



SOC-as-a-Service: All the Benefits of a Security Operations Center Without the High Costs of a DIY Solution

Arctic Wolf Networks CyberSOC Review



A SANS Service Review

Written by Sonny Sarai

March 2017

*Sponsored by
Arctic Wolf*

Introduction

Malicious actors know midsize companies are high-value targets, rife with credit card data, personally identifiable information, and sensitive health information, among other data types that can be monetized.

To protect themselves from today's cyber threats, most enterprises implement a security operations center (SOC) with trained staff and expensive technology—and all the constant training and upgrading that go with it. But SOC's are harder to support for midsize organizations. Because most midsize companies lack the protections that large enterprises have, they are often targeted as lower hanging fruit.¹ Once inside, attackers can remain hidden for a longer period because these organizations lack the technology and skills to detect and respond to threats in a timely fashion.

Cyber security and risk are a top concern for midsize organizations, according to a recent Deloitte survey, which found 61 percent of respondents cited implementation of new security processes as the most important focus of their IT security spending.² Midsize organizations face a challenge in that they have many of the same security issues as a large enterprise but lack the budget and expertise to address them. Traditional MSSP services are good for managing infrastructure, but they fall short when it comes to advanced threat detection and providing greater visibility into the environment. One means of accomplishing this is through an affordable, easy-to-install SOC-as-a-service, such as Arctic Wolf's SOC service.

In this paper, we reviewed Arctic Wolf's services from a customer's point of view and found that its CyberSOC (SOC-as-a-service) offering provided visibility into events we launched in our mock midsize enterprise, caught and helped us repair vulnerabilities we purposely left in the environment for review, and provided accurate reporting throughout the review. Most important, we were also afforded access, as needed, to a live engineer to send reports and help troubleshoot investigations. All of this worked seamlessly—without the high costs of implementation, configuration and tuning. The results of our review, including mock use cases, follow.

¹ "Huge rise in hack attacks as cyber-criminals target small businesses," www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses

² "Technology in the mid-market—Taking ownership," <https://www2.deloitte.com/us/en/pages/deloitte-growth-enterprise-services/articles/technology-trends-middle-market-companies-survey.html>



Getting Started

In the review, we concentrated on the following areas:

- Ease of deployment
- Mean time to detect
- Customization
- Customer portal
- Cost vs. benefits

Lab Environment

Our lab environment simulated a scaled-down series of systems representing a typical midsize infrastructure. We ran a Juniper NS5GT, recognizing it is an older firewall but knowing the make and model had no applicability to this service review. The firewall needed only the capability to send logs to Arctic Wolf. The firewall consisted of a DMZ and internal interface.

Systems in the lab were configured as follows:

Internal Zone

- Two Windows 2008 R2 Active Directory servers
- Two Windows 7 domain members
- Windows 2003 file server
- Centos 7 server running Squid proxy
- Wi-Fi network attached to the internal zone

DMZ

- Windows 2008 R2 server running IIS
- CentOS 7 system running Apache web server

All servers and workstations were running on an ESXi 6.0 hypervisor.



Live Engineer

Once enrolled, we received an email from Arctic Wolf with a link to create an account on its portal. The email was from our own dedicated Concierge Security Engineer (CSE) with whom we would work for all Arctic Wolf-related issues.

Our CSE sent us a questionnaire to be filled out and sent back to Arctic Wolf. This provided the information to preconfigure the sensors prior to shipment. We provided primary and secondary contact information, network/IP information, log sources, customization information and prerequisite instructions. After our Arctic Wolf CSE reviewed it, we had a kickoff/technical meeting with him to go over the on-boarding process and escalation procedures and discuss the on-boarding document.

Setup Documentation

Arctic Wolf also gave us access to a setup document. This provided information on how to configure logging on our Active Directory servers, with an option to configure it manually or automatically.

We selected the automated configuration. The document provided screenshots on how to correctly configure auditing through Group Policy. After that was configured, we executed a PowerShell script written by Arctic Wolf, which created the service account Arctic Wolf uses to communicate with Active Directory, and configured it to send logs to the sensor, all of which took less than 10 minutes. Our remaining systems were configured to send Windows Event Log or Linux/network logs via syslog to the sensor.

Sensor Installation

Our environment required two sensors: one for the DMZ and one for the internal network. The sensors act as flow creators and aggregators, intrusion detection systems and syslog targets. It is a black box, so we did not have the capability to access it. We just cabled it.



Getting Started (CONTINUED)

There are multiple ways to set up the sensor in an environment like ours. One option is to configure it in-line with your firewall so all traffic passes through it. The second option is to configure port mirroring. We chose to configure it in-line in our lab (see Figure 1).³

Other than the sensor, there is nothing else to install for the service from a network traffic perspective. The sensor collects the packet data and analyzes flows. This data is captured, compressed, encrypted and sent to the AWN Cloud.

There is very little to install or configure when sending syslog data to the sensor. Most network devices come with out-of-the box capabilities to send logs to the sensor, and most, if not all, Linux systems come with some form of syslog installed. This allows you to easily configure the system to send log data to the sensor.

Windows systems can be slightly more involved. We decided to install an agent and configure the agent to convert the binary event logs to syslog format and send the logs to the sensor. The install and configuration of the agent took less than 10 minutes.

The setup took very little time. We connected the sensor into our network, and Arctic Wolf confirmed it was seeing traffic within minutes. It immediately began collecting our events after we connected the sensor in our environment. Arctic Wolf refers to each log or packet entry as an observation. An observation can be any event received as a packet or log.

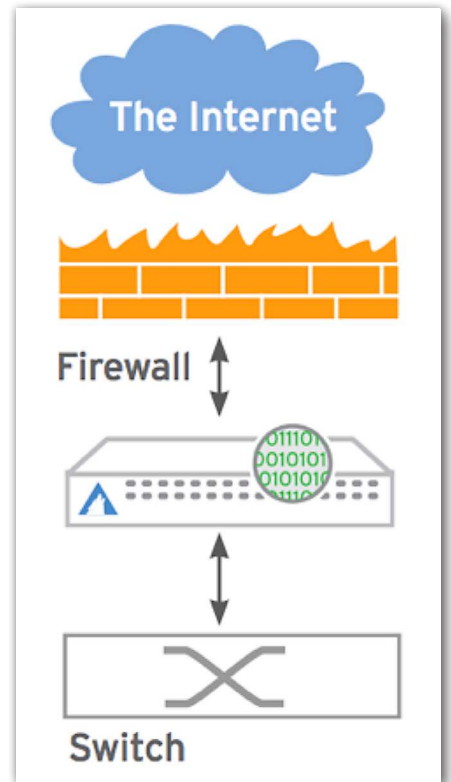


Figure 1.
Arctic Wolf Simplified Network Map

³ "Arctic Wolf AWN100 Sensor: Inline Installation Guide," https://welcome.arcticwolf.com/setup/PDF/AWN100_Inline.pdf



AWN Service Architecture

AWN's robust service architecture is designed with flexibility and scalability in mind. This allows AWN to ingest log and flow data in near real time, correlate data from multiple sources, and provide customers with actionable information about threats. Some of the most prominent components of AWN's service architecture include:

- **Cloud-Based Architecture.** AWN CyberSOC is a distributed, cloud-based SOC delivered through a subscription service. An AWN sensor sits in your network where you would send all your machine data, which is then uploaded to AWN's SOC to analyze—usually within seconds after it is generated. The deployment is as simple as racking the preconfigured sensor in your network, and threat monitoring begins.
- **SOC-as-a-Service.** AWN CyberSOC combines human and machine intelligence to analyze millions of events in real time for 24/7 threat detection. The machine learning, threat intelligence feeds and big data security analytics tools collect and correlate security events from all infrastructure, security devices and applications before delivering events to your designated CSE to review and respond to in seconds. If a threat is detected, the CSE notifies you with details, forensic analysis and recommended remediation for incident response. This not only helps protect your organization from a data breach, but also saves valuable time for your IT and security teams.
- **Storage and Retention.** The CyberSOC is built on Amazon cloud, so it can scale up and out easily. This enables the solution to have built-in storage. By default the security events are stored for 90 days, but for a marginal additional fee you can store logs for one to five years. The subscription fee is not based on log volume or speed, and you can store any volume of events that IT creates without the hassle of additional storage or an analytics platform.
- **Purpose-Built Technology.** The distributed cloud SOC is built and maintained on a proprietary technology that helps Arctic Wolf maintain custom capabilities and independence from any specific toolset. A large team of security experts continuously updates the platform, making it easy for the CSE to deliver services easily.
- **Customer Rule Engine (CRule).** Each customer is different and needs some level of customization to ensure Arctic Wolf monitors what is important.

For instance, if there were a phishing attack on one of our users, we would want to automate to detect and isolate similar attacks on all users. Or we might need to prevent “whale watching,” which requires closely monitoring high-value users 24/7 for any suspicious activities. This could easily be done by calling our CSE, who could take care of our customization needs in a day or two. The same is true for our security information and event management (SIEM), which would take us hours of coding, customization and testing, and may break many other things.



Utilizing the SOC

Arctic Wolf's SOC-as-a-service provided us a strong customer portal, easy customization features and, most important, a live human to help diagnose problems and detect threats.

Concierge Security Engineer

Arctic Wolf's philosophy is for the CSE to be an extension of the customer's IT or information security team. Everything is done through the CSE, from customizing alerts to personalizing how the customer is notified of security incidents. Customers do not have to learn how to use a new product or configure any type of application, which provides tremendous value for midsize companies that either do not have dedicated security personnel or have IT staff who are already stretched.

There are many benefits to having a dedicated CSE:

1. Our CSE, over time, gained a deeper understanding of our environment and made more informed security recommendations for our environment.
2. The CSE was our single point of contact at Arctic Wolf, so we always knew who we would be working with.
3. He knew how to work with our existing technologies and understood the decisions we made on our technology choices without us having to re-explain this to a new CSE.
4. During a security incident, we leveraged the CSE's experience in dealing with similar incidents to help us with our own investigation.
5. Because we had established a working relationship with the CSE, investigating with him was like working with someone on our own IT team.

The CSE holds a regular meeting with the customer and reviews an executive summary report (which provides the overall security posture of the customer), results of a monthly external vulnerability scan and a general security review.



Utilizing the SOC (CONTINUED)

For example, the CSE's report includes the number of events (observations) ingested by the sensor (for this sample, it was 3 million), total number of investigations (1,618), and total number of reported incidents that were brought to the customer's attention (12), as illustrated in Figure 2.



Figure 2. Arctic Wolf Executive Summary

As seen in Figure 2, the biggest benefit our CSE provided was reducing false positives by vetting events to find meaningful and actionable security events, and applying context and recommended actions so we knew what to do with the incident.

Ranking Assets

We then set out to identify the critical assets in our lab in order to monitor and scrutinize their logs for anomalous behavior. For example, some assets may have a PCI or HIPAA network segment with compliance rules that must be adhered to, so these systems would be more heavily monitored and have additional alerting compared with other areas of the network. Our CSE customized all the alerts for us, and he was flexible about configuring the service to work within our operational processes.



Arctic Wolf can look at login events over time and help build a baseline of normal login patterns, review login activity and alert on any logins outside of these “normal” hours. The same principles can be applied when monitoring any other type of account activity.

Ranking Severity

Our CSE also customized incident handling based on severity of threats for what we needed. We identified what constituted a severity one alert and then a severity two (for the purposes of our evaluation, we limited our severity levels to only a severity one and severity two).

With our CSE’s assistance, we were able to rate threats and vulnerabilities against these severity levels; the CSE then configured the requirements for us. For example, we ranked ransomware detection; inbound firewall rules allowing RDP, SQL or the SMB protocol; and any type of Metasploit traffic outbound as a high severity (one) event level, requiring an immediate phone call from our CSE and an email sent to a designated email address describing the incident and next steps. Incidents are generated into a ticket system on the customer premises for tracking purposes.

We then included connections to known bad IP addresses, odd-looking DNS requests and critical systems accessing the Internet as severity two level. This would generate an email similar to the information provided in a severity one incident but no phone call.

Ranking Alerts

The last piece of customization our CSE did for us was applying alerts on specific user accounts. We monitored accounts with administrative privileges such as domain admins and user accounts tied to senior staff such as the executive team within our lab domain.

An example of an alert we put in place is if a domain admin account logs in after business hours, such as at 2 a.m. With its history of collected login events over time, Arctic Wolf helped build a baseline of what is normal. We then reviewed login activity to alert on any logins outside of these “normal” hours.

The same principles can be applied when monitoring any other type of account activity: Create a baseline by analyzing what is normal behavior for a period, and then build alerts on events of interest outside of regular behavior.



Customer Portal

We logged into the portal using a web browser over HTTPS. (We had already configured access to the portal, in accordance with the initial instructions we received from Arctic Wolf.)

The default page provides a dashboard including a high-level status of our environment, from which we could quickly assess the security health of our environment through the lens of Arctic Wolf. See Figure 3.

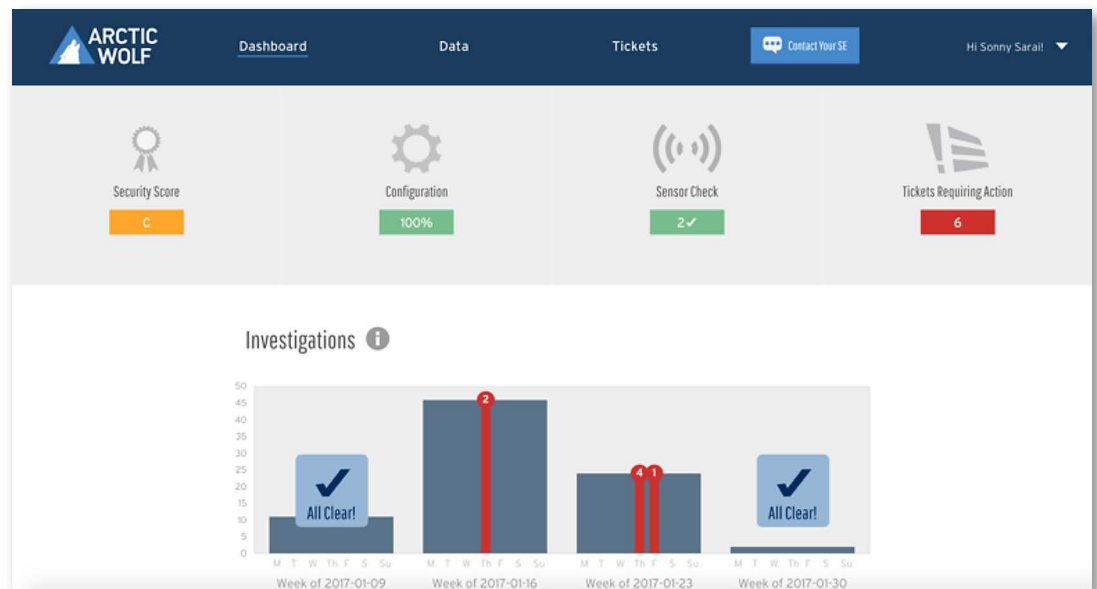


Figure 3. Arctic Wolf Portal Dashboard

The portal provides a dashboard of icons to view what is occurring inside your network, as well as visibility into what the CSE is working on for your network. The portal is well laid out and does not bog the customer down with overly technical information or clutter, providing enough information to either investigate something yourself or consult the CSE to discuss further.



Security Score

As seen in Figure 3, our Security Score was graded at a C—not very good. Our CSE used a few different criteria when determining the security score:

- Cleanliness of the customer environment
- Configuration of the customer environment
- Responsive to tickets

In our case, we received the low grade because we did not want to close most of our tickets. This is by design, as we will be discussing in the next section.

Configuration

The Configuration rating identifies what devices are currently logging to Arctic Wolf and what devices are not. When you hover over the Configuration icon, you are presented with an opportunity to View Breakdown. This shows what logs are configured correctly to send logs to Arctic Wolf. It is here where you can determine if there are other security-related log types you should be sending, so Arctic Wolf has a better picture of what is occurring in your environment (see Figure 4).

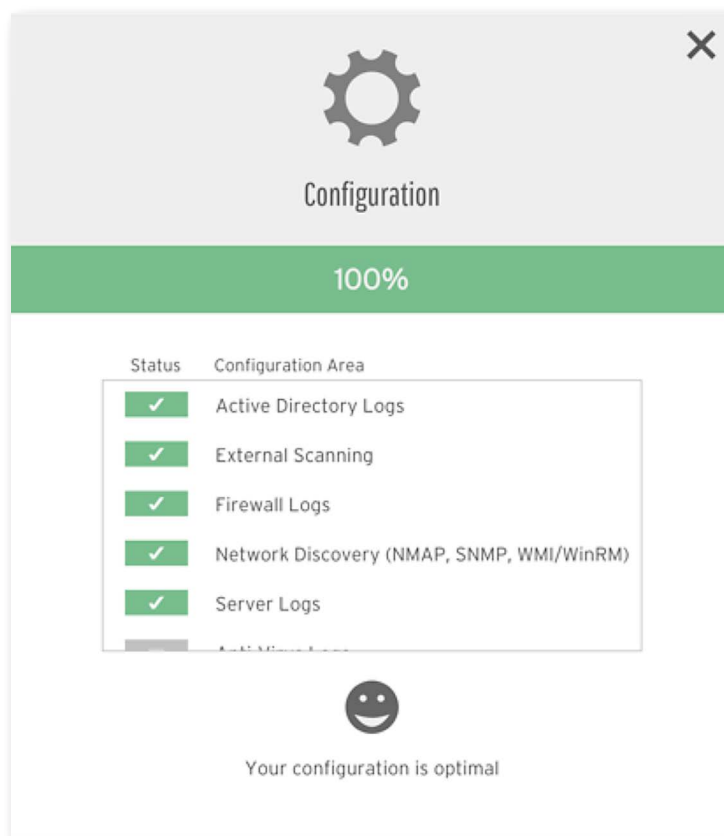


Figure 4. Arctic Wolf Portal Configuration Summary



Sensor Check

The Sensor Check section told us the health of the sensors as well as the traffic flowing through the sensors. This not only indicates if the sensors are working correctly, but you can also determine a baseline of normal traffic to compare against when you are investigating anomalous traffic (see Figure 5). Note, that if the sensor goes offline you will be notified by Arctic Wolf to get it back up; it is not your responsibility to alert when issues arise.

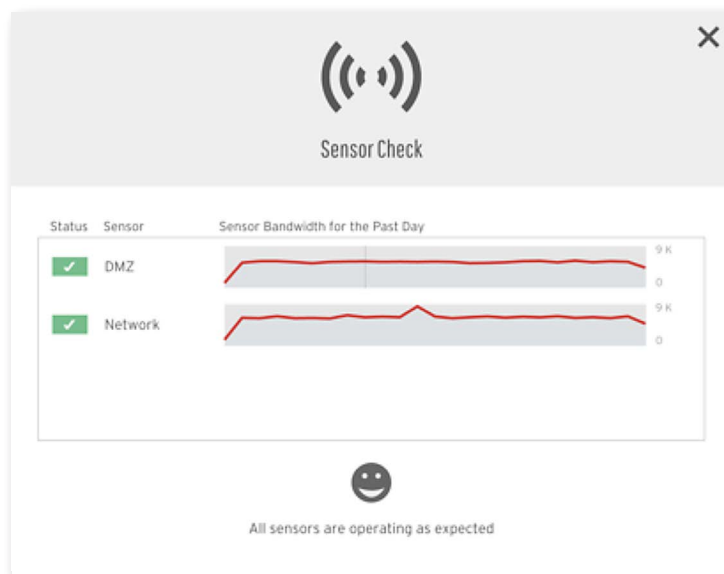


Figure 5. Sensor Check

Tickets & Data Tab

We managed our open tickets in the Tickets window. It showed us a list of all the tickets requiring action.

The information in the Data Tab contains a summarization of log data to aid in the investigation. It is a starting point to pivot from and filter on. Examples include:

- Devices on the network
- Protocols used
- Categories (e.g., hacking)
- Location of the traffic (both source and destination)

After going through all this setup and reviewing it with our security engineer, we jumped right into testing various mock scenarios with real-world applicability. For all the scenarios we tested, there were incidents that were identified with a specific call to action for the customer. This demonstrates that incident monitoring, detection and response occurs in real time. The results of these tests are covered in the next section.



SOC in Action

To test the value of using SOC-as-a-service for incident response, we used the summary information on the portal to launch investigations into two incident response scenarios: a web server attack and illicit user behavior.

Scenario 1: Identify Source of Attacks Against Our Web Server

In our mock environment, we set up a website that sits in our DMZ. This site is accessible over the Internet. We wanted to simulate real-world threats against a customer's website with an Internet presence. An example would be a customer's e-commerce website that generates income.

How do we leverage Arctic Wolf to help identify any attacks against our website and subsequently assist with defense strategies? We started our investigation on the portal.

We filtered on inbound traffic, and sensor view was set to "All Sensors." From there, we were able to quickly determine the amount of traffic coming inbound to our web server. See Figure 6.

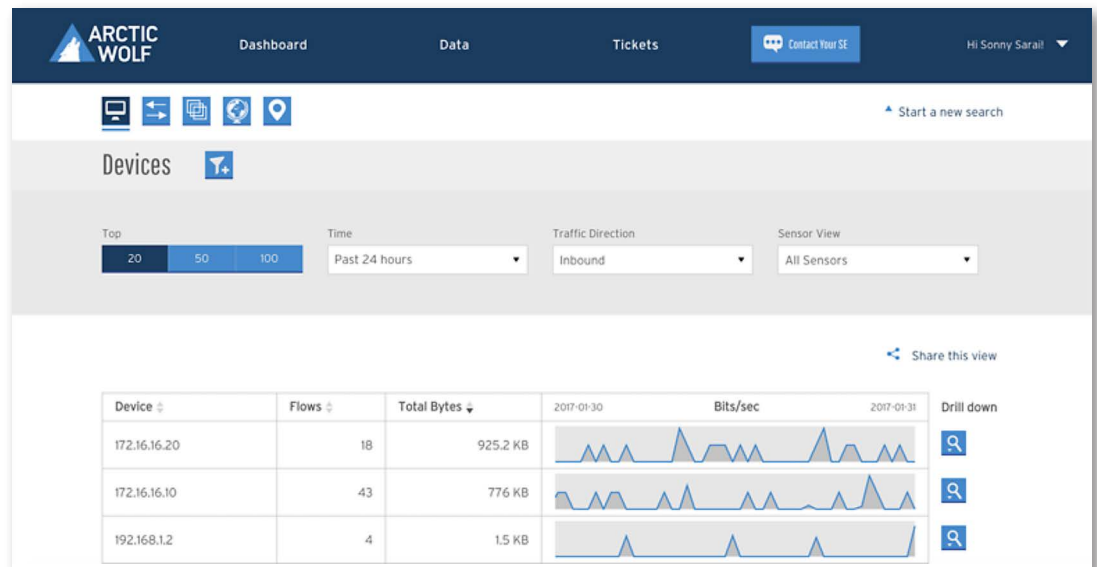


Figure 6. Arctic Wolf Portal: Inbound Traffic to DMZ



SOC in Action (CONTINUED)

The portal allowed us to dig even further and identify where the traffic originated. In a situation where a customer's web servers are getting attacked, it helps to quickly identify source IP addresses and even source countries. This can assist in a customer's implementation of geo-IP blocking at the firewall level. In our case, we were receiving web-related attack attempts originating predominantly from Russia, China and the United States. Most attempts were from known malicious IP addresses. See Figure 7.

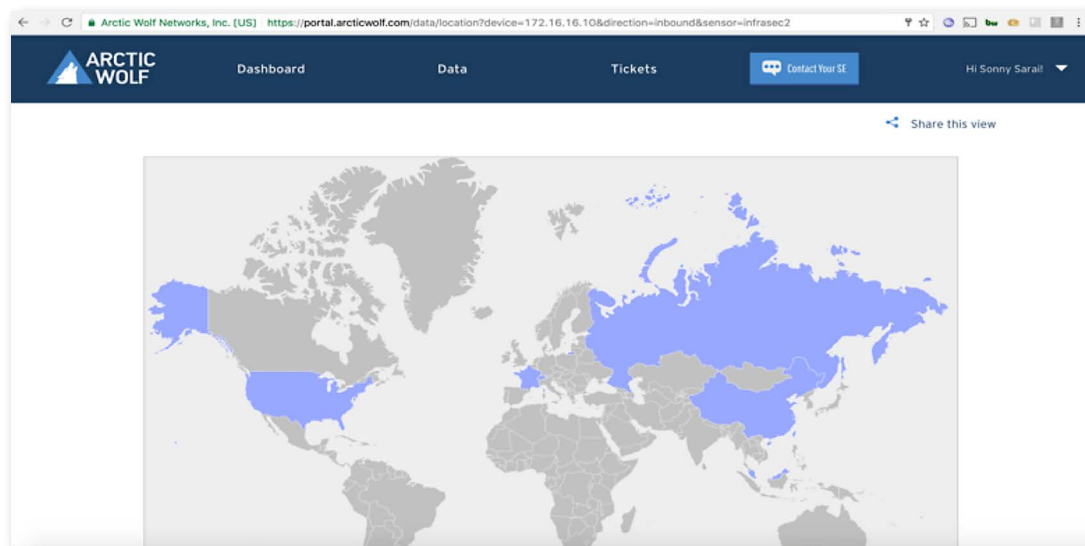


Figure 7. Arctic Wolf Portal: Geolocation

We concluded these connections from China, Russia and the United States were bots attempting web attacks against our site. We came to that conclusion by looking at the web requests in our server access logs.

A customer can leverage this information on the portal if its site starts experiencing performance degradation. These bots are notorious for sending thousands of requests per second, potentially causing a website to slow to a crawl. By using the portal to see if there is malicious traffic coming from a specific country, that information can be used to configure geo-IP blocking on the offending country or create a whitelist of only approved countries.

The information needed to understand attacks on our web server was easy to get to and clearly presented so that the right assessments could be made quickly. This helped us make a more informed decision on how to defend against these attacks. The customer portal interface is intuitive and easy to navigate, so no user training was required. Companies that have less experienced staff could just contact their CSE, who would do the same analysis for them and provide clear recommendations about how to protect themselves from these attacks.



Scenario 2: Investigate Unusual Surfing Habits in the Workplace

We wanted to use the portal to determine if anyone was browsing “suspicious” sites, so in the portal, we clicked on **Data>Categories**, and selected **Interesting**. See Figure 8.

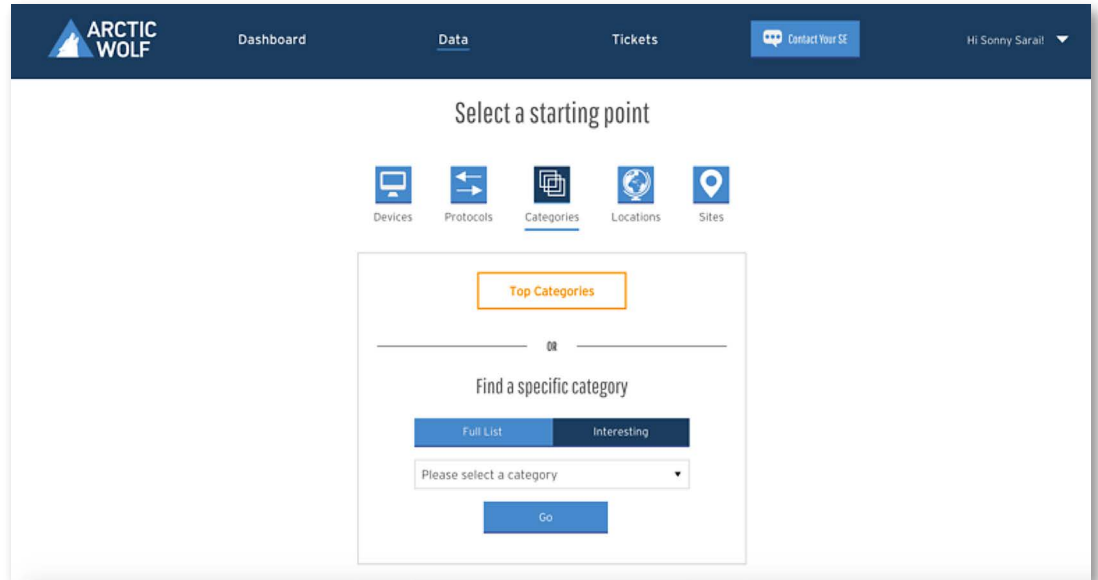


Figure 8. Arctic Wolf Portal: Categories

We selected the **All Interesting** category from the drop-down, which detected one device browsing to a site categorized as a hacking site. And we investigated further into the flow and log data, finally drilling down to the host itself that is doing the clicking on malicious sites by clicking on the magnifying glass button on the far right and selecting device. The portal showed the source IP address that was doing the clicking. See Figure 9.

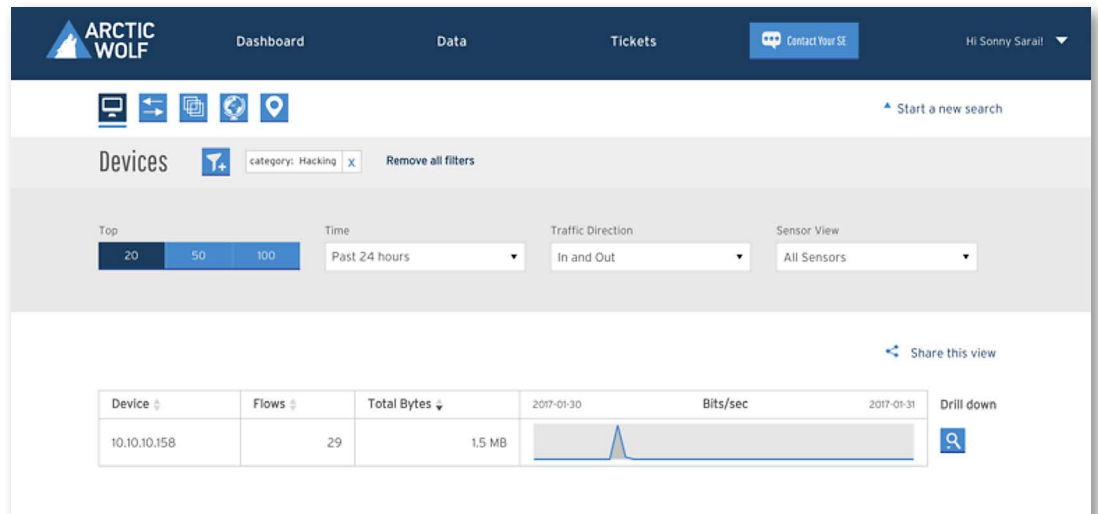


Figure 9. Arctic Wolf Portal: Device IP



Knowing the offending IP address made it easier for us to block the bad behavior, but we first decided to go one step further: We clicked the Drill Down button again and selected Sites. It told us what website was visited by 10.10.10.158, which turned out to be a forum on jailbreaking iPhones (see Figure 10).

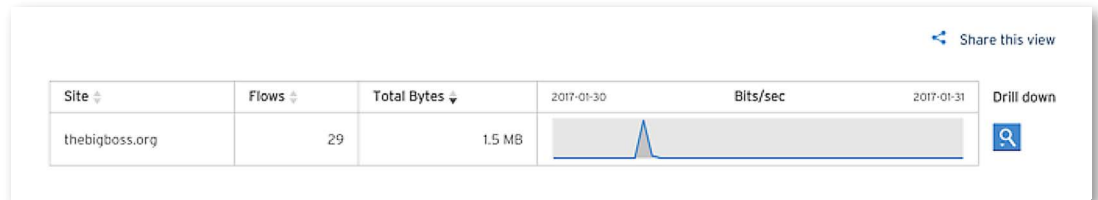


Figure 10. Arctic Wolf Portal: Suspicious Site

With this information, we could confidently shut down the bad behavior and block the website. We could also use it as training for the user who was caught going to unapproved sites and who may be intent on jailbreaking a company iPhone. Although we went through the analysis ourselves, we could have requested the same analysis to be performed by our CSE.

Mean Time to Detect

A large part of our review of Arctic Wolf's SOC-as-a-service was how quickly its SOC can detect security-related events and subsequently send us an alert. To review this, we simulated real-world attacks, possible indicators of compromise and system compromises.

Scenario 1: Ransomware

We started with a ransomware attack, because ransomware has become the primary threat impacting organizations, according to a recent SANS survey.⁴ To review Arctic Wolf's ability to detect ransomware, we decided not to use any antivirus logs and strictly focus on packet inspection by Arctic Wolf for detection. New variants of ransomware get released often and Antivirus signatures have not been updated, meaning there is a window of opportunity for an attacker to have the ransomware go undetected by antivirus.

We sent the ransomware as an attachment in a phishing email using Cerber ransomware. We detonated it on our Windows 7 domain workstation. Within seconds, the files on our shares were encrypted with a message demanding us to pay by bitcoin to get the decryption key. We carried out this operation at 2 a.m. to see how quickly AWN could detect and call us.

⁴ "From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector," www.sans.org/reading-room/whitepapers/analyst/trenches-2016-survey-security-risk-financial-sector-37337



SOC in Action (CONTINUED)

Within five minutes of infection, the Arctic Wolf's SOC team called to inform us that our environment had been infected with the Cerber ransomware as well as additional information such as the IP of the infected system and recommendations on how to contain the threat. The reason it took five minutes was the SOC conducted its own traffic analysis to ensure it was not a false positive. A ticket was subsequently created with a CSV attached detailing flow information. See Figures 11 and 12.

The screenshot displays the Arctic Wolf Portal interface. The top navigation bar includes the Arctic Wolf logo, 'Dashboard', 'Data', 'Tickets', and a 'Contact Your SE' button. The user 'Hi Sonny Sarail' is logged in. The 'Tickets' section is active, showing a list of tickets on the left and a detailed view of ticket 13797 on the right. The ticket details include the incident type 'Ransomware/Cerber Checkin M3 (13)', systems impacted '10.10.10.153', and a description stating the system has been compromised. Recommended actions advise disconnecting the system and re-imaging it.

ARCTIC WOLF Dashboard Data Tickets Contact Your SE Hi Sonny Sarail

Status: Active Closed All Last Updated: Past 30 Days Ticket Type: All Types Search: Type to search...

TICKETS

13797 - Last updated on 2017-01-23
Incident: Ransomware/Cerber Checkin ...

13273 - Last updated on 2017-01-10
Welcome to the AWN Cyber-SOC Service

Incident Type: Ransomware/Cerber Checkin M3 (13)
Systems Impacted: 10.10.10.153
Description:
The system 10.10.10.153 has been compromised. Evidence of the compromise is detailed below:
Ransomware/Cerber Checkin M3 (13) has been found on this system.
A large amount of UDP traffic has been seen going outbound from 10.10.10.153 to 90.2.1.3. Please see the attached for further details.
Incident Detected: 2017-01-19 09:15:21 (UTC)
Recommended Actions:
The system 10.10.10.153 should be disconnected from the network and re-imaged depending on your remediation policies. For more information, please contact your Security Engineer, support@arcticwolf.com.

Figure 11. Arctic Wolf Portal: Cerber Ransomware Ticket

	A	B	C	D	E	F	G	H	I
1	@timestamp	c-ip	cs-direction	s-ip	s-port	cs-appname	total-bytes	c-dns	te
2	2017-01-19T09:15:28.518000	10.10.10.153	outbound	91.239.25.255	6892 udp		42		
3	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.254	6892 udp		42		
4	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.253	6892 udp		42		
5	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.252	6892 udp		42		
6	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.251	6892 udp		42		
7	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.250	6892 udp		42		
8	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.249	6892 udp		42		
9	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.248	6892 udp		42		
10	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.247	6892 udp		42		
11	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.246	6892 udp		42		
12	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.245	6892 udp		42		
13	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.244	6892 udp		42		
14	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.243	6892 udp		42		
15	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.242	6892 udp		42		
16	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.241	6892 udp		42		
17	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.240	6892 udp		42		
18	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.239	6892 udp		42		
19	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.238	6892 udp		42		
20	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.237	6892 udp		42		
21	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.236	6892 udp		42		
22	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.235	6892 udp		42		
23	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.234	6892 udp		42		
24	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.233	6892 udp		42		
25	2017-01-19T09:15:27.517000	10.10.10.153	outbound	91.239.25.232	6892 udp		42		
26	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.231	6892 udp		42		
27	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.230	6892 udp		42		
28	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.229	6892 udp		42		
29	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.228	6892 udp		42		
30	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.227	6892 udp		42		
31	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.226	6892 udp		42		
32	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.225	6892 udp		42		
33	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.224	6892 udp		42		
34	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.223	6892 udp		42		
35	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.222	6892 udp		42		
36	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.221	6892 udp		42		
37	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.220	6892 udp		42		
38	2017-01-19T09:15:27.516000	10.10.10.153	outbound	91.239.25.219	6892 udp		42		

Figure 12. Arctic Wolf Portal: CSV File Attached to the Cerber Ransomware Ticket



SOC in Action (CONTINUED)

Although Arctic Wolf does not focus on prevention, it can detect this malicious behavior and notify the customer quickly. This allows the customer time to contain the threat. For example, it can block the attachment at the email gateway so no other systems get infected. Or it can create a rudimentary indicator of compromise based on Arctic Wolf's detection criteria to see if any other systems are infected.

Scenario 2: Anomalous Traffic

Next, we wanted to test one of the customization rules we created with our CSE: All lab desktops must use our lab proxy for Internet access, and all other traffic is blocked at the firewall. We set up the rule to alert on any traffic outbound to the Internet when the source IP address was not our proxy. (This behavior is indicative of a system infected with malware attempting to call home.)

We received an email (as per our escalation procedures) describing the event. A ticket was also generated in our portal. We decided this would be a severity two issue, which requires only an email being sent out.

The ticket shows the source address that is trying to connect out to the Internet bypassing the proxy. It also shows the destination address and port. In this case, the destination host was a malicious IP address in China. It has been noted by various threat intelligence sources that this IP address engages in nefarious activities. See Figure 13.

The screenshot displays the Arctic Wolf Portal interface. At the top, there's a navigation bar with 'Dashboard', 'Data', and 'Tickets' tabs. A 'Contact Your SE' button and a user profile 'Hi Sonny Sarail' are also visible. Below the navigation bar, there's a filter section with 'Status' (Active, Closed, All), 'Last Updated' (Past 30 Days), 'Ticket Type' (All Types), and a 'Search' bar. The main content area shows a list of tickets on the left and a detailed view of a selected ticket on the right. The selected ticket is titled 'Incident Type: Anomalous Traffic' and 'Systems Impacted: win7-patched (10.10.10.153)'. The description states: 'The system win7-patched (10.10.10.153) has exhibited anomalous traffic patterns. A summary and some samples are listed below: Flows detected to prohibited geo location (China). External IP 182.100.67.118 (Netname CHINANET-JX). Port tcp/80 (does not conform to typical HTTP)'. The incident was detected on 2017-01-27 14:25:26 (UTC). Recommended actions include blocking connections on the firewall and running a full anti-malware scan. For more information, contact the Security Engineer at support@arcticwolf.com.

Ticket ID	Status	Last Updated	Incident Type
13784	Active	2017-01-31	AWN Portal Access
14036	Active	2017-01-27	Incident: Anomalous Traffic - win7-patc...
14003	Active	2017-01-26	Incident: Misconfigured System - win2k...
13997	Active	2017-01-26	Incident: Misconfigured System - 172.16...
13996	Active	2017-01-26	Incident: Misconfigured System - ad02...
13994	Active	2017-01-26	Incident: Misconfigured System - ad01 (L...

Figure 13. Arctic Wolf Portal: Ticket on Anomalous Traffic



Scenario 3: Security Testing Arctic Wolf's Intrusion Detection System (IDS)

We wanted to test Arctic Wolf's IDS capabilities. More specifically, could it detect an attacker active on a compromised system? We decided to use Metasploit to create a malicious PDF that spawns a meterpreter shell communicating back to our command and control server. Once the PDF was clicked on in the "victim system," our attacking system had complete control of it. Our attacking system was on an external network, so the compromised system had to go through the sensor and firewall to receive instructions from the attacking system.

Arctic Wolf sent an email and generated a ticket in the portal indicating the IDS had detected a compromised system. The ticket included information such as the IP address of the compromised system and the IDS signature that triggered the alert (see Figure 14).

The screenshot shows the Arctic Wolf portal interface. At the top, there's a navigation bar with 'Dashboard', 'Data', and 'Tickets' (selected). A user profile 'Hi Sonny Sarail' is visible. Below the navigation bar, there are filters for 'Status' (Active, Closed, All), 'Last Updated' (Past 30 Days), 'Ticket Type' (All Types), and a search bar. The main content area displays a list of tickets on the left and a detailed view of a selected ticket on the right.

Ticket ID	Status	Last Updated	Incident Type
13784	Active	2017-01-31	AWN Portal Access
14036	Active	2017-01-27	Incident: Anomalous Traffic - win7-patc...
14003	Active	2017-01-26	Incident: Misconfigured System - win2k...
13997	Active	2017-01-26	Incident: Misconfigured System - 172.16...
13996	Active	2017-01-26	Incident: Misconfigured System - ad02...
13994	Active	2017-01-26	Incident: Misconfigured System - ad01 (L...

Incident Type: Anomalous Traffic
Systems Impacted: win7-patched (10.10.10.153)
Description:
 The system win7-patched (10.10.10.153) has exhibited anomalous traffic patterns. A summary and some samples are listed below:
 Flows detected to prohibited geo location (China).
 • External IP 182.100.67.118 (Netname CHINANET-JX)
 • Port tcp/80 (does not conform to typical HTTP)
 Incident Detected: 2017-01-27 14:25:26 (UTC)
Recommended Actions:
 Block these connections on the firewall to start, then investigate the system for what process is initiating them. I recommend running a full anti-malware scan for certainty.
 For more information, please contact your Security Engineer, support@arcticwolf.com.

Figure 14. Arctic Wolf Portal: Ticket on Compromised System

Having the IDS, packet and log collector all in one appliance gives Arctic Wolf the capability to correlate events quickly. The sensor does not have a dependency on any external tools. In this case, the IDS detected malicious code from analyzing traffic all done within the same appliance.



For midsize organizations, SOC-as-a-service brings two important advantages over building it yourself: One is low cost, and the other is skills and technologies that are tested and mature.

Practical Pricing

Arctic Wolf service is based on number of users, servers and sensors. There is no additional charge on data volume. Typically the number of sensors is based on number of firewalls. Other companies may charge on events per second or how many gigabytes of ingestion per day. Arctic Wolf's straightforward pricing model is competitive and attractive for midmarket organizations that want a simple, predictable pricing framework that is easy to understand.

Building a world-class SOC can be a lengthy task.⁵ So much thought goes into the planning stage, and that is just the start. The resources and training alone can be a high cost to an organization. There is also a significant capital cost for technologies running in the SOC.

With Arctic Wolf, SOC expertise can be leveraged immediately, with access to a live CSE starting at enrollment and all the security tools it already has in place. The installation is simple and done in minutes. This in stark contrast to the years it could take if an organization tried to set up a SOC itself.

⁵ "Building a World-Class Security Operations Center: A Roadmap," www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907



Conclusion

Our evaluation of Arctic Wolf's SOC-as-a-service provided us insight into its monitoring, detecting and alerting capabilities. Combining a flow monitor, IDS/IPS and log collector into one appliance makes customer implementation simple. Assigning a dedicated CSE gives customers the peace of mind that they have one point of contact.

The CSE, over time, learns the customer's environment and can make recommendations specifically tailored to the customer. This focus on using both technology and a dedicated security engineer provides greater visibility into the customer's environment and reduces the number of false positives because events are being vetted by a trained person. It is an effective strategy that can quickly raise the customer's security posture by leveraging the CSE's expertise.

The biggest challenge for midsize companies is finding the resources to manage millions of security events. Most events go unnoticed, or engineers spend a lot of time triaging events. AWN was able to analyze our 3 million events into 1,600-plus investigations that turned into a simple 12 tickets that we could manage.

Arctic Wolf's service allows midsize organizations to get a SOC up and running in minutes and at a fraction of the cost of point solutions or a full-time security engineer. It is definitely a faster, better and cheaper option than building a SOC in-house. Bottom line: With its short time to implement and comparatively low cost, CyberSOC is a comprehensive SOC-as-a-service solution for midsize companies that gives all the capabilities of a typical SOC.



About the Author

Sonny Sarai, SANS GIAC Advisor, has more than 10 years' IT experience, seven of them in an information security capacity. He now works in the Canadian retail space as a senior information security analyst, responsible for data governance, compliance, penetration testing, digital forensics and incident response. Sonny holds a degree in forensic investigation with distinction, specializing in computer crime. He holds industry-leading certifications from SANS in advanced digital forensics (GCFA) and security essentials (GSEC) and is working toward becoming a Certified Intrusion Analyst (GCIA). Sonny has a lab that consists of systems at his home and in the cloud for testing, research and development.

Sponsor

SANS would like to thank this paper's sponsor:

