upon termination of cloud-based deployments, Cygilant will retain customer event log data in cold storage for up to 30 days. (Data storage charges apply.)
- Cygilant shall transfer data from cloud storage to the customer upon written request. (Data transfer charges apply.)

23. What points of ongoing technical integration do you expect we will need to perform?

To ensure ongoing technical integration, the Hospital will simply need to enable each device (i.e firewall, domain controller, server, cloud infrastructure, etc.) for monitoring. The AlienVault USM Anywhere SIEM can interface with most existing IT/security products through log delivery and are collected through various mechanisms. Collection mechanisms are primarily syslog and NxLog. If logs can be delivered (usually through syslog) into the SIEM, the expectation is that they will be available to be analyzed for potential security threats. Where the SIEM identifies a potentially security incident based on these logs, they will be presented to the Cygilant SOC within the SOCVue platform. Here is the most updated list of supported sources (AlienApps): https://cybersecurity.att.com/documentation/resources/pdf/usm-anywhere-alienapps-list.pdf

Some examples of logs include: Windows, Linux, Azure, Cisco Meraki, VMWare, PaloAlto, Semantic, BitDefender, etc.

If there is a commissioned device that is not listed on the supported devices list or there is not an active collection mechanism built into the SIEM for that supported technology, Cygilant and the Hospital's Cybersecurity Advisor will open a support ticket with AlienVault USM Anywhere support on behalf of the Hospital's team. AlienVault USM Anywhere will then custom-build a collection mechanism for that unsupported device, to ensure we can parse the log data and allow our SOC team to ingest and monitor that device for alerting purposes.

Any devices can be added or removed by the Cygilant SOC Team and/or the Hospital's Cybersecurity Advisor. All that is required is that their logs are sent to the SIEM, which can be done without any specific input from Cygilant. However, Cygilant asks that the Hospital inform Cygilant as a courtesy if they intend on adding or removing large volumes or noisy devices to ensure the Hospital receives the expected outcomes. The Hospital can inform Cygilant through phone, email, or SOCVue ticket. Subsequently, as long as logs continue to be delivered into the SIEM, service will be maintained.

For the ongoing integration between the Hospital' network and the SIEM technology, Cygilant will perform ongoing patches and updates. Cygilant can coordinate with the Hospital on times for this to occur. As with any system that must get patched, log collection will temporarily halt while the system is being updated or services are restarting.

24. Does your solution expect/require tools (SIEM, IDS/IPS, AV, EDR, Vulnerability Manager) be in place already?

No, as part of the service agreement Cygilant will provide access to and install all technologies for SIEM, IDS, AV/EDR and Vulnerability Management. The costs of these technologies are built into Cygilant's overall licensing proposal, attached to this RFP.

25. What are the total network bandwidth requirements for your solution?

The AlienVault USM Anywhere SIEM is hosted within AWS, by Cygilant. In order to collect data from the Hospital District – the District will need to download and install a very lightweight data sensor on one of their VMWare servers. The data sensor requires very little bandwidth requirements for the install and ongoing production.

26. What type of access/permissions will you need to our network?

Cygilant will need an outbound connection, through one of the District's external firewalls, to establish a connection to the sensor being hosted in the AWS cloud. Once that connection is established, we can start to send logs directly from network devices, cloud infrastructure, etc. to the AlienVault USM Anywhere SIEM.

27. What redundancies are in place to ensure constant operation of your solution?

Cygilant Responsibilities Include:

- Cygilant will ensure that Cygilant analysts and engineers assigned to the service are knowledgeable about the Cygilant and AlienVault toolsets.
- Cygilant will deliver the service as detailed in Section 4: Service Features.
- Cygilant analysts are responsible for meeting the SLAs in Section 7: Target Service Levels
- Cygilant is responsible for notifying Customer about data overages in a timely manner and giving Customer the option to purchase additional data.
- Cygilant shall retain the collected event log data for 12 months. (Additional storage is available for a fee.)
- Upon termination of cloud-based deployments, Cygilant will retain customer event log data in cold storage for up to 30 days. (Data storage charges apply.)
- Cygilant shall transfer data from cloud storage to the customer upon written request. (Data transfer charges apply.)

28. What redundancies do you expect us to have in place to accommodate constant operation?

The Hospital's Security Monitoring (AlienVault) Responsibilities Include:

- Customer shall cooperate with and assist the SOCVue Services Team in the performance of the services, and will provide the following resources necessary for the SOCVue Services Team's performance hereunder as specified.
- Customer is responsible for maintaining port/protocols required for communication between managed nodes and the security monitoring components (on-premises or cloud-based).
- If remote VPN access is required, Customer shall grant and provide the SOCVue Services Team with secure remote VPN access to the system running the security monitoring platform at all times during the term including all required access credentials (e.g. IP Address, URL, login account, password, etc.).
- Customer shall provide a list of authorized contact information (including name, phone, email, etc.) for both business hours and after hours.
- Customer shall appoint a contact designated to work with the SOCVue Services Team for all aspects, including escalations, related to the service(s) that will have authority to act on behalf of Customer.
- Customer will promptly communicate to the SOCVue Services Team any questions or concerns relating to the proper delivery of the services provided.
- Customer is responsible for remediation of any incidents about which they are notified.
- Customer will be responsible for providing the SOCVue Services Team with a complete listing of devices, servers, and applications to be monitored.
- Customer is responsible for procuring the necessary data quota to cover the monthly event volumes transmitted to AlienVault USM. In the event of an overage, Customer is responsible for taking action to reduce data volume or procure additional data in a timely manner.
- Customer is responsible for the cost of storing data beyond the standard 12-month retention period that comes with the purchased subscription level.
- Customer will be responsible for configuring the devices, servers and applications that will be monitored per the SOCVue Services Team instructions.
- Customer must provide and maintain a suitable system, meeting minimum system specifications, in a networked environment, with properly installed and patched Operating System (OS) software for operating any security monitoring components installed in the customer's environment.
- Customer must provide the appropriate prerequisite hardware and software necessary for the security monitoring components to be installed and operate properly.
- For on-premises components, Customer is responsible for backups and restore of the solution and all data needed.

The Hospital's Managed Endpoint (SentinelOne) Responsibilities Include:

- Customer shall cooperate with and assist the Cygilant Services Team in the performance of the services and will provide the following resources necessary for the Cygilant Services Team's performance hereunder as specified.
- Customer shall appoint a contact designated to work with the Cygilant Services Team for all aspects, including escalations, related to the service(s) that will have authority to act on behalf of Customer.

- Customer shall provide a list of authorized contact information (including name, phone, email, etc.) for both business hours and after hours.
- Customer will notify Cygilant of a change to contact details and provide alternative contacts in times of short-term unavailability.
- Customer will promptly communicate to the Cygilant Services Team any questions or concerns relating to the proper delivery of the services provided.
- Customer is responsible for maintaining port/protocols required for communication between endpoint agents and SentinelOne cloud components.
- Customer will be responsible for providing the Cygilant Services Team with a complete listing of endpoints to be licensed and protected by SentinelOne.
- Customer is responsible for verifying remediation of any incidents detected by the SentinelOne solution.

The Hospital's Vulnerability Management (Qualys) Responsibilities Include:

- Customer shall cooperate with and assist Cygilant in the performance of the services, and will provide the following resources necessary for Cygilant's performance hereunder as specified.
- Customer shall grant and provide Cygilant secure access to the system running the vulnerability scanner during the term including all required access credentials (e.g. IP Address, URL, login account, password, etc.).
- Customer shall ensure connectivity from vulnerability scanning tool and target systems.
- Customer shall provide a list of authorized contact information (including name, phone, email, etc.).
- Customer shall appoint a contact designated to work with Cygilant for all aspects, including escalations, related to the services that will have authority to act on behalf of customer.
- Customer will promptly communicate to Cygilant any questions or concerns relating to the proper delivery of the services provided.
- Customer is responsible for remediation of any vulnerability of which they are notified.
- Customer will be responsible for providing Cygilant with a complete listing of nodes to be managed and licensed, along with system credentials if required for a credentialed scan.
- Customer is responsible for procuring necessary node licenses for the vulnerability scanning.
- Customer must provide and maintain a suitable system, meeting minimum system specifications, in a networked environment, with properly installed and patched Operating System (OS) software for operating the vulnerability scanner.
- Customer must provide the appropriate prerequisite hardware and software necessary for the vulnerability scanners to be installed and operate properly.
- Customer is responsible for backing up and restoring the solution and all data needed.
- Customer is responsible for maintaining the confidentiality of SOCVue account credentials and is not to share credentials with other users. Cygilant retains the right to terminate access for violations.

29. **Please provide Software and Vendor names for your AV/EDR, IDS/IPS, SIEM, Vulnerability Management Systems, and any other services offered. If you are only offering management of existing services, please list compatible AV/EDR, IDS/IPS, Vulnerability Managers, and SIEM that you are able to manage for us.**

SIEM – AlienVault USM Anywhere

USM Anywhere centralizes security monitoring of networks and devices in the cloud, on premises, and in remote locations, helping you to detect threats virtually anywhere. USM Anywhere automatically collects and analyzes data across your attack surface, helping you to quickly gain centralized security visibility without the complexity of multiple disparate security technologies. With threat intelligence provided by AT&T Alien Labs, USM Anywhere is updated automatically to stay on top of evolving and emerging threats, so your team can focus on responding to alerts. USM Anywhere supports a growing ecosystem of AlienApps, enabling you to orchestrate and automate actions towards other security technologies so you can respond to incidents quickly and easily. It additionally provides main functionalities below:

Discover

- Network asset discovery
- Software & services discovery
- AWS asset discovery
- Azure asset discovery
- Google Cloud Platform asset discovery

Analyze

- SIEM event correlation, auto-prioritized alarms
- User activity monitoring
- Up to 90-days of online, searchable events

Detect

- Cloud intrusion detection (AWS, Azure, GCP)
- Network intrusion detection (NIDS)
- Host intrusion detection (HIDS)
- Endpoint Detection and Response (EDR)

Respond

- Forensics querying
- Automate & orchestrate response
- Notifications and ticketing

Assess

- Vulnerability scanning
- Cloud infrastructure assessment
- User & asset configuration
- Dark web monitoring

Report

- Pre-built compliance reporting templates
- Pre-built event reporting templates
- Customizable views and dashboards
- Log storage

Refer to AT&T website for information: (https://cybersecurity.att.com/products/usm-anywhere)

IDS – AlienVault USM Anywhere

AlienVault NIDS plays an important role in the USM Anywhere SIEM technology and provides contextualized alerting directly to our SOC through its built-in function. By detecting malicious network events, it provides vital information for correlation directives and cross-correlation rules. Combining this information with the events collected from other devices, USM Anywhere presents a complete picture of the malicious activity.

The AlienVault NIDS functionality, including monitoring network traffic and detecting malicious events, takes place on the USM Sensor. The USM Server consumes the NIDS signatures through plugins, which generates the AlienVault NIDS events. The correlation engine processes and correlates the normalized events, then stores them in the SIEM database.

Refer to AT&T website for information: (https://cybersecurity.att.com/documentation/usm-appliance/ids-configuration/about-alienvault-nids.htm)

AV/EDR – SentinelOne

The SentinelOne EDR platform unified prevention, detection and response in a single purpose-built agent powered by machine learning and automation. It provides and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into endpoint environment with full context, real-time forensics. This protects Windows, Mac and Linux.

SentinelOne Complete features include:

- Endpoint Prevention (EPP) to stop a wide range of malware, Trojans, hacking tools, and ransomware before they start.
- ActiveEDR Basic for Detection & Response (EDR) works in real time with or without cloud connectivity. ActiveEDR detects highly sophisticated malware, memory exploits, script misuse and other fileless attacks as they attempt to do damage. ActiveEDR responds at machine speed to autonomously contain damage
- ActiveEDR recovery gets users up and running in minutes and includes 100% remediation as well as rollback for Microsoft Windows
- Device Control for policy-based control of all USB device peripherals
- Firewall Control for policy-based control of network connectivity to and from assets, including location awareness
- Full Remote Shell capability for direct endpoint access by incident responders and forensics personnel

Refer to SentinelOne website for information: (https://www.sentinelone.com/platform/singularity-control/)

Vulnerability Management – Qualys

30. Do you threat hunt 24x7x365?

Cygilant has developed a 24x7x365 Security Monitoring service that addresses the significant challenges of security monitoring products:

- Managing the complexity of SIEM and Log Management products
- Lack of trained personnel to manage SIEM and Log Management products
- Difficulty of gaining useful or meaningful information from SIEM and Log Management products

SOCVue® Security Monitoring is a subscription-based service that delivers the proper people, process, and technology for an effective security program. Cygilant Cybersecurity Advisors (CA) will install and manage the AlienVault USM solution, and the Cygilant Security Operations Center (SOC) will continuously monitor and make customers aware of potential security incidents.

The service will help customers implement best practices for the maintenance, monitoring, and analysis of audit logs as recommended by SANS and the Center for Internet Security (Critical Security Control #6).

The key benefits that SOCVue Security Monitoring delivers to customers are:

- 24x7x365 Continuous monitoring of log and event data to detect potential security incidents
- Integrated network intrusion detection (IDS), file integrity monitoring (FIM), and threat intelligence feeds
- Timely investigation and notification about incidents that need attention
- Reporting on security events and alerts
- Assistance with compliance needs regarding FFIEC, PCI DSS, HIPAA, and other regulations
- Ongoing monitoring of the security monitoring application
- Monthly review with your Cygilant CA covering the customer's overall security posture and overall system health

31. During off hours is it an on call staffing or are there live analysts in SOC 24/7?

During off hours, Cygilant has 24x7 live SOC analysts staffed to support the needs and concerns of the Hospital District. They can be reached via direct phone or via email (soc@cygilant.com).

32. Are there times you do not provide monitoring services?

No, Cygilant will monitor Mayer Memorial Hospital District 24x7x365.

33. How many technical staff members do you have in total between all SOCs?

Cygilant has 35 security professionals globally.

34. Are analysts and engineers allocated evenly over shifts?

No, Cygilant SOC members, both analysts and engineers, are assigned in alignment to a few different factors:

- Busy and quiet periods of alert generation
- Customer hours of business
- Backlog of security engineering work
- Response to customer escalations
- Response to threat intelligence and significant immediate threats

35. **What Information Technology and Information Security certifications are held by your staff? Please list how many of each certification**.

Our staff have a range of industry standard certifications including from CompTIA, Microsoft, and courses in cyber security from accredited universities.

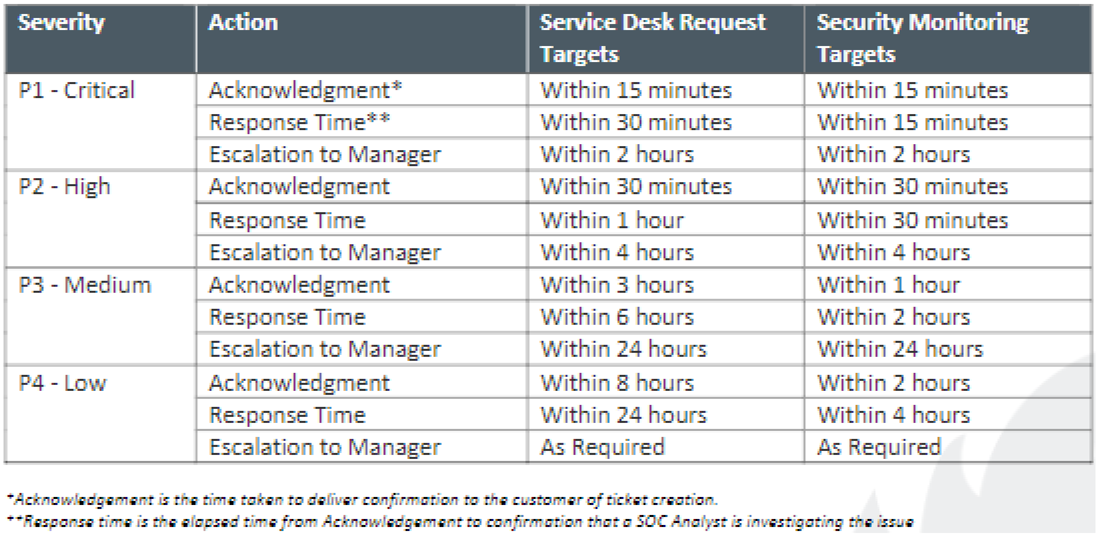
36. How do you keep your staff current with technology?

Cygilant SOC Analysts are trained in our internal and 3rd party partner tools as standard. Additional technology added to our service delivery is supported by appropriate training

37. Do you allocate time for your staff to attend training and/or obtain additional certifications?

Cygilant trains security analysts internally by using a combination of on-the-job shadowing and internal training resources to ensure analysts are fully equipped to analyse incidents and follow Cygilant's internal processes and systems. Training is provided for staff on a regular basis to support continual improvement, and certifications are supported when needed to formalize ongoing development.

38. What's your average response time?



Severity	Action	Service Desk Request Targets	Security Monitoring Targets
P1 - Critical	Acknowledgment*	Within 15 minutes	Within 15 minutes
	Response Time**	Within 30 minutes	Within 15 minutes
	Escalation to Manager	Within 2 hours	Within 2 hours
P2 - High	Acknowledgment	Within 30 minutes	Within 30 minutes
	Response Time	Within 1 hour	Within 30 minutes
	Escalation to Manager	Within 4 hours	Within 4 hours
P3 - Medium	Acknowledgment	Within 3 hours	Within 1 hour
	Response Time	Within 6 hours	Within 2 hours
	Escalation to Manager	Within 24 hours	Within 24 hours
P4 - Low	Acknowledgment	Within 8 hours	Within 2 hours
	Response Time	Within 24 hours	Within 4 hours
	Escalation to Manager	As Required	As Required

**Acknowledgement is the time taken to deliver confirmation to the customer of ticket creation.*
***Response time is the elapsed time from Acknowledgement to confirmation that a SOC Analyst is investigating the issue*

39. What's your average time to resolution?

Please refer to above answer to question no. 38.

40. Can I call into the SOC? Will I speak to an automated phone tree/scheduler?

For urgent issues, the Hospital will be given a direct phone line and email (soc@cygilant.com) to the SOC for any outstanding issues/concerns – and have access to this phone line/email on a 24x7 basis. The 24x7 SOC and an analyst will address those issues in real-time within our outlined SLAs. Therefore, the Hospital can reach out to and work directly with a SOC team member avoiding an automated phone tree/scheduler, as described above.

During normal business hours, the Hospital can raise any questions and concerns by 1) reaching out to their dedicated Cybersecurity Advisor via phone and email to ask for assistance on ongoing issues. If the Cybersecurity Advisor decides your issue needs to be escalated to the SOC, he/she will do so on your behalf and work with you until your issues are entirely resolved. 2) open a ticket in our SOCVue platform. The SOCVue platform will allow you to:

- View and manage alerts and incidents
- Initiate and manage tickets
- Track remediation outcomes
- Access security and compliance reporting

41. Do you perform background checks on your employees with access to customer information?

All Cygilant employees undergo full, enhanced background checks.

42. Will anyone ever access my data or perform investigations outside a secure environment (i.e. Home office, etc)

Your Cybersecurity Advisor will have access to both your SOCVue platform instance and your SIEM technology. However, there are security processes in place to ensure the security of the Hospital's data. Logs are encrypted in transit from the LogPoint collector to the LogPoint backend using Transport Layer Security (TLS) encryption. Alert data is encrypted in transit from the LogPoint backend to Cygilant using TLS. Log data stored in the Cygilant cloud is encrypted at rest using 256-bit Advanced Encryption Standard (AES).

43. Please describe your process for providing security for systems that cannot be secured to best practices, such as legacy systems that have not been replaced yet.

Best practice is always contextual, and Cyber Security is an exercise in Elastic Defense (Castle Defense / Defense in Depth) - Layers of security, not just a single line. The essence of this starts with doing the basics well. i.e., Regular Scans for Vulnerabilities, Manage Patching, Protect Endpoints, Monitor Systems, Continual Review & Improvement, Plan Actions for Response, etc.

Our security services are designed to cover these basics, to give an in depth defense against compromise, which works in partnership with your security program - Especially when some measures can't be taken (E.g. Awareness of XP vulnerabilities on POS devices via Qualys → CSA Team Advise upgrade path → Can't because of system driver support → CSA advises strategy to protect in multiple layers → Firewall / UAC / System Hardening / Best Practice Checks → Deploy Sentinel One Legacy Client for windows XP → Configure log monitoring → Regularly review status of high value / risk targets → Advise on future upgrade path.

44. Is security event data shared across your customer base? How is this handled to ensure confidentiality and HIPAA compliance?

Cygilant's SOCVue logically separates user data throughout its life cycle by marking/associating it with a code that is uniquely assigned to each customer. This code is used to logically differentiate, store, and retrieve data during all SOCVue operations. Authorization checks prevent a customer from accessing the data of another customer.

Furthermore, all data collected, processed, and stored by Cygilant is secured using industry best practices including encryption in-transit and at-rest, secure development practices, change control methodologies, and employee screening. Cygilant security controls are audited regularly and certified for SOC 2 compliance. Any third-party products used by Cygilant to deliver the service are SOC 2 and/or EAL 2+ certified.

45. How do you intend to help MMHD mitigate the impact of supply chain attacks?

Cygilant's services provide defense in depth, with multiple layers of protection and detection at different points in our customer's environments. This gives us the capability to detect lateral movement / post compromise activities, even against zero-day supply chain attacks. We monitor threat intelligence sources to learn of any new threats on IT supply chain assets and take immediate action to investigate and understand them when they are revealed. Following on from this, we undertake activities to add new detection for indicators of compromise, while working with our customers who may have been exposed to review their systems historically for any signs of exploit. Finally, our CSA team can work with your IT and internal security teams on ways to harden your own deployments, to include suppliers which align to standard such as SOC2, PCI, and ISO27001, all of which decrease your risk.

46. How do you handle onboarding and visibility of Cloud/SaaS environments such as O365 or cloud based EHRs?

The Hospital District will work directly with both the SOC team and their Cybersecurity Advisor for the onboarding and visibility of Cloud/SaaS environments suck as O365, etc. The Hospital District will notify their CSA of certain cloud environments that they would like to be monitored. As a result, the CSA will start to collect and ingest that data through the AlienVault SIEM and the SOC team will set certain alert rulesets that coincide with the Hospital District's preferred method of monitoring and other rulebooks already in place with the Cygilant SOC.

47. How do you monitor endpoints?

Cygilant will monitor all Mayers Memorial Hospital District's endpoint through our 24x7 Security Monitoring and Endpoint Management services. Both services are monitored and maintained by Cygilant's 24x7 global SOC, through the utilization of the AlienVault USM Anywhere SIEM Technology and SentinelOne EDR. We collect log and activity data either directly from the endpoint itself or through SentinelOne's EDR platform – for further analysis and investigation. All of the District's servers and workstations are fed through SentinelOne's EDR product – endpoints other than servers and workstations can be fed through the AlienVault SIEM. Those endpoints being fed through SentinelOne are monitored as followed:

SentinelOne Control is a Next Generation AntiVirus combining Endpoint Protection Platform (EPP) and EDR on a single agent. Static AI replaces traditional signatures and predicts malicious files. Behavioral artificial intelligence (AI) identifies and stops fileless attacks in real time. Autonomous and automatic threat responses trigger protective actions. SentinelOne also includes one-click remediation of unauthorized changes and one-click rollback to restore Windows systems affected by an attack. SentinelOne Control also includes:

- Network Control – policy-based control for inbound and outbound traffic on Windows, Linux, and Mac.
- Device Control – granular control for USB and Bluetooth on Windows and Mac.
- Rogue Device Discovery – uses passive and active sweeps to detect devices that are not

protected by SentinelOne.

The SentinelOne data is then fed through and collected by the AlienVault USM Anywhere SIEM. Depending on the alert rule of SentinelOne and alerts generated by the SIEM, the SOC will monitor these alerts for the Hospital District. Therefore, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. The SOC also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. By feeding the SentinelOne EDR produce through the AlienVault SIEM, the SOC team can cross correlate activity across the District's entire environment. Therefore, Cygilant's SOC teams provides better alerting, threat monitoring and will achieve full, 24x7 network visibility.

48. How do you monitor networks?

Similarly, to how Cygilant monitors the Hospital District's endpoints, we can monitor their networks through our 24x7 Security Monitoring service. Cygilant collects all log and event activity directly from every network device and cloud application/infrastructure on Mayers Memorial Hospital District's network. All the log and event activity are fed through the AlienVault USM Anywhere SIEM technology for security contextualization and analysis. The alerts generated by the SIEM technology are sent directly to Cygilant's SOCVue Platform which platform ingests 5 different Threat Intelligence feeds for further investigation. In real-time and on a 24x7x365 basis, the SOC team will monitor all alerts and activity across the Hospital Districts networks. Cygilant achieves this through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. Through these processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. Cygilant also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. Furthermore, every workflow follows these rules and is documented and recorded for compliance purposes.

49. What (if any) access to Firewalls are necessary to adequately monitor?

There will be no access needed from the Hospital District's firewalls for Cygilant's Security Monitoring service and the 24x7 SOC team to adequately monitor them. The Hospital would have to forward the log data – either via syslog or NxLog – to the AlienVault data collector (sensor). This data is then transmitted to AlienVault USM Anywhere for processing/threat intelligence/parsing/etc. Alerts generated by the AlienVault SIEM are collected by the cloud based Cygilant SOCVue platform for review by the SOC.

If the Hospital District has any firewalls owned and maintained by a third-party vendor, Cygilant will need approval and access from that third-party vendor to send log data from those firewalls to the AlienVault sensor.

4.d MDR

50. Do you offer different service level options for security monitoring/alerting?

No.

51. If yes, what service level option are you quoting for?

Please refer to my answer to No. 50.

52. Does your service include a process for adding new rules/event correlations/sources? If yes, please explain your approach for communicating and gaining approval for these recommendations.

The District will have ongoing monthly meetings with the assigned Cybersecurity Advisor to review open tickets and incidents, analyze alert rules, discuss event correlations, reporting needs and future deployment plans, and schedule follow-up calls as needed. They will also engage in discussions around current sources being collected and sources to add/remove from the service. These types of changes will frequently be discussed in these meetings. If a change is within the scope of the existing agreement, the Cybersecurity Advisor, with the Districts' permission, will be able to make those changes accordingly. If the change is a new feature and there is a cost involved, the Cybersecurity Advisor, Cygilant Account Manager, and District's team will discuss, agree on, and make changes based on what is in the best interest of the customer.

53. How often are signatures and threat intel updated?

Signatures and threat intelligence are updated based on new and evolving threats. Depending on the SIEM or MDR platform, regular updates can range from once a month to several times a week. For significant emerging threats impacting our customer base (E.g. Hafnium, SolarWinds, Kaseya), we seek to deploy security content as soon as it is available, outside of release schedules, E.g. less than 24 hours in some cases.

54. How do you classify/prioritize security events?

Severity	Description
P1 – Critical	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be an ACTIVE threat against business impacting customer assets.
P2 - High	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a PROBABLE (current, possible impact) threat against business impacting customer assets.
P3 - Medium	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a POTENTIAL (not current, may have future impact) threat against business impacting customer assets.
P4 - Low	An Incident identified either by automated correlation rules or through SOC analysis that may require further investigation, with no apparent threat against business impacting customer assets.

55. What is your process for detecting and responding to a threat?

The SOC team will continuously investigate and triage any alerts or incidents occurring on the Hospital's network to ensure there is no real threat to their security or network. This investigation begins at the SIEM level – configuring and finetuning the technology to trigger alerts for suspicious activity or security violations. These alerts are investigated on a 24x7 basis by Cygilant SOC analysts through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. If an alert generated by the SIEM technology requires further investigation by a SOC analyst, rather than being ruled out as a false positive, white noise, etc. the SOC analyst will create an incident and begin investigating that alert. Through these incident review processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. The SOC also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. After an incident has been fully investigated by our SOC and is needed to be escalated to the Hospital District, the SOC team will open a "ticket".

Dependent on customer handling preferences and the analysis done by the SOC, the SOC will provide actionable remediation guidance to be able to respond to the outstanding threat. If there are steps able to be taken utilizing both the SIEM technology and SentinelOne – depending on customer handling preferences – the SOC can respond in alignment with those processes.

56. How are events sorted between positive and false positive?

Customer onboarding includes a period of configuration and baselining, which allows us to configure the SIEM alerts to be relevant and vastly reduce false positives. During normal operations, if SOC analysis of alerts determines a false positive is present or suspected, a ticket will be created to modify customer security content to eliminate it. This is a process of continual improvement in line with the lifecycle of security content management. (NB. False Positive is explicitly defined here as being a detection / content issue… I.e. an alert was raised saying "X has been detected" when X was not present - NOT a true positive alert, of low / no security threat or value.)

57. What is the turn-around time from detection to remediation, on average?

For our MDR service, the average time is almost immediate, because most remediation activities are automated in the platform, before additional analysis or review where needed. This process is tuned during onboarding to avoid operations interruptions on business-critical systems and software.

58. How do you teach your clients to improve their security postures?

Cygilant teams, both the Cybersecurity Advisor (CSA) and the SOC team, work with our customers on constantly updating our knowledge of their environment and their risk profiles. During these regular reviews, the Cybersecurity Advisor will seek to identify the highest priority security risks through dialog with the customer. Cygilant will also build a knowledgebase about authorized admins and "normal" activity on the network. These regular reviews with your CSA will be conducted monthly meetings with your team. The goal of those meeting is to discuss how you can improve your cybersecurity posture – i.e. reducing incident response time, generating better alerts coinciding with your security objectives, relying on your CSA as an "advisor" to ask question about improvement, etc. We want to give you access to the security experts (CSA and SOC) so that we can not only meet your security objectives, but also grow and improve them.

59. How do you improve monitoring capabilities over time based on event history?

All Cygilant SOC services are based on the principle of continual improvement. Our MDR service is regularly updated with new alert content, based on historical events and the changing threat landscape (new threats). Our analysts continually look for improvement opportunities, from all points of our operations and analysis workflows. In parallel, the MDR service platform and endpoint agents use machine learning techniques to continually monitor for and respond to zero day / unknown threats.

60. Does your proposal include 24x7 hunting for threats(including zero day threats) within our environment?

The SOC provides 24x7 threat monitoring of event logs and alerts. Threat intelligence staff at Cygilant will develop new security detection content when new zero-day threats are announced. We often deploy new detection policies even before our security vendor partners are able to release updates to the products. In these situations, the SOC will perform proactive hunts in your environment if there is a possibility that the zero day may have been exploited before being discovered by the industry and disclosed publicly.

61. How do you perform this hunting?

Threat hunting is performed using inbuilt tools inside our MDR.

62. Is there any special software we need to deploy to support this hunting?

Yes, the Sentinel One agent must be deployed on all monitored endpoints, alongside log collectors on servers. This software is included in the cost proposal attached to the RFP above.

63. What part do humans play in the threat hunting lifecycle?

Humans are a core component of threat hunting, using their knowledge and expertise to identify potentially suspicious activity over and above what pre-determined analytics or machine learning can spot. Our threat hunting is aided by the tools available, but is very much built around human processes and insight

64. Describe your methodology for remediation on our behalf and how notification of these actions will be handled.

Our MDR platform implements proactive blocking and quarantine of malicious threats. It also supports detection of threats which are deemed suspicious, which are available for an analyst to choose to kill or quarantine from the console. In both cases customers are notified about all actions taken. Depending on customer preference we can put in place escalation requirements before analysts actively kill / quarantine or can edit the detection logic to whitelist activity.

4.e Incident Analysis and Response

65. Do you perform real-time inspection of every packet utilizing full packet capture? If you do full packet capture please explain how long you do it for, when it starts, and how long you retain it for?

Cygilant cannot perform this type of activity, but we can leverage our Cygilant partners on a separate retainer that can accommodate these requests. Retainers for our partners can be discussed as an add-on to Cygilant's services. Our partners' retainers are not included in the cost proposal of this RFP.

66. Does your solution detect unknown threats and attacks leveraging patterns and behavioral analytics?

Our MDR service contains both signature and machine learning / AI backed detection which is able to identify anomalous and suspicious behavior without advanced signature knowledge of the malicious activity.

67. Does your solution detect based on signatures and IOC's?

Yes, our SIEM and MDR have the ability to detect or block activity based on emerging IoCs, signatures and correlation rules defined by the vendor or by Cygilant.

68. Do you do full forensic analysis to confirm threats and eliminate false positives?

Cygilant analyzes the information available inside the systems based on the data being passed to us from the customer network. This data is inspected to confirm the existence of a threat over and above whatever information is available in an alarm directly. It is also used to support recommendations for whitelisting / suppression of benign activity inside the customer environment. We do not have access directly to hosts for the purposes of investigation and require partnership with the customer where additional information must be gathered.

69. Are you able to do near real-time communication disruption and isolation of threats on client's behalf?

Our MDR service has the ability to isolate a potentially infected host from the network entirely while retaining MDR access or to enact firewall rules to block network communication with destinations based on the threat.

70. If so, are these placed autonomously or by human decision? If both please specify when and how the decision is derived.

It is possible to configure the MDR to automatically enact these reactions to malicious threats. Generally, this not how our MDR customers have the system configured and it is left to analyst discretion on a case-by-case basis. Given that the MDR kills and quarantine a threat, then it is unusual for us to suspect additional activity on the host such that isolation or firewall blocking is immediately required outside of the customer directing us to enact that. Therefore, those actions are taken after customer engagement if the customer requests it for additional mitigation. This arrangement is open to change based on customer preferences.

71. Please describe the level of support provided until incident is remediated and threat actor is eliminated.

The SOC is available to provide insight and analysis of data which is present in the SIEM. We will liaise with any external forensics team or internal remediation team for the customer as needed. The SOC will be on hand to analyze the data at the Hospital Districts disposal until the issue is resolved.

72. Do you charge retainers or extra fees on top of your base costs for this incident response capability? If so, please elaborate on what this entails and how you charge for these services

We do not support services for forensics / incident response directly. Should this service be needed we have a partnership with Incident Response companies who can be engaged for additional fees. We will then work directly with that IR organization and yourselves regarding incident response based on the information we have available inside our systems.

73. What would constitute a variable bill?

Cygilant does not charge via variable bill, these costs are built into our annual cost of our services. If we need to engage in a retainer with an Incident Response partner, those costs will depend on that partner.

74. At what point do you engage MMHD's Information Security Staff to assist?

Should activity be blocked by our MDR then the District would be notified after the fact that it has occurred and may be asked to carry out further investigation to conclude that no additional threat persists. Should activity be detected by the SIEM and an analyst has evaluated it as a valid threat requiring further remediation then this will be raised to the Hospital District for further assistance.

75. What does your normal escalation and notification process look like?

The SOC team will continuously investigate and triage any alerts or incidents occurring on the Hospital's network to ensure there is no real threat to their security or network. This investigation begins at the SIEM level – configuring and finetuning the technology to trigger alerts for suspicious activity or security violations. These alerts are investigated on a 24x7 basis by Cygilant SOC analysts through a Level 1-to-4-tiered model of alert recognition and escalation, which is the most comprehensive alert investigation and triage process in the industry. If an alert generated by the SIEM technology requires further investigation by a SOC analyst, rather than being ruled out as a false positive, white noise, etc. the SOC analyst will create an incident and begin investigating that alert. Through these incident review processes, the SOC provides detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations, and suggest improvements. The SOC also advises on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation. Cygilant does not just forward event logs without context – our SOC analysts provide analysis and stand by to answer any questions. After an incident has been fully investigated by our SOC and is needed to be escalated to the Hospital District, the SOC team will open a "ticket".

"Tickets" are actionable security related incidents or custom alerts that the SOC team has escalated directly to the Hospital District for action needed to be taken to remediate or needed interaction between the Hospital and the SOC. The severity of these tickets can range from "Critical to Low" dependent on the severity of the event determined by the SOC and customer handling preferences. The Hospital will decide with their Cybersecurity Advisor and the SOC team during onboarding to determine how they prefer to be notified, either via phone call or email. The Hospital District can also determine a chain of command within their IT team as part of the ticketing process to ensure that the SOC will reach an IT team member at the Hospital District and notify them of the security incident.

Every "open ticket" (i.e. tickets that are unresolved between the SOC and the Hospital District) are integrated with our SOCVue platform to be worked-on and viewed by the Hospital District. The SOCVue platform is a multi-tenant interactive platform created and developed by Cygilant. The purpose of SOCVue is to provide the Hospital District a single pane of glass to simplify and consolidate multiple streams of security data to help detect and respond to threats faster. It will allow the Hospital District to view and manage alerts and incidents, initiate, and manage tickets, track remediation outcomes, and access security and compliance reporting. The SOC team works in the same SOCVue platform as the Hospital District to provide direct, customizable alerts. Therefore, the Districts are alerted on both critical security-related incidents and any customizable alerts desired. Also, by working in the same platform, the Hospital District can see Cygilant's SOC threat hunting and monitoring processes in real-time.

At a high level, SOCVue provides an overarching view of the Districts' entire environment for complete network visibility, portrayed through dashboards. The dashboards provide meaningful information about network activity without having to dive deeper into alerts or incidents. Examples of these dashboards include: Nodes being collected from, Assets at Risk, Top Source and Destination IPs, Alerts by Severity, and Average Time to Incident Resolution. However, the SOCVue platform also allows the Hospital District a granular view of their environment all the way down to the raw log if needed.

In the SOCVue dashboard, there will be an "open tickets" drilldown. This drilldown will provide all of the open tickets that are either security-related incidents or custom alerts that have been escalated by the SOC team to the Hospital District. By simply responding to these tickets, the Districts and the SOC will resolve and close out that security related incident or custom alert. However, the Districts can further drilldown into that ticket to both the incident and the alert level. In the incident drilldown, the SOC will provide information on the time of the alert, affected system, probable cause, impact, best practices and suggested remedy. This shows the forensic analysis done by the SOC to ultimately escalate this incident to an alert. Furthermore, in the incident drilldown, the Hospital District will be able to dive deeper all the way down to the Alert Drilldown. In the alert drilldown, the Hospital District will be able to get information about the alert that triggered the incident, down to the raw log itself.

Please see attached photos of our SOCVue platform:

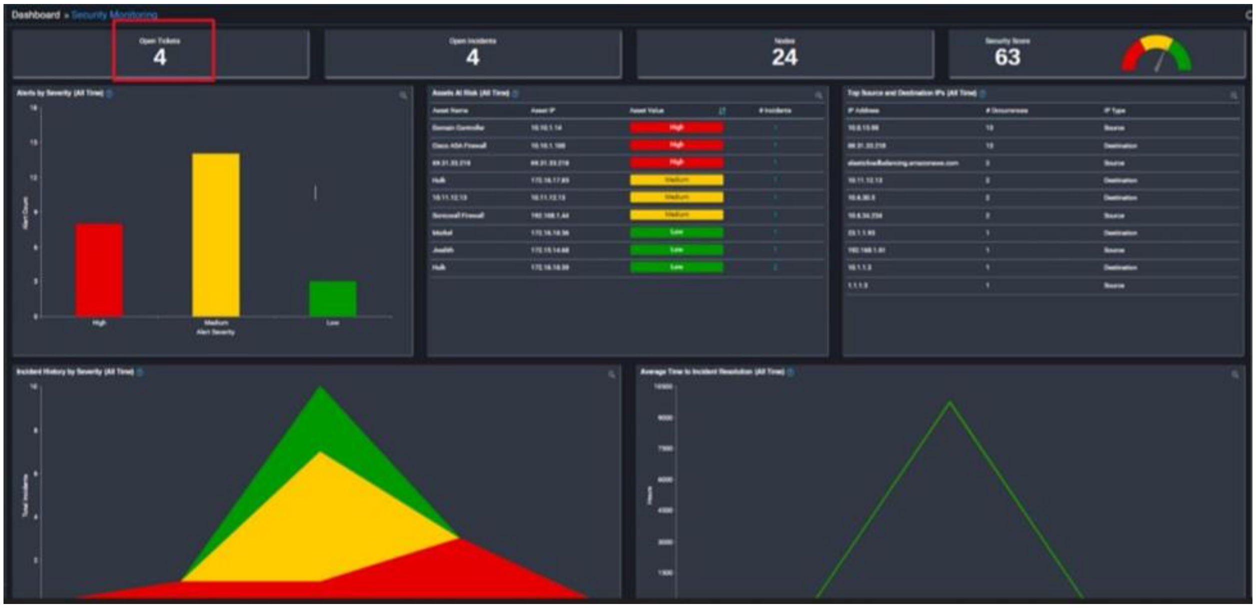
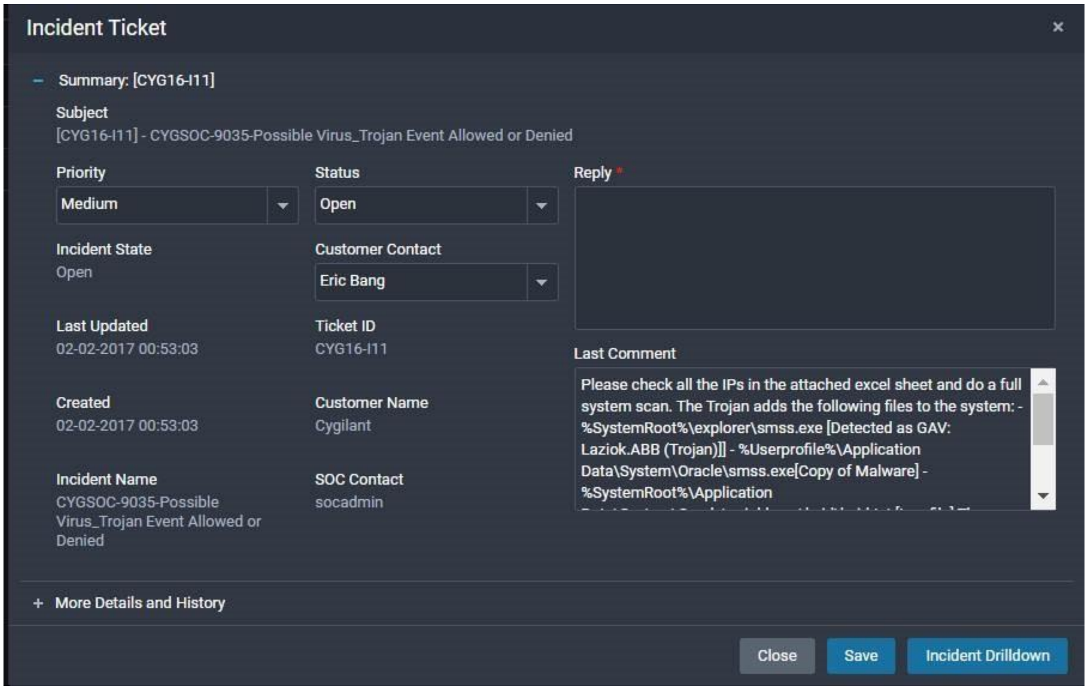

Dashboard » Security Monitoring
Open Tickets
4
Open Incidents
4
Nodes
24
Security Score
63
Alerts by Severity (All Time)
High
Medium
Low
Alert Severity
Assets At Risk (All Time)
Top Source and Destination IPs (All Time)
Incident History by Severity (All Time)
Average Time to Incident Resolution (All Time)

Figure 1: SOCVue Dashboard View



Incident Ticket ×

− Summary: [CYG16-I11]

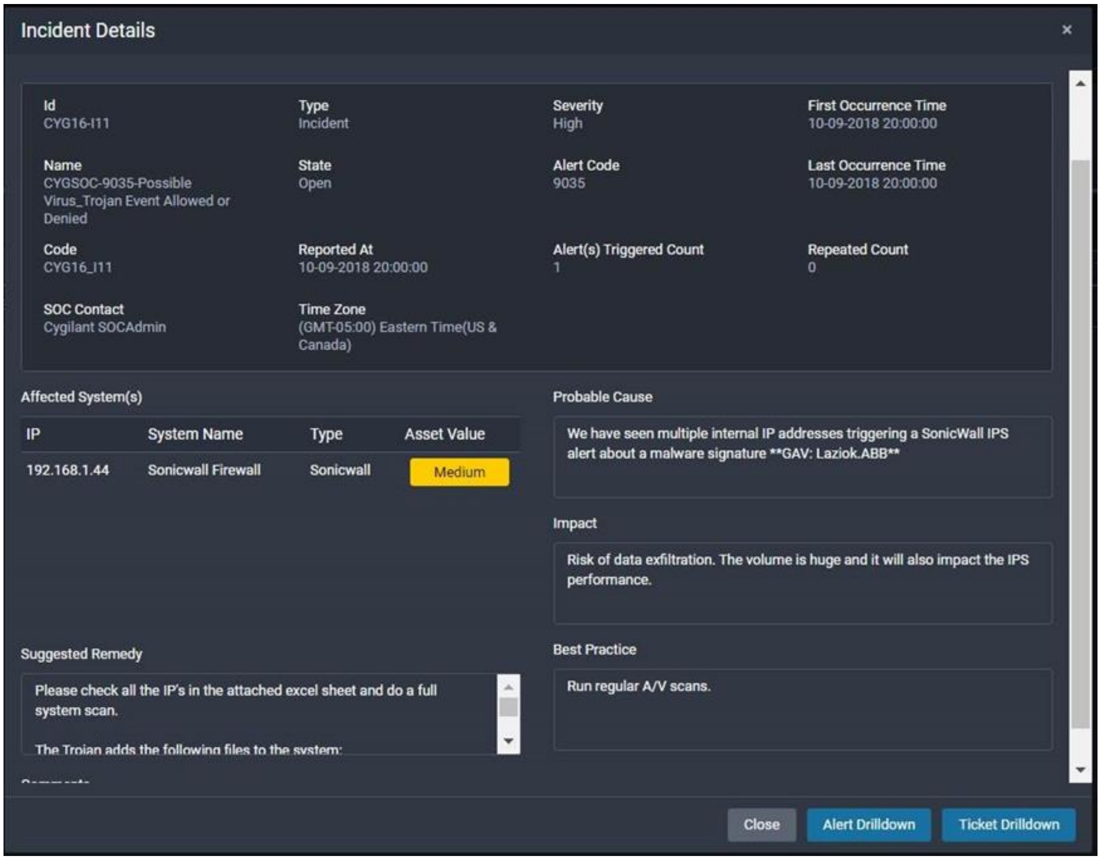
Subject

[CYG16-I11] - CYGSOC-9035-Possible Virus_Trojan Event Allowed or Denied

Priority Medium	Status Open	Reply *
Incident State Open	Customer Contact Eric Bang	
Last Updated 02-02-2017 00:53:03	Ticket ID CYG16-I11	Last Comment Please check all the IPs in the attached excel sheet and do a full system scan. The Trojan adds the following files to the system: - %SystemRoot%\explorer\smss.exe [Detected as GAV: Laziok.ABB (Trojan)]] - %Userprofile%\Application Data\System\Oracle\smss.exe[Copy of Malware] - %SystemRoot%\Application
Created 02-02-2017 00:53:03	Customer Name Cygilant	
Incident Name CYGSOC-9035-Possible Virus_Trojan Event Allowed or Denied	SOC Contact socadmin	

+ More Details and History

Figure 2: Incident Ticket



Incident Details ×

Id
CYG16-I11

Type
Incident

Severity
High

First Occurrence Time
10-09-2018 20:00:00

Name
CYGSOC-9035-Possible Virus_Trojan Event Allowed or Denied

State
Open

Alert Code
9035

Last Occurrence Time
10-09-2018 20:00:00

Code
CYG16_I11

Reported At
10-09-2018 20:00:00

Alert(s) Triggered Count
1

Repeated Count
0

SOC Contact
Cygilant SOCAdmin

Time Zone
(GMT-05:00) Eastern Time(US & Canada)

Affected System(s)

IP	System Name	Type	Asset Value
192.168.1.44	Sonicwall Firewall	Sonicwall	Medium

Probable Cause

We have seen multiple internal IP addresses triggering a SonicWall IPS alert about a malware signature **GAV: Laziok.ABB**

Impact

Risk of data exfiltration. The volume is huge and it will also impact the IPS performance.

Suggested Remedy

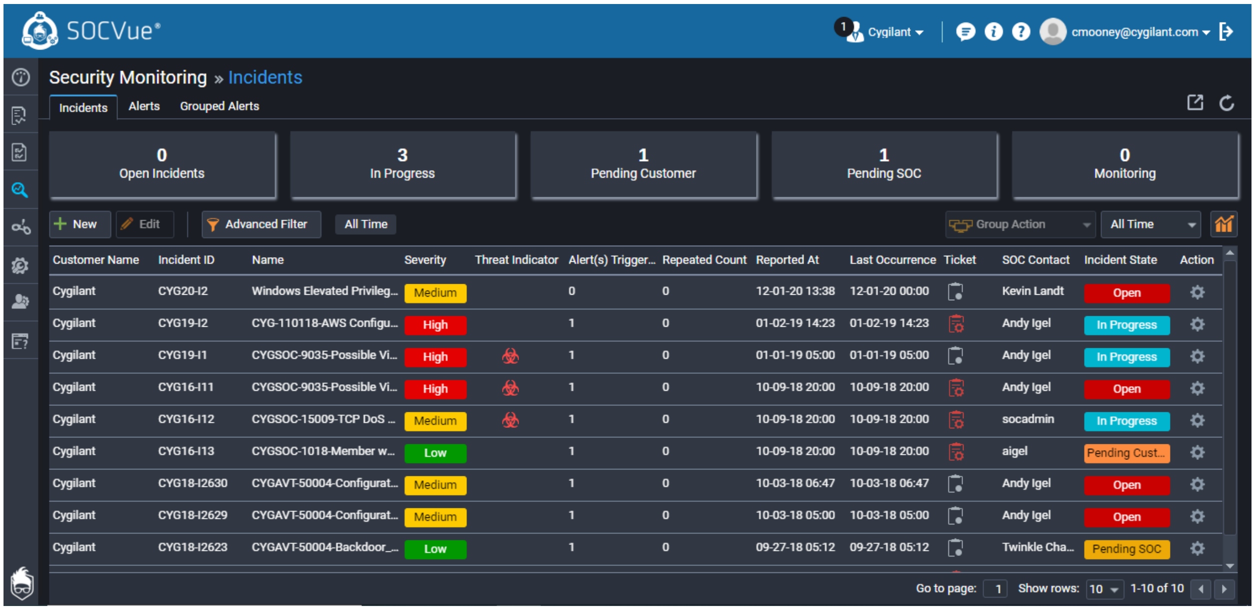
Please check all the IP's in the attached excel sheet and do a full system scan.

The Trojan adds the following files to the system:

Best Practice

Run regular A/V scans.

Figure 3: Incident Ticket Details



Security Monitoring » Incidents

0 Open Incidents | 3 In Progress | 1 Pending Customer | 1 Pending SOC | 0 Monitoring

Customer Name	Incident ID	Name	Severity	Threat Indicator	Alert(s) Trigger...	Repeated Count	Reported At	Last Occurrence	Ticket	SOC Contact	Incident State	Action
Cygilant	CYG20-I2	Windows Elevated Privileg...	Medium		0	0	12-01-20 13:38	12-01-20 00:00		Kevin Landt	Open	⚙
Cygilant	CYG19-I2	CYG-110118-AWS Configu...	High		1	0	01-02-19 14:23	01-02-19 14:23		Andy Igel	In Progress	⚙
Cygilant	CYG19-I1	CYGSOC-9035-Possible Vi...	High	☣	1	0	01-01-19 05:00	01-01-19 05:00		Andy Igel	In Progress	⚙
Cygilant	CYG16-I11	CYGSOC-9035-Possible Vi...	High	☣	1	0	10-09-18 20:00	10-09-18 20:00		Andy Igel	Open	⚙
Cygilant	CYG16-I12	CYGSOC-15009-TCP DoS ...	Medium	☣	1	0	10-09-18 20:00	10-09-18 20:00		socadmin	In Progress	⚙
Cygilant	CYG16-I13	CYGSOC-1018-Member w...	Low		1	0	10-09-18 20:00	10-09-18 20:00		aigel	Pending Cust...	⚙
Cygilant	CYG18-I2630	CYGAVT-50004-Configurat...	Medium		1	0	10-03-18 06:47	10-03-18 06:47		Andy Igel	Open	⚙
Cygilant	CYG18-I2629	CYGAVT-50004-Configurat...	Medium		1	0	10-03-18 05:00	10-03-18 05:00		Andy Igel	Open	⚙
Cygilant	CYG18-I2623	CYGAVT-50004-Backdoor_...	Low		1	0	09-27-18 05:12	09-27-18 05:12		Twinkle Cha...	Pending SOC	⚙

Go to page: 1 Show rows: 10 1-10 of 10

Figure 4: SOCVue Incidents List

76. Does your service provide full response reports on investigations?

Should a customer require a formal report about activity from an investigation of a potential breach then that can be provided after the investigation concludes and any remediation activity has been carried out.

77. How quickly can a full breach report be developed so we can notify affected individuals?

This would be dependent on the complexity of the investigation and what activity needs to be performed by an Incident Response partner of Cygilant's. We are happy to engage with supplying information and narratives to the construction with such a report with our Incident Response partners. We have a list of partners we can engage, and the District can choose from.

4.f Metrics, Reporting and Dashboards

78. Do you provide operational reports to your customers?

Cygilant creates monthly scorecards as well as executive reports that are generated on a regular cadence and sent directly to the customer. Your Cygilant Cybersecurity Advisor will review the options with the Hospital during onboarding. Some examples include monthly executive summary, compliance reports (HIPAA, NIST, etc.) for auditing, and monthly scorecards.

We have standard reports as well as we can create ad-hoc/custom reports based on the requirements needed to your liking. These reports can be adjusted to daily/weekly/monthly as an example.

AlienVault USM Anywhere generates these reports:

- **My Reports -** These reports are generated from your report creation feature and are selectable by categories, which are assets, asset groups, alarms, events, vulnerabilities, and configuration issues. You can also choose the format of the report (HTML and CSV).
- **Compliance Templates -** These are compliance templates based on alarms, vulnerabilities, and events collected in the system. The templates are grouped into PCI, NIST CSF, HIPAA, and ISO 27001. See USM Anywhere Compliance Templates.
- **Event Type Templates -** These are event templates based on event categorization by type of data source and by the most used data sources, see USM Anywhere Event Type Templates.
-

79. What is the frequency for customer reporting?

The Hospital can reach out to the Cybersecurity Advisor as many times during the partnership for any type of reports they would want to be generated and can also run their own ad-hoc reports at their own discretion. These unlimited reports are included in the agreed upon service contract. The monthly SOC reports/scorecards are generated on a monthly based and discussed as part of the monthly meetings with your Cybersecurity Advisor. The Hospital can also propose changes to the monthly SOC reports to generate new data

80. Can you provide sample reports?

Sample monthly SOC reports are attached on pages *47-53* of this RFP. The report attached is customized to the client's environment, needs and security objectives.

81. What is your preferred method for delivery of customer reports?

The preferred method for the delivery of customer reports is our SOCVue platform. The reports the Hospital requests will be imported into the "Reports" tab of our SOCVue portal for historical and logging purposes. The Cybersecurity Advisor will also generate and deliver monthly reports and ad-hoc reports directly to the customer, as requested.

If the customer would like to run their own ad-hoc reports by logging into the back-end SIEM – aforementioned above, they can generate those reports in real-time and download those reports as necessary.

82. Are real time data and operational reports exportable? If so, what formats are supported?

The Hospital can export real-time data and operational reports via the back-end AlienVault USM SIEM technology as well as our Cygilant SOCVue portal. All data and reports are exportable via PDF, HTML, CSV, etc.

If the Hospital would prefer the data and reports be exported by their Cybersecurity Advisor, they can reach out to that Advisor and request the data and reports as necessary.

4.g Data Management

83. Where does my data reside?

Cygilant maintains strict written information security and confidentiality policies that ensure security controls are in place to protect customer data. These policies and employee training practices are audited by a third party for SOC 2 compliance. These documented policies include, but are not limited to, the following areas, which are reviewed and updated on a regular basis: Physical Security, Access Controls, Software Development Lifecycle, Data Retention, Backup Policy, Configuration Standards, Incident Handling, and Acceptable Use. Cygilant's Security and Compliance Manager works with business groups within the company to ensure implementation and auditing.

Furthermore, Cygilant hosts the AlienVault USM Anywhere instance and customer data in AWS Northeast. Cygilant would house the main SIEM back end in AWS and a smaller lightweight data collector for AlienVault would be set up to facilitate the collection of logs/events to forward to the cloud based SIEM. The installation of the sensor is either on a VMWare or HyperV server – and based on the Hospital's network, the sensor will be installed on VMWare. Furthermore, Cygilant purposefully hosts in AWS – to ensure the safety of customer data.

84. Data retention: How long will your company store data collected/created?

The Districts data will be collected and stored in AWS for the entire duration of the contract. Event logs will be available in AlienVault USM for analysis and reporting during the Hot Storage period. The Hot Storage period is 15 Days, 30 Days, or 90 Days depending on your purchase agreement. After the Hot Storage period, logs will be archived and will no longer be available for the Cygilant SOC team to search, report or provide forensics on. However, the logs are still available for the customer to download and utilize on their own. Logs will be archived for a total of 12 months from the collection time.

To help meet compliance requirements, event log data will be archived in cloud storage beyond the hot storage search and report timeframe. The archived data will not be immediately available for analysis and reporting. Archived data will be provided to the customer in CSV format upon request within 3 business days (Data transfer charges apply). Logs will be retained for a total of 12 months from the collection date. Additional storage beyond 12 months is available for an additional fee.

85. Data destruction: What is the process for purging or destroying historical data after use?

Events and log data collected by AlienVault are kept in hot storage for the time period you select (15, 30, or 90 days) and then purged automatically. Raw logs are stored by AlienVault for the duration of your subscription. If your subscription expires and you decide not to renew, your AlienVault USM Anywhere instance will be decommissioned 14 days after the expiration. All data, including asset information, orchestration rules, user credentials, events, and vulnerabilities (hot storage), and raw logs (cold storage), will be destroyed.

AlienVault alarm data forwarded to the Cygilant SOCVue platform will be stored for 1 year or until your agreement ends. You then have 30 days to request the data. Cygilant will delete your SOCVue account and purge the associated data 30 days after the agreement ends.

86. In the event we need comprehensive forensic data for a breach investigation, can you provide it and to what degree?

Event data in AlienVault hot storage is available for the Cygilant SOC to search and include in reports to assist in a breach investigation. The SOC will assist you with interpreting the data as it relates to the security incident. Raw log data in AlienVault cold storage will no longer be available for the Cygilant SOC team to search, report or provide further analysis on. However, the logs are still available for the customer to download and utilize on their own. This archived data will be provided to the customer in CSV format upon request within 3 business days. Analysis of cold storage data might be possible as an additional professional services engagement depending on availability of SOC resources. Cygilant cannot provide forensic data beyond what was collected as part of the ongoing service. For more comprehensive forensic services, Cygilant can recommend and introduce one of our incident response partners.

4.h Pricing

87. What services from your offerings are being proposed?

Security Monitoring, Endpoint Management (Detection and Response) and Vulnerability Management

88. What is the pricing model for each component?

Cygilant's Security-as-a-Service offerings are subscription-based services licensed to Mayers Memorial Hospital District in the attached pricing proposal. The pricing for our services is an all-encompassing price. There are no one-time costs tied to the contract. All costs are recurring costs and payment is due annually. All technology used (AlienVault USM Anywhere SIEM, SentinelOne, Qualys and SOCVue platform) to perform Cygilant's services are included in the overall price of the agreement.

89. Are additional discount rates available for longer duration contracts? If so, what are they for what duration?

Yes, the cost/year for Cygilant's Security-as-a-Service will be discounted on a 3-year agreement (paid annually) as compared to the 1-year agreement attached in this RFP proposal.

90. Please provide detailed cost breakdowns of your proposal including any additional startup costs, maintenance costs, ongoing support costs, incident retainers and other fees or required payments associated to your solution. If third party software or subscription services are required, include these in this assessment.

A detailed cost breakdown of our proposal is presented on page 3 of this RFP.

4.i Client Satisfaction

91. How do you track your customer satisfaction?

Each of our customers is assigned a dedicated CyberSecurity Advisor (CSA). Your CSA will conduct monthly meetings with your team to go over everything that's taken place over the last 30 days as well as provide reports to the team. In addition to the CSA, you will be assigned an Account Manager (Sales Representative) and Executive Sponsor (member of our Senior Management Team) to ensure excellence of our services. Customer centricity is very important to our organization, and we strive for excellence.

92. Do you have SLA's or SLO's? If so, please provide the matrix.

Service desk requests can be initiated by call or email, or by opening a ticket in SOCVue.

The Cygilant SOC will respond to service desk requests based on the priority level of the request as shown in Table 6 below.

Severity	Action	Service Desk Request Targets	Security Monitoring Targets
P1 – Critical	Acknowledgement*	Within 15 minutes	Within 15 minutes
	Response Time**	Within 30 minutes	Within 15 minutes
	Escalation to Manager	Within 2 hours	Within 2 hours
P2 - High	Acknowledgement	Within 30 minutes	Within 30 minutes
	Response Time	Within 1 hour	Within 30 minutes
	Escalation to Manager	Within 4 hours	Within 4 hours
P3 - Medium	Acknowledgement	Within 3 hours	Within 1 hour
	Response Time	Within 6 hours	Within 2 hours
	Escalation to Manager	Within 24 hours	Within 24 hours
P4 - Low	Acknowledgement	Within 8 hours	Within 2 minutes

Severity	Action	Service Desk Request Targets	Security Monitoring Targets
	Response Time	Within 24 hours	Within 4 minutes
	Escalation to Manager	As Required	As Required

Table 1: Service Desk Service Level Agreements

*Acknowledgement is the time taken to deliver confirmation to the customer of ticket creation. Notification SLAs are subject to low-noise default settings, modified by customer notification preferences.
**Response time is the elapsed time from Acknowledgement to confirmation that a SOC Analyst is investigating the issue.

Cygilant may schedule maintenance outages for Cygilant-owned equipment/servers that are being utilized to perform the services with 24 hours' notice to designated customer contacts. The Service Levels are subject to the following terms, conditions, and limitations:

- The Service Levels shall not apply during scheduled maintenance outages.
- The Service Levels shall not apply in the event of any customer-caused service outage that prohibits or otherwise limits Cygilant from providing the Service, delivering the Service Levels or managed service descriptions, including, but not limited to, customer's misconduct, negligence, inaccurate or incomplete information, modifications made to the Services, or any unauthorized modifications made to any managed hardware or software by the customer, its employees, agents, or third parties acting on behalf of the customer.

Furthermore, the Service Levels shall not apply to the extent that the customer does not fulfill and comply with the obligations and interdependencies set forth within contractual documents.

93. How will breaches of SLA be handled?

When SLA breaches are escalated, Cygilant would perform an RCA (root cause analysis) which would investigate what caused the miss. With that, we would make process or personnel adjustments to prevent reoccurrence.

94. Do you ever participate in meetings with clients, regulators and due diligence questionnaires?

Cygilant engages in regular monthly meeting with our clients – as part of the partnership the District and the Cybersecurity Advisor. We are happy to supply necessary information needed for meeting with regulators as well. If the District would need a representative from Cygilant to come on-site for assistance, we are happy to do so as well.

5. Cygilant Security-as-a-Service Technical Explanation

SOCVue Security Monitoring (AlienVault USM Anywhere)

Overview:

Cygilant has developed a 24x7 global Security Monitoring service that addresses the significant challenges of security monitoring products:

- Managing the complexity of SIEM and Log Management products
- Lack of trained personnel to manage SIEM and Log Management products
- Difficulty of gaining useful or meaningful information from SIEM and Log Management products

SOCVue® Security Monitoring is a subscription-based service that delivers the proper people, process, and technology for an effective security program. Cygilant Cybersecurity Advisors (CA) will install and manage the AlienVault USM solution, and the Cygilant Security Operations Center (SOC) will continuously monitor and make customers aware of potential security incidents.

The service will help customers implement best practices for the maintenance, monitoring, and analysis of audit logs as recommended by SANS and the Center for Internet Security (Critical Security Control #6).

The key benefits that SOCVue Security Monitoring delivers to customers are:

- Continuous monitoring of log and event data to detect potential security incidents
- Integrated network intrusion detection (IDS), file integrity monitoring (FIM), and threat intelligence feeds
- Timely investigation and notification about incidents that need attention
- Reporting on security events and alerts
- Assistance with compliance needs regarding FFIEC, PCI DSS, HIPAA, and other regulations
- Ongoing monitoring of the security monitoring application
- Monthly review with your Cygilant CA covering the customer's overall security posture and overall system health

Key Components of the Service:

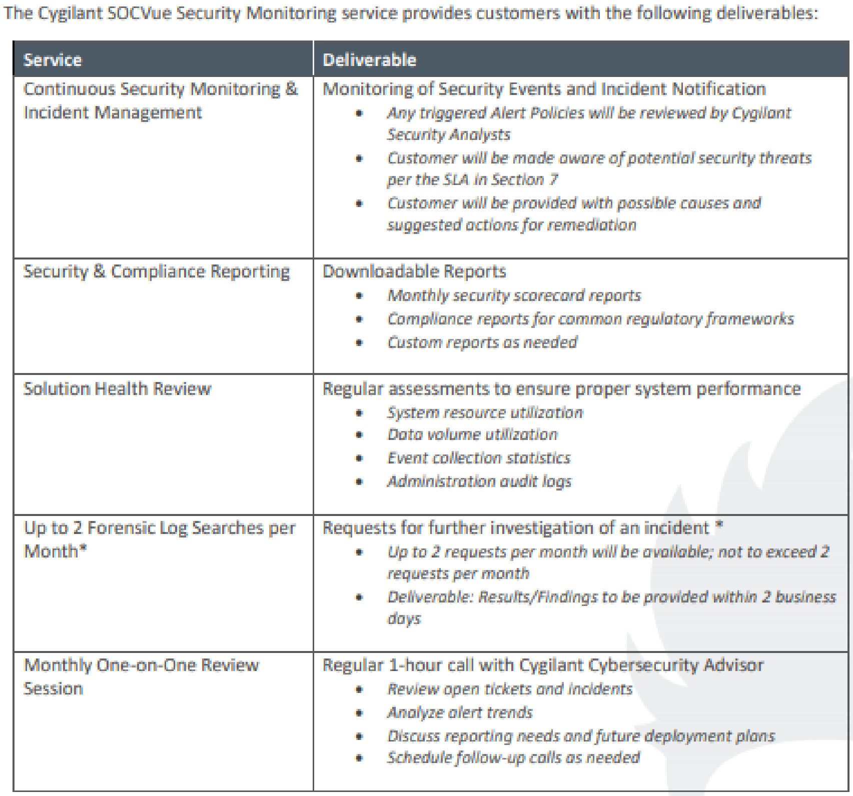
An effective security program is made up of People, Process, and Technology. Traditional security monitoring products have focused on the technology aspect without considering how to derive value from the solution. SOCVue Security Monitoring takes a more holistic approach, leading to more actionable intelligence and a proactive security posture.

1. **People**
   a. Cygilant Security Operations Center (SOC) – The Cygilant SOC is operational 24x7 and serves as an extension of the customer's own security and IT staff.
   b. Security and Product Expertise – The Cygilant SOC is staffed by information security experts and technicians who are experienced at deploying, managing, and optimizing security monitoring technologies.

   c. Continuous Monitoring – The SOC team provides around-the-clock coverage of the customer's security environment and will provide timely notification of any security incidents.

2. **Process**
   a. Audit Log Management – The Cygilant SOC helps implement formal process for the Maintenance, Monitoring and Analysis of Audit Logs as recommended by SANS/CIS Critical Security Control #6.
   b. Alert Policies – The SOC team will develop a set of correlation rules that will trigger an alert for suspicious activity or security violations, and they will continuously tune and update policies on an ongoing basis.
   c. Incident Response – The SOC team uses an integrated ticketing system to guide customers through the incident response process from detection to resolution.
3. **Technology**
   a. AlienVault USM – The solution collects, stores, and analyzes security event data from across the IT infrastructure. The solution is cloud-based but may include an on-premises sensor based on your needs.
   b. Managed Solution – Unlike traditional, complicated SIEM solutions, the AlienVault platform is installed, configured, and maintained by the Cygilant SOC team as part of the service.
   c. Cygilant SOCVue® Platform – Manage your incident response process with integrated dashboards, ticketing, and reporting through Cygilant's custom-built Security Operations and Analytics Platform.

Service Features:



The Cygilant SOCVue Security Monitoring service provides customers with the following deliverables:

Service	Deliverable
Continuous Security Monitoring & Incident Management	Monitoring of Security Events and Incident Notification • *Any triggered Alert Policies will be reviewed by Cygilant Security Analysts* • *Customer will be made aware of potential security threats per the SLA in Section 7* • *Customer will be provided with possible causes and suggested actions for remediation*
Security & Compliance Reporting	Downloadable Reports • *Monthly security scorecard reports* • *Compliance reports for common regulatory frameworks* • *Custom reports as needed*
Solution Health Review	Regular assessments to ensure proper system performance • *System resource utilization* • *Data volume utilization* • *Event collection statistics* • *Administration audit logs*
Up to 2 Forensic Log Searches per Month*	Requests for further investigation of an incident * • *Up to 2 requests per month will be available; not to exceed 2 requests per month* • *Deliverable: Results/Findings to be provided within 2 business days*
Monthly One-on-One Review Session	Regular 1-hour call with Cygilant Cybersecurity Advisor • *Review open tickets and incidents* • *Analyze alert trends* • *Discuss reporting needs and future deployment plans* • *Schedule follow-up calls as needed*

SOCVue Endpoint Management (SentinelOne EDR)

Overview:

Rooted in 20 years of experience and with hundreds of customers, Cygilant has developed a managed endpoint security service in partnership with SentinelOne that addresses the challenges of preventing, detecting, and responding to attacks – both known and unknown.

Key Benefits:

- Improved security posture – Take advantage of SentinelOne's patented AI algorithms to detect a wide array of threats, plus self-healing response capabilities that reverse malicious activity in real time.
- Dedicated cybersecurity team – Our team of cybersecurity experts work with you for efficient installation and system tuning. You get time back to focus on other priorities.
- Maximize ROI – Cygilant's affordable Cybersecurity-as-a-Service provides deployment guidance and regular health checks to ensure you are getting the most from your investment.

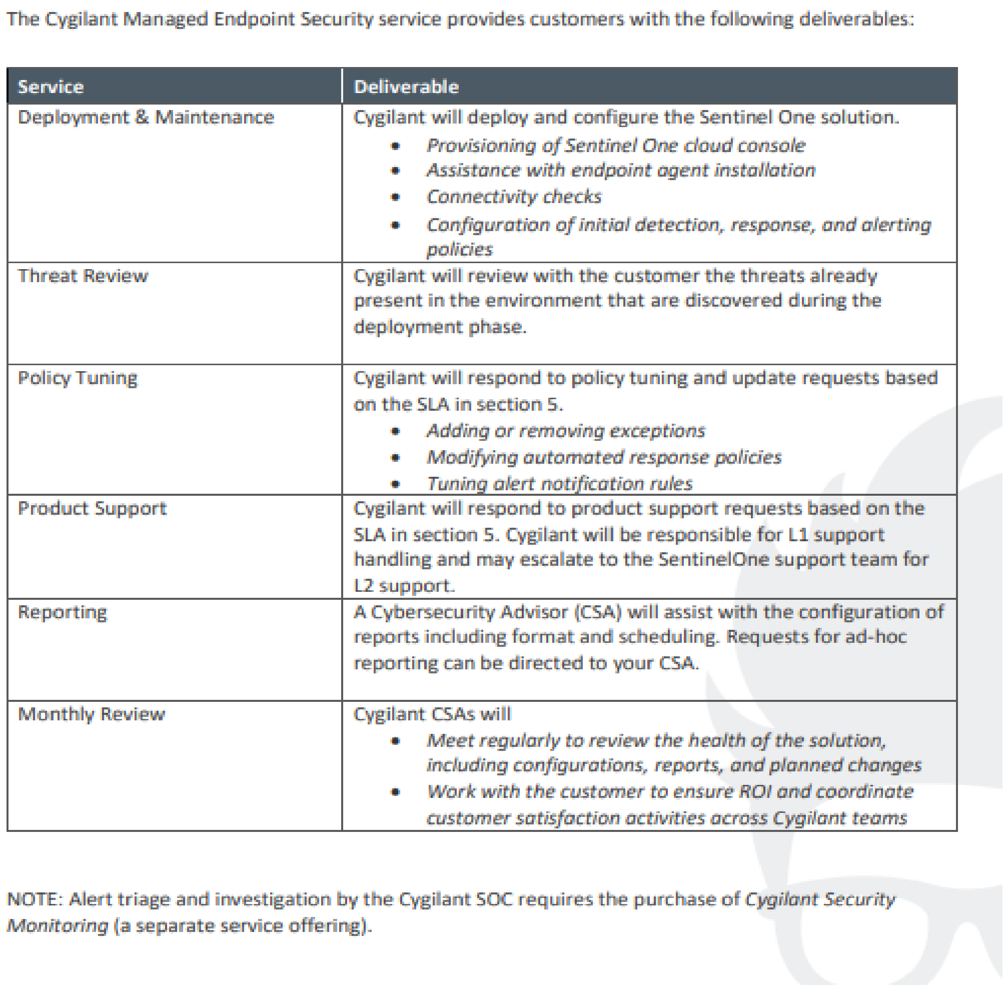
You can also add 24x7 security operations coverage for your SentinelOne alerts by adding the Cygilant Security Monitoring service to your subscription package.

The Security Monitoring service includes the following benefits:

- Cygilant SOCVue platform – Manage your incident response process with integrated dashboards, ticketing, and reporting through Cygilant's security operations platform.
- Managed SIEM – Best-of-breed AlienVault solution is installed, configured, and maintained by Cygilant Cybersecurity Advisors.
- Alerts – The SOC develops a set of correlation rules to trigger alerts for suspicious activity or security violations. Rules are fine-tuned, and policies updated to meet your needs.
- Audit log management – Cygilant helps implement the maintenance, monitoring and analysis of audit logs to help meet compliance requirements.
- Security and compliance reporting – Monthly security scorecard reports, scheduled event reports on a daily or weekly basis, automated compliance reports for common regulatory frameworks and custom reports as needed.

Combining log management and security information and event management (SIEM) technology with a 24/7 Security Operations Center (SOC), Cygilant helps you to proactively eliminate threats and meet compliance objectives

Service Features:



The Cygilant Managed Endpoint Security service provides customers with the following deliverables:

Service	Deliverable
Deployment & Maintenance	Cygilant will deploy and configure the Sentinel One solution. • *Provisioning of Sentinel One cloud console* • *Assistance with endpoint agent installation* • *Connectivity checks* • *Configuration of initial detection, response, and alerting policies*
Threat Review	Cygilant will review with the customer the threats already present in the environment that are discovered during the deployment phase.
Policy Tuning	Cygilant will respond to policy tuning and update requests based on the SLA in section 5. • *Adding or removing exceptions* • *Modifying automated response policies* • *Tuning alert notification rules*
Product Support	Cygilant will respond to product support requests based on the SLA in section 5. Cygilant will be responsible for L1 support handling and may escalate to the SentinelOne support team for L2 support.
Reporting	A Cybersecurity Advisor (CSA) will assist with the configuration of reports including format and scheduling. Requests for ad-hoc reporting can be directed to your CSA.
Monthly Review	Cygilant CSAs will • *Meet regularly to review the health of the solution, including configurations, reports, and planned changes* • *Work with the customer to ensure ROI and coordinate customer satisfaction activities across Cygilant teams*

NOTE: Alert triage and investigation by the Cygilant SOC requires the purchase of *Cygilant Security Monitoring* (a separate service offering).

SOCVue Unlimited Vulnerability Management (Qualys)

Overview:

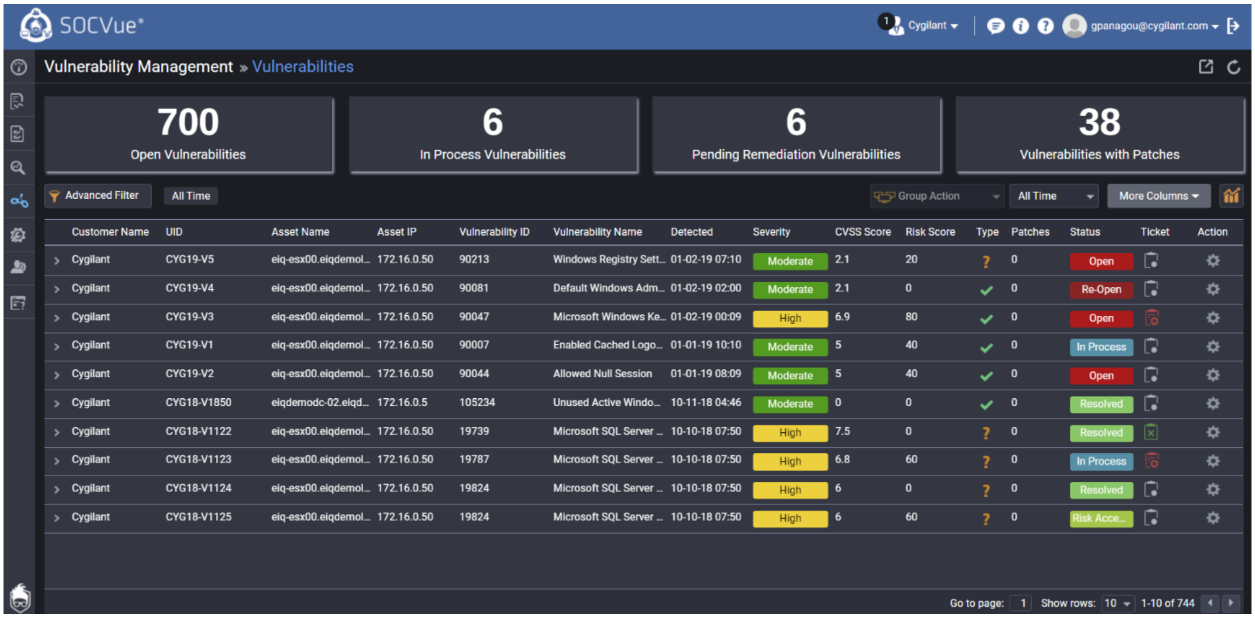
Software flaws or misconfigurations could allow cyber-attackers to gain access to IT systems. These vulnerabilities need to be quickly detected and remediated before they can be exploited.

Cygilant's SOCVue® Vulnerability Management is a subscription-based service that helps you quickly detect vulnerabilities and provides guidance for remediation. Because it is a managed service, Cygilant handles the deployment and configuration, schedules scans on your behalf, and assists with reporting.

The key benefits delivered by SOCVue Vulnerability Management Service are:

- Regular scanning of IT systems for vulnerabilities to reduce security risk
- Vulnerability reports that provide guidance for reducing your attack surface
- Executive reports to provide summary data for all stakeholders
- SOCVue interface for sorting, filtering, and adding tickets to vulnerabilities
- Monthly meeting with your Cygilant Cybersecurity Advisor to discuss scanning needs and review vulnerability trends

SOCVue Vulnerability Dashboard:



Vulnerability Management » Vulnerabilities

700 Open Vulnerabilities

6 In Process Vulnerabilities

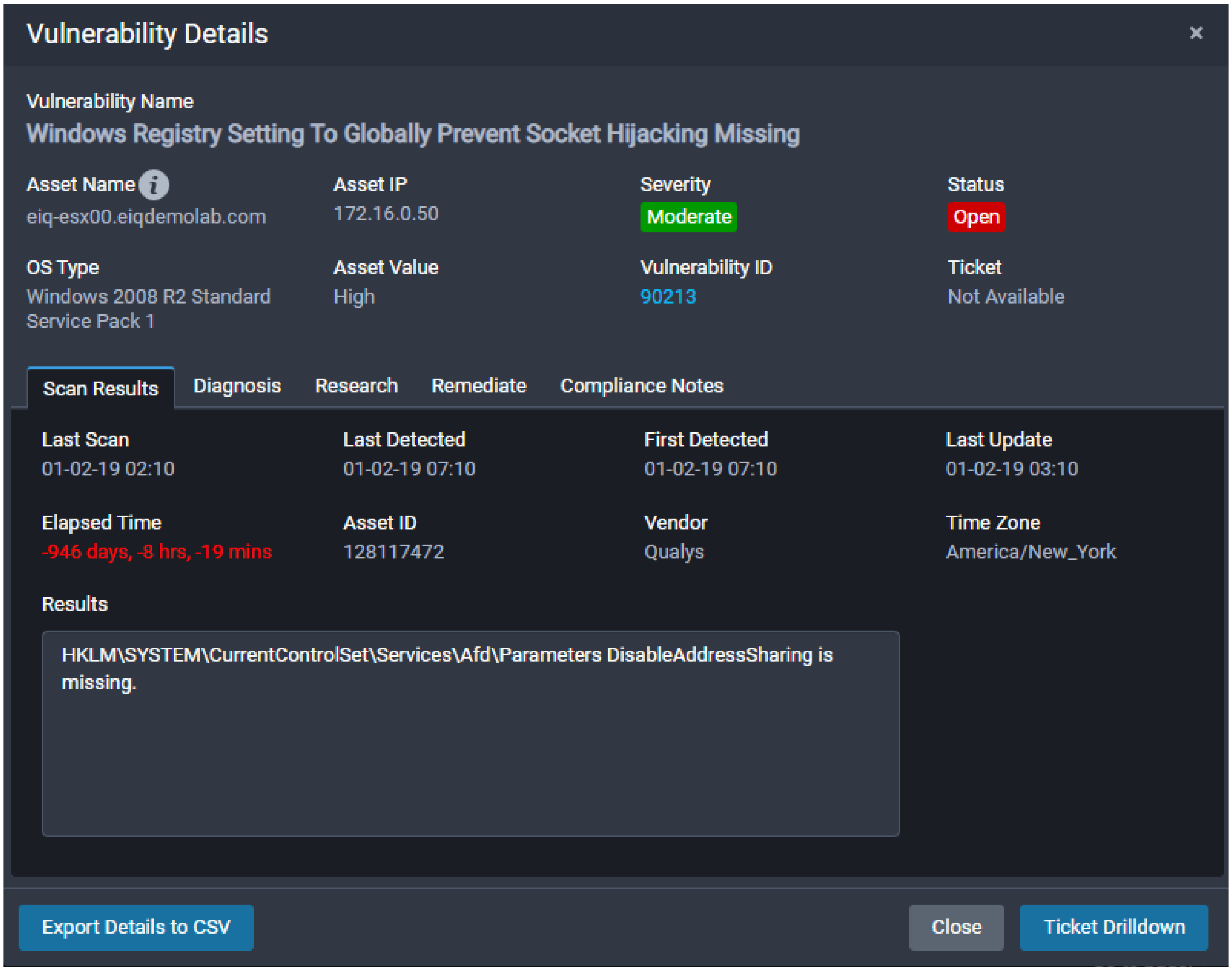
6 Pending Remediation Vulnerabilities

38 Vulnerabilities with Patches

Customer Name	UID	Asset Name	Asset IP	Vulnerability ID	Vulnerability Name	Detected	Severity	CVSS Score	Risk Score	Type	Patches	Status	Ticket	Action
Cygilant	CYG19-V5	eiq-esx00.eiqdemol...	172.16.0.50	90213	Windows Registry Sett...	01-02-19 07:10	Moderate	2.1	20	?	0	Open		⚙
Cygilant	CYG19-V4	eiq-esx00.eiqdemol...	172.16.0.50	90081	Default Windows Adm...	01-02-19 02:00	Moderate	2.1	0	✓	0	Re-Open		⚙
Cygilant	CYG19-V3	eiq-esx00.eiqdemol...	172.16.0.50	90047	Microsoft Windows Ke...	01-02-19 00:09	High	6.9	80	✓	0	Open		⚙
Cygilant	CYG19-V1	eiq-esx00.eiqdemol...	172.16.0.50	90007	Enabled Cached Logo...	01-01-19 10:10	Moderate	5	40	✓	0	In Process		⚙
Cygilant	CYG19-V2	eiq-esx00.eiqdemol...	172.16.0.50	90044	Allowed Null Session	01-01-19 08:09	Moderate	5	40	✓	0	Open		⚙
Cygilant	CYG18-V1850	eiqdemodc-02.eiqd...	172.16.0.5	105234	Unused Active Windo...	10-11-18 04:46	Moderate	0	0	✓	0	Resolved		⚙
Cygilant	CYG18-V1122	eiq-esx00.eiqdemol...	172.16.0.50	19739	Microsoft SQL Server ...	10-10-18 07:50	High	7.5	0	?	0	Resolved		⚙
Cygilant	CYG18-V1123	eiq-esx00.eiqdemol...	172.16.0.50	19787	Microsoft SQL Server ...	10-10-18 07:50	High	6.8	60	?	0	In Process		⚙
Cygilant	CYG18-V1124	eiq-esx00.eiqdemol...	172.16.0.50	19824	Microsoft SQL Server ...	10-10-18 07:50	High	6	0	?	0	Resolved		⚙
Cygilant	CYG18-V1125	eiq-esx00.eiqdemol...	172.16.0.50	19824	Microsoft SQL Server ...	10-10-18 07:50	High	6	60	?	0	Risk Acce...		⚙

Go to page: 1 Show rows: 10 1-10 of 744

Figure 1: SOCVue Vulnerability Dashboard



Vulnerability Details

Vulnerability Name
Windows Registry Setting To Globally Prevent Socket Hijacking Missing

Asset Name	Asset IP	Severity	Status
eiq-esx00.eiqdemolab.com	172.16.0.50	Moderate	Open

OS Type	Asset Value	Vulnerability ID	Ticket
Windows 2008 R2 Standard Service Pack 1	High	90213	Not Available

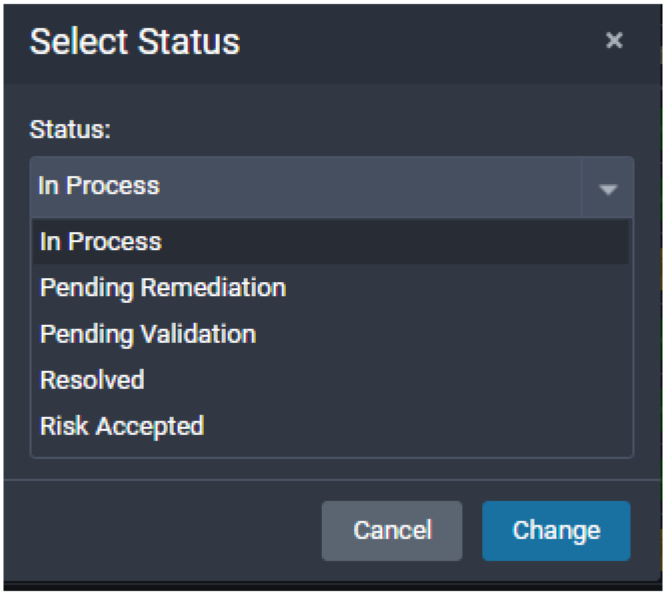
Last Scan	Last Detected	First Detected	Last Update
01-02-19 02:10	01-02-19 07:10	01-02-19 07:10	01-02-19 03:10

Elapsed Time	Asset ID	Vendor	Time Zone
-946 days, -8 hrs, -19 mins	128117472	Qualys	America/New_York

Results

HKLM\SYSTEM\CurrentControlSet\Services\Afd\Parameters DisableAddressSharing is missing.

Figure 2: SOCVue Vulnerability Details

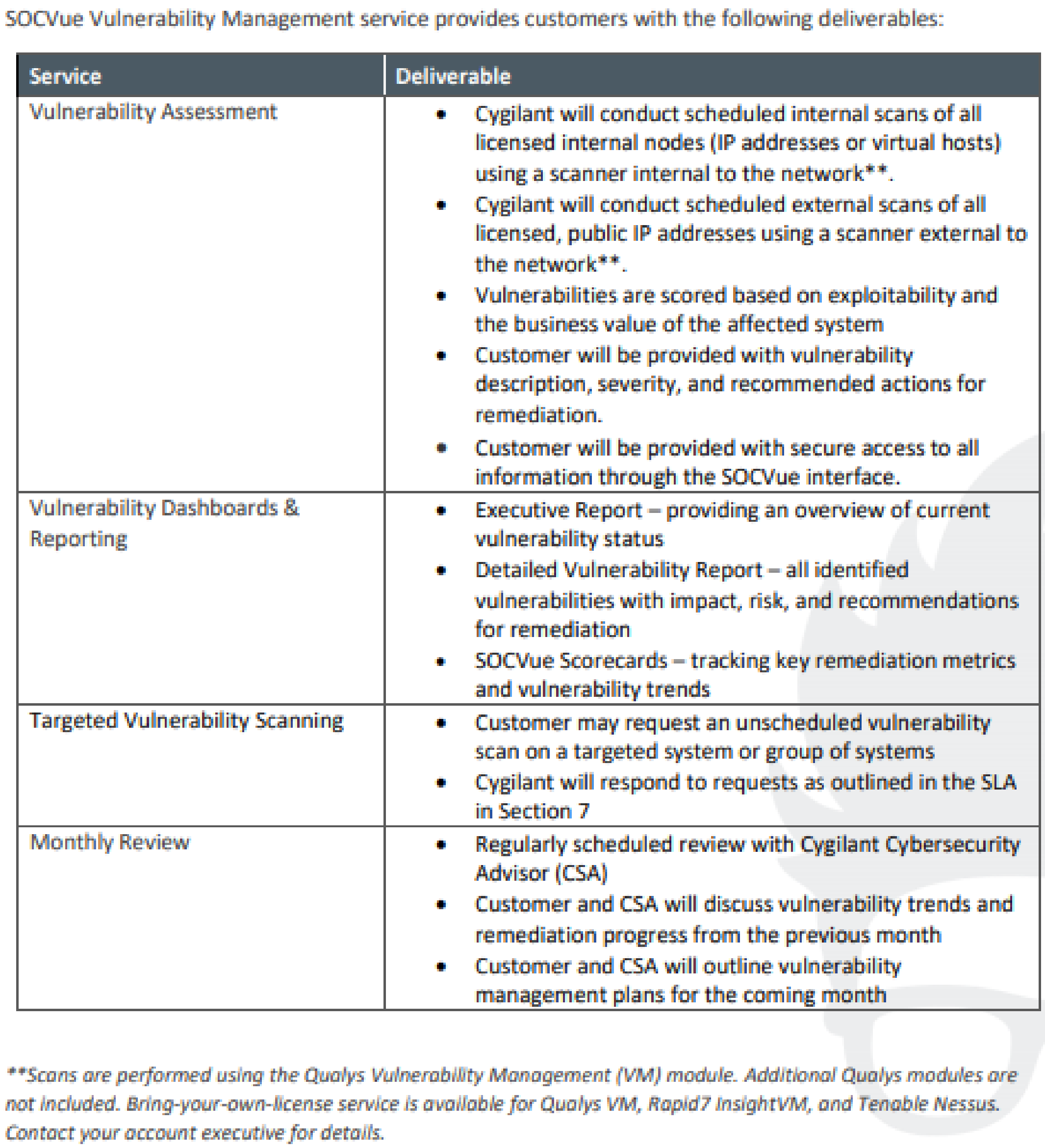


Select Status

Status: In Process

Figure 3: SOCVue Vulnerability Change Status Workflow

Service Features:



SOCVue Vulnerability Management service provides customers with the following deliverables:

Service	Deliverable
Vulnerability Assessment	- Cygilant will conduct scheduled internal scans of all licensed internal nodes (IP addresses or virtual hosts) using a scanner internal to the network**. - Cygilant will conduct scheduled external scans of all licensed, public IP addresses using a scanner external to the network**. - Vulnerabilities are scored based on exploitability and the business value of the affected system - Customer will be provided with vulnerability description, severity, and recommended actions for remediation. - Customer will be provided with secure access to all information through the SOCVue interface.
Vulnerability Dashboards & Reporting	- Executive Report – providing an overview of current vulnerability status - Detailed Vulnerability Report – all identified vulnerabilities with impact, risk, and recommendations for remediation - SOCVue Scorecards – tracking key remediation metrics and vulnerability trends
Targeted Vulnerability Scanning	- Customer may request an unscheduled vulnerability scan on a targeted system or group of systems - Cygilant will respond to requests as outlined in the SLA in Section 7
Monthly Review	- Regularly scheduled review with Cygilant Cybersecurity Advisor (CSA) - Customer and CSA will discuss vulnerability trends and remediation progress from the previous month - Customer and CSA will outline vulnerability management plans for the coming month

***Scans are performed using the Qualys Vulnerability Management (VM) module. Additional Qualys modules are not included. Bring-your-own-license service is available for Qualys VM, Rapid7 InsightVM, and Tenable Nessus. Contact your account executive for details.*

6. References

6.a Van Buren County Hospital (Keosauqua, IA)

Nate Mahon – IT Manager
nathan.mahon@vbch.org
(319) 293-3171

6.b Fitchburg State University (Fitchburg, MA)

Sherry Horeanopoulos – Information Security Officer
sah@fitchburgstate.edu
(978) 665-3000

6.c University Credit Union (Miami, FL)

Eric Hoskins – Chief Information Officer
ehoskins@ucumiami.org
(786) 425-5000

7. Additional Information

6.a Sample Monthly SOC Report:

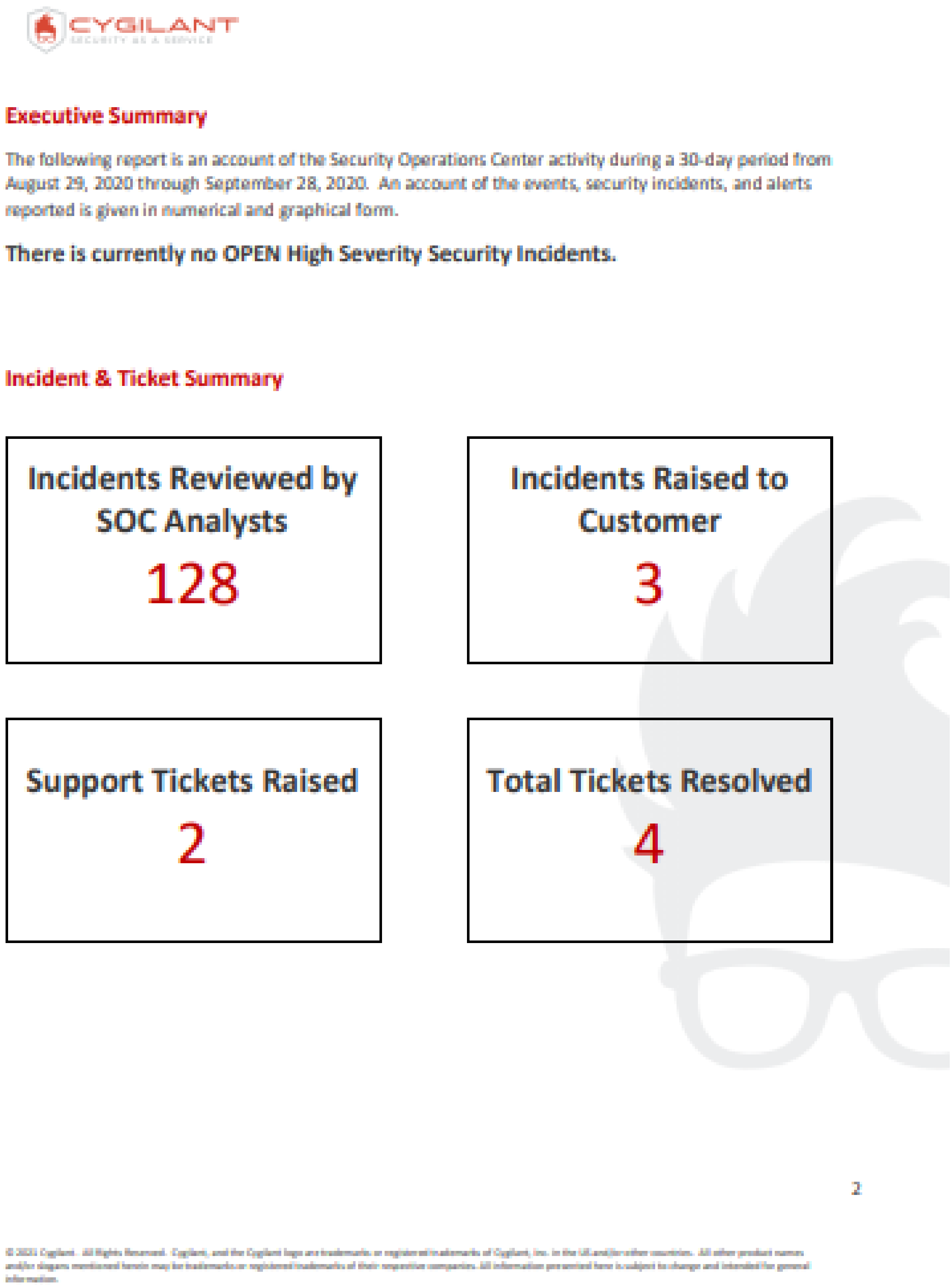
CYGILANT
SECURITY AS A SERVICE

Security Operations Report

August 29, 2020 to September 28, 2020

Summary Report

1



Executive Summary

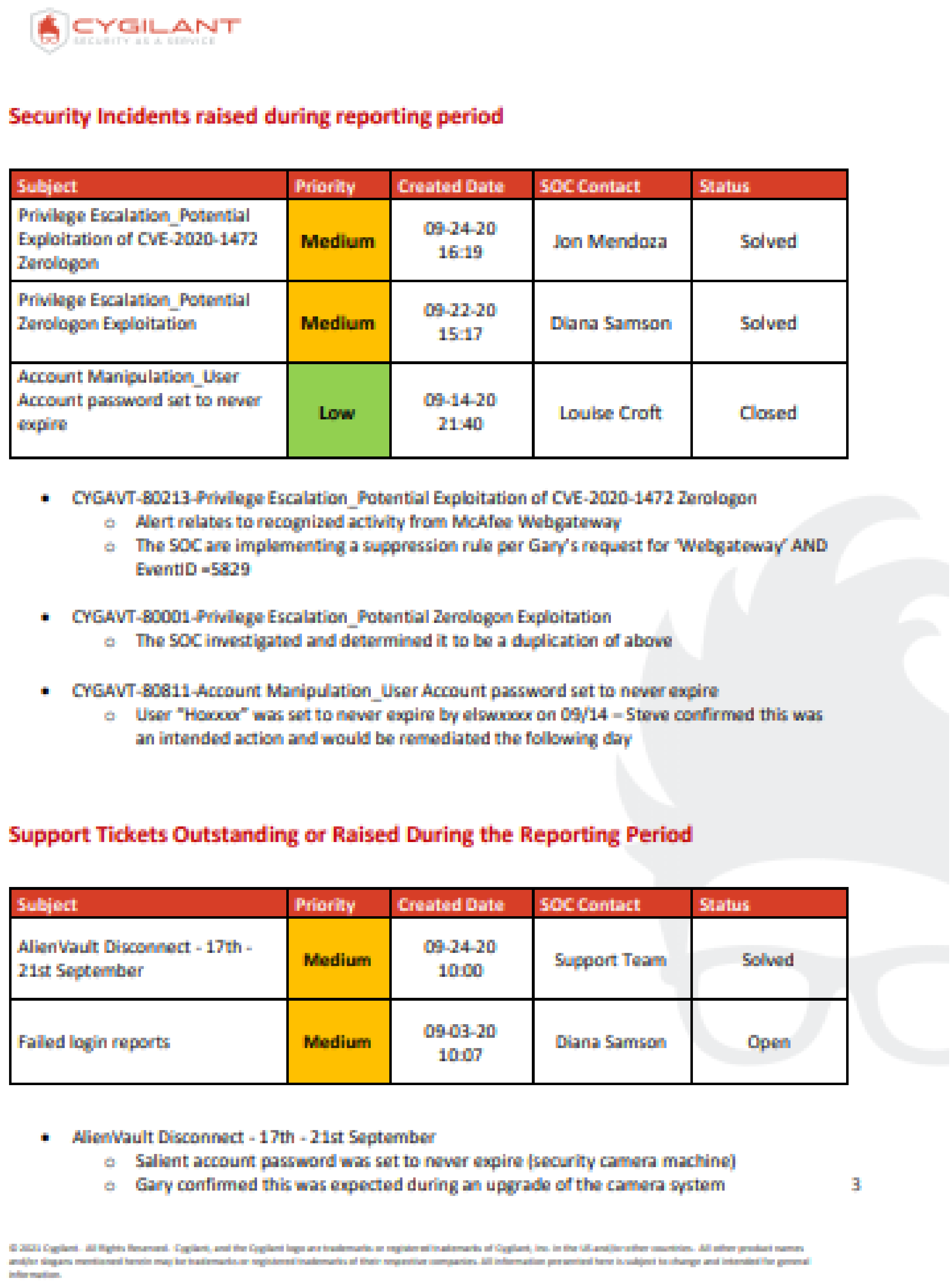
The following report is an account of the Security Operations Center activity during a 30-day period from August 29, 2020 through September 28, 2020. An account of the events, security incidents, and alerts reported is given in numerical and graphical form.

There is currently no OPEN High Severity Security Incidents.

Incident & Ticket Summary

Incidents Reviewed by SOC Analysts	Incidents Raised to Customer
128	3
Support Tickets Raised	**Total Tickets Resolved**
2	4

2



CYGILANT
SECURITY AS A SERVICE

Security Incidents raised during reporting period

Subject	Priority	Created Date	SOC Contact	Status
Privilege Escalation_Potential Exploitation of CVE-2020-1472 Zerologon	Medium	09-24-20 16:19	Jon Mendoza	Solved
Privilege Escalation_Potential Zerologon Exploitation	Medium	09-22-20 15:17	Diana Samson	Solved
Account Manipulation_User Account password set to never expire	Low	09-14-20 21:40	Louise Croft	Closed

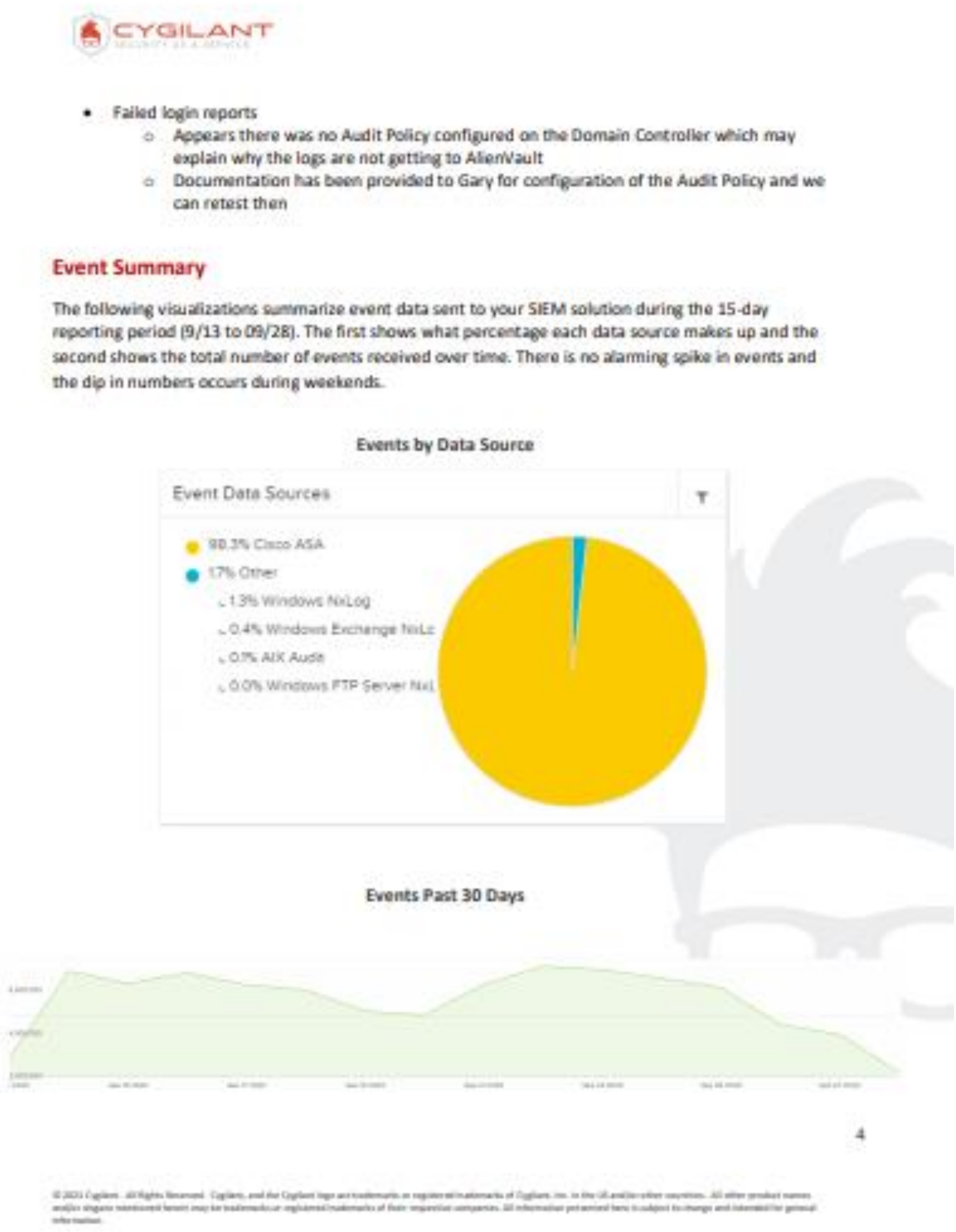
- CYGAVT-80213-Privilege Escalation_Potential Exploitation of CVE-2020-1472 Zerologon
  - Alert relates to recognized activity from McAfee Webgateway
  - The SOC are implementing a suppression rule per Gary's request for 'Webgateway' AND EventID =5829
- CYGAVT-80001-Privilege Escalation_Potential Zerologon Exploitation
  - The SOC investigated and determined it to be a duplication of above
- CYGAVT-80811-Account Manipulation_User Account password set to never expire
  - User "Hoxxxx" was set to never expire by elswxxxx on 09/14 – Steve confirmed this was an intended action and would be remediated the following day

Support Tickets Outstanding or Raised During the Reporting Period

Subject	Priority	Created Date	SOC Contact	Status
AlienVault Disconnect - 17th - 21st September	Medium	09-24-20 10:00	Support Team	Solved
Failed login reports	Medium	09-03-20 10:07	Diana Samson	Open

- AlienVault Disconnect - 17th - 21st September
  - Salient account password was set to never expire (security camera machine)
  - Gary confirmed this was expected during an upgrade of the camera system

3



- Failed login reports
    - Appears there was no Audit Policy configured on the Domain Controller which may explain why the logs are not getting to AlienVault
    - Documentation has been provided to Gary for configuration of the Audit Policy and we can retest then

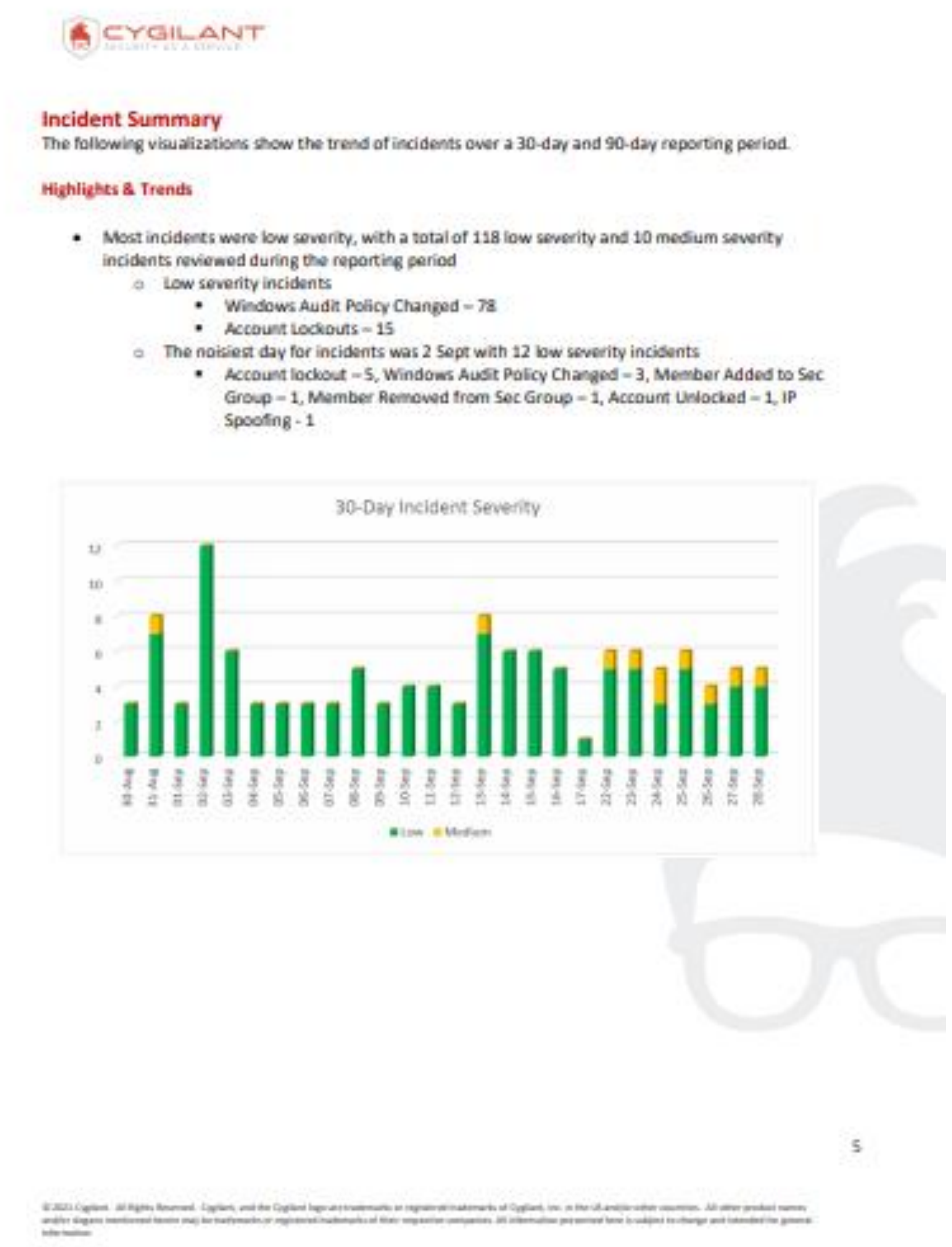
Event Summary

The following visualizations summarize event data sent to your SIEM solution during the 15-day reporting period (9/13 to 09/28). The first shows what percentage each data source makes up and the second shows the total number of events received over time. There is no alarming spike in events and the dip in numbers occurs during weekends.

Events by Data Source

Events Past 30 Days

4

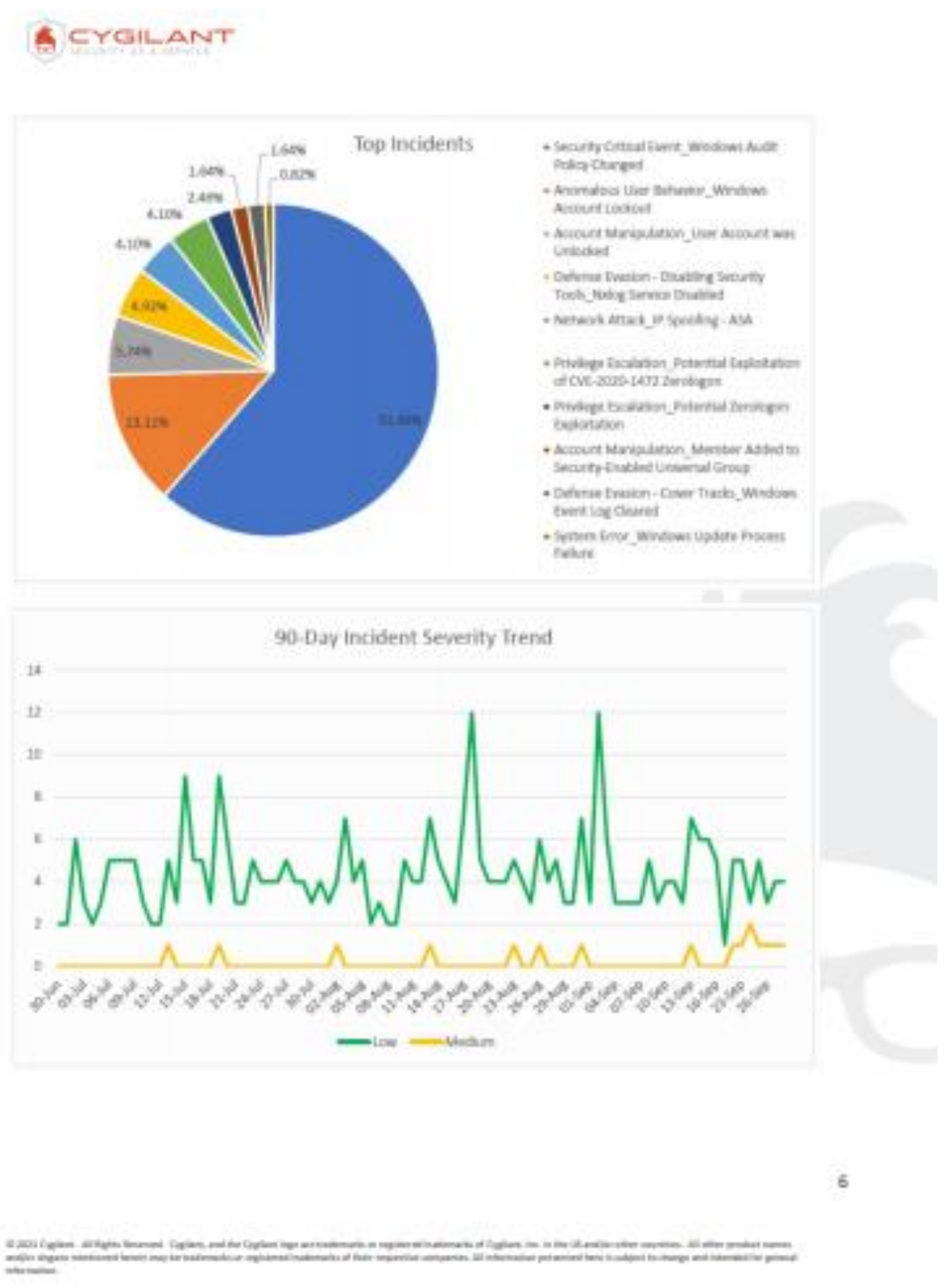


Incident Summary

The following visualizations show the trend of incidents over a 30-day and 90-day reporting period.

Highlights & Trends

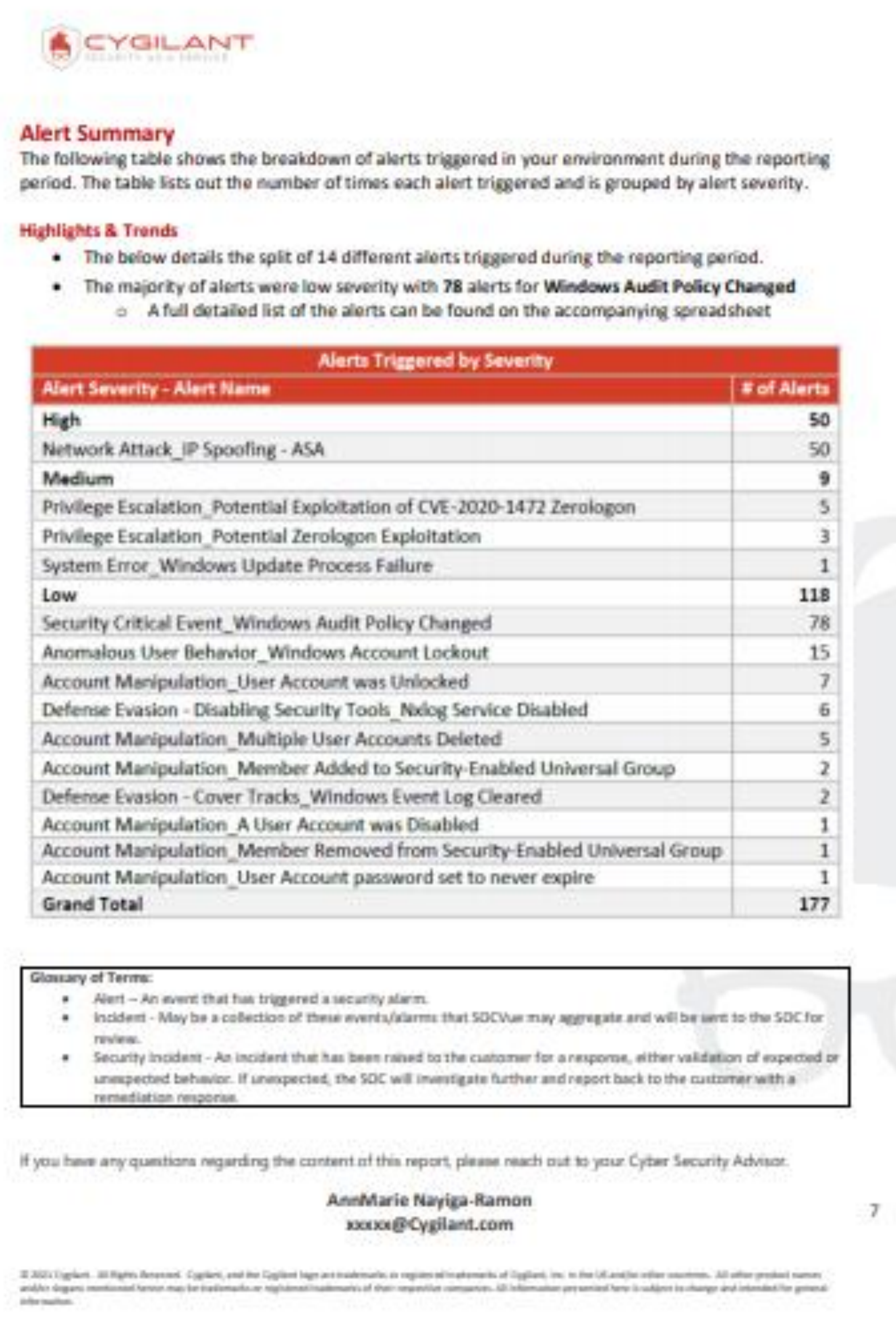
- Most incidents were low severity, with a total of 118 low severity and 10 medium severity incidents reviewed during the reporting period
  - Low severity incidents
    - Windows Audit Policy Changed – 78
    - Account Lockouts – 15
  - The noisiest day for incidents was 2 Sept with 12 low severity incidents
    - Account lockout – 5, Windows Audit Policy Changed – 3, Member Added to Sec Group – 1, Member Removed from Sec Group – 1, Account Unlocked – 1, IP Spoofing - 1



CYGILANT
SECURITY AS A SERVICE

- Security Critical Event_Windows Audit Policy Changed
- Anomalous User Behavior_Windows Account Lockout
- Account Manipulation_User Account was Unlocked
- Defense Evasion - Disabling Security Tools_Nxlog Service Disabled
- Network Attack_IP Spoofing - ASA
- Privilege Escalation_Potential Exploitation of CVE-2020-1472 Zerologon
- Privilege Escalation_Potential Zerologon Exploitation
- Account Manipulation_Member Added to Security-Enabled Universal Group
- Defense Evasion - Cover Tracks_Windows Event Log Cleared
- System Error_Windows Update Process Failure

6



Alert Summary

The following table shows the breakdown of alerts triggered in your environment during the reporting period. The table lists out the number of times each alert triggered and is grouped by alert severity.

Highlights & Trends

- The below details the split of 14 different alerts triggered during the reporting period.
- The majority of alerts were low severity with **78** alerts for **Windows Audit Policy Changed**
  - A full detailed list of the alerts can be found on the accompanying spreadsheet

Alerts Triggered by Severity	
Alert Severity - Alert Name	**# of Alerts**
High	**50**
Network Attack_IP Spoofing - ASA	50
Medium	**9**
Privilege Escalation_Potential Exploitation of CVE-2020-1472 Zerologon	5
Privilege Escalation_Potential Zerologon Exploitation	3
System Error_Windows Update Process Failure	1
Low	**118**
Security Critical Event_Windows Audit Policy Changed	78
Anomalous User Behavior_Windows Account Lockout	15
Account Manipulation_User Account was Unlocked	7
Defense Evasion - Disabling Security Tools_Nxlog Service Disabled	6
Account Manipulation_Multiple User Accounts Deleted	5
Account Manipulation_Member Added to Security-Enabled Universal Group	2
Defense Evasion - Cover Tracks_Windows Event Log Cleared	2
Account Manipulation_A User Account was Disabled	1
Account Manipulation_Member Removed from Security-Enabled Universal Group	1
Account Manipulation_User Account password set to never expire	1
Grand Total	**177**

Glossary of Terms:

- Alert – An event that has triggered a security alarm.
- Incident - May be a collection of these events/alarms that SOCVue may aggregate and will be sent to the SOC for review.
- Security Incident - An incident that has been raised to the customer for a response, either validation of expected or unexpected behavior. If unexpected, the SOC will investigate further and report back to the customer with a remediation response.

If you have any questions regarding the content of this report, please reach out to your Cyber Security Advisor.

AnnMarie Nayiga-Ramon
xxxxx@Cygilant.com

7