SANS

WHAT WORKS™

Using Cisco Stealthwatch to Increase Security By Enhancing Critical Security Control Performance

SPONSORED BY

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know about? Let us know.

www.sans.org/whatworks

ABOUT ERIE INSURANCE

For more than 90 years, Erie Insurance has been fulfilling its promise to customers to provide auto, home, business and life insurance rooted in the principles of honesty, decency, service, and of course, affordability. Erie Insurance offers products that protect without surprises. Erie's vast network of independent insurance agents serves more than 4 million insurance customers in 12 states and the District of Columbia. With its agents, Erie Insurance continues to carry out the company's founding purpose, "To provide our policyholders with as near perfect protection, as near perfect service as is humanly possible and to do so at the lowest possible cost."

ABOUT THE USER

Jamison Budacki, a Senior Information Security Architect, joined Erie Insurance in 2011. Jamison's focus at Erie Insurance is on developing usable security architectures as well as developing monitoring and detection solutions that can be used across the corporate network. Jamison works daily with business partners to ensure that secure solutions are developed with a people, process, and technology philosophy. Prior to Erie Insurance, Jamison worked as a Security Engineer for a Fortune 100 company on the Incident Response team. Jamison received his Bachelor of Science in Informatics from the School of Informatics and Computing at Indiana University in 2005. Jamison has maintained a CISSP certification since 2007. He resides in Erie, Pennsylvania, with his wife and their two sons.

ABOUT THE INTERVIEWER

John Pescatore, SANS Director of Emerging Security Trends

Mr. Pescatore joined SANS in January 2013 with 35 years' experience in computer, network and information security. He was Gartner's lead security analyst for 13 years, working with global 5000 corporations and major technology and service providers. Prior to joining Gartner Inc. in 1999, Mr. Pescatore was Senior Consultant for Entrust Technologies and Trusted Information Systems, where he started, grew and managed security consulting groups focusing on firewalls, network security, encryption and Public Key Infrastructures. Prior to that, Mr. Pescatore spent 11 years with GTE developing secure computing and telecommunications systems. Mr. Pescatore began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems. He holds a Bachelor's degree in Electrical Engineering from the University of Connecticut and is an NSA Certified Cryptologic Engineer. He is an Extra class amateur radio operator, callsign K3TN.

SUMMARY

Audits, penetration tests, and self-assessments had convinced the Senior Information Security Architect at Erie Insurance that Erie needed to improve situational awareness to speed up detection, response and resolution of cyber-threats. Erie focused on tools that could be shared by the security group and the network operations group, to increase collaboration and coordination of efforts. After evaluating several products, Erie chose Cisco Stealthwatch and was able to document improvement in security metrics, including more effective coverage and implementation of the CIS Critical Security Controls.

Q Give us an idea of your background and your role at Erie Insurance.

A My name is Jamison Budacki, and I'm a Senior Information Security Architect at Erie Insurance. I've been there for about five years. My role consists of setting the direction for Information Security for the company and ensuring that the business's future direction is done with security in mind. Before that, I was an Information Security Engineer at a Fortune 100 company where I worked for five years on the incident response team.

Q In your role as InfoSec architect, do you report to the CISO?

A I am currently on the Enterprise Architecture team. I work closely with the Information Security department on a daily basis. Enterprise Architecture and Information Security both report to the CISO.

Q What sort of problems were you having or what reasons did you have for looking around for solutions like Stealthwatch?

A We needed improved situational awareness on our network as a whole, especially insight into our remote branch locations. Our prior toolset led to a number of challenges, some of which were:

Challenges	Targeted Opportunities
Multiple Tools	Reduce the time to find the information
Too much information	Improve efficiency and time usage
Manual correlation	Improve remediation time
Poor proactive alerts and alarms	Improve mean time to know (MTTK)
Limited Retention	Increase historical data retention
No compatibility with other technology	Increase value with compatibility
No user attribution	Gain user and device information

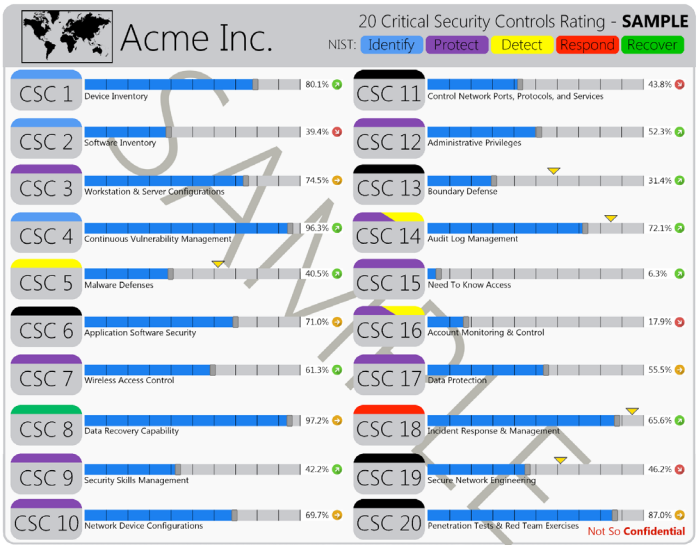
Q There are often tools the security side may buy and use, and then there are often tools in use by network operations. Is there a consolidated view across network operations on the security side? Are they done independently? How does that work?

A In the past they were absolutely done independently. Over the past couple of years, we started to work closely with the network team. Through our collaboration, we started to get insight into things like using NetFlow with Stealthwatch, and deploying Cisco ISE and integrating it into our existing processes and technology. The recent collaboration has really benefited both teams, allowing us to share technologies and ideas that make each team better.

Q Since you were down the path of looking for solutions, you probably knew you were going to end up having to spend some money. How did you get the budget to do this or how did you convince management? Was it a specific initiative or was it just part of architecture improvements? How did you justify the budget to do this?

A We had numerous penetration tests that had similar themes and underscored our need to improve in areas such as network segmentation and monitoring and detection capabilities. As part of our strategy for addressing those issues, we adopted the CIS Critical Security Controls (version 5.1). We conducted a self-assessment against the 20 controls with the goal of getting an understanding of how we scored in each of the controls. When it came time to purchase a new technology or perform an initiative within information security, we would take the idea and evaluate it against the CIS Critical Security Controls. We then asked ourselves, "Does this move our self-assessment scores if we were to do this?" The analysis and capabilities that Stealthwatch offers had a significant impact on our self-assessment scores.

To give some context to our approach, the scorecard below illustrates self-assessment scores before and after the Stealthwatch implementation for a fictitious company. For example, the blue bar and the percentage to the right of each control represent the scores of Acme, Inc. before implementing Stealthwatch. The gold triangle shows the self-assessment score after implementation.



- CSC 5: Malware Defenses improved by 21%.
- CSC 13: Boundary Defense improved by 27%.
- CSC 14: Maintenance, Monitoring, and Analysis of Audit Logs improved by 13%.
- CSC 18: Incident Response and Management increased by 7%.
- CSC 19: Secure Network Engineering increased by 15%.

A few years later, we also conducted the same process for the NIST Cybersecurity Framework. Like the previous scorecard for the CSCs, the scorecard below was designed to portray our self-assessment against the NIST Cybersecurity Framework. Once again, the blue bar illustrates the level of maturity before implementing Stealthwatch and the gold triangle shows the level of maturity after implementation. Stealthwatch had a high impact on the Detect function, a medium impact on the Respond function, and a low impact on both the Identify and Protect functions, respectively. Lastly, two sections were added to the scorecard; the first is titled "major milestones" and the other "targeted objective." The major milestones section is the chance to highlight what went well in the self-assessment period. The targeted-objectives section is the time to show what will be done for the next assessment period. The key for these is to speak in business terms as this scorecard can be shared with the board of directors to answer the question "How is my information security team doing?"

Aside from greatly improving our self-assessment scores, Stealthwatch has reduced our mean time to know (MTTK) and our mean time to respond (MTTR). Stealthwatch has also been integrated with other investigation tools for greater operational insight into incidents and visibility into all areas of our network.

Q So, you had a good starting point. Walk us through the process you used to evaluate and to find a good solution.

A Basically, we created a list of criteria that were important to us. Then, we took a look at some of the vendors in the space and attended the vendor webinars to get an idea of each vendor's capabilities. From there, we narrowed it down and had some further discussions with a few select vendors. Lastly, we conducted a POC in our lab environment.

Another benefit was having experience with NetFlow technologies at my previous employer.

Q How many different companies did you compare when you got to the proof of concept bakeoff?

A We started with two commercial products, Cisco and Plixer, and a few open-source programs. We quickly eliminated a few due to the lack of some of our requirements. We then fully tested the Cisco Stealthwatch solution in the lab, because we had some interesting use-cases at the time. One of the use-cases was utilizing Gigamon to create the flows. This was a new function for Gigamon and we wanted to make sure we were getting the output we expected. The second use-case was testing new firewall code that would enable the NAT stitching that we needed.

Q What were your top two or three criteria?

A The biggest one for us was the scalability and compatibility with other tools. As I mentioned earlier, we have quite a few tools that we like to integrate with, such as our SIEM, Gigamon, IP Address Management, Cisco ISE, and Cisco ASA firewalls. We also have secondary firewall vendors and wireless intrusion detection sensors.

One of the use-cases was that we really needed to address NAT stitching and the ability to pull some user attribution out of the firewall logs that we already had. Another major compatibility use-case we had was to utilize our existing Gigamon infrastructure. We use Gigamon for its SPAN session capabilities, deduplication, and creation of the NetFlow records. So, for us, our Gigamon infrastructure is the starting point for all of our NetFlow minus a few of the firewalls.

Q So, to get an idea architecturally, you had Gigamon feeding NetFlow data to Stealthwatch, you used a top-level SIEM side/reporting side, and you had IP address management data. Where were things like the user attribution? Where is that all getting tied together?

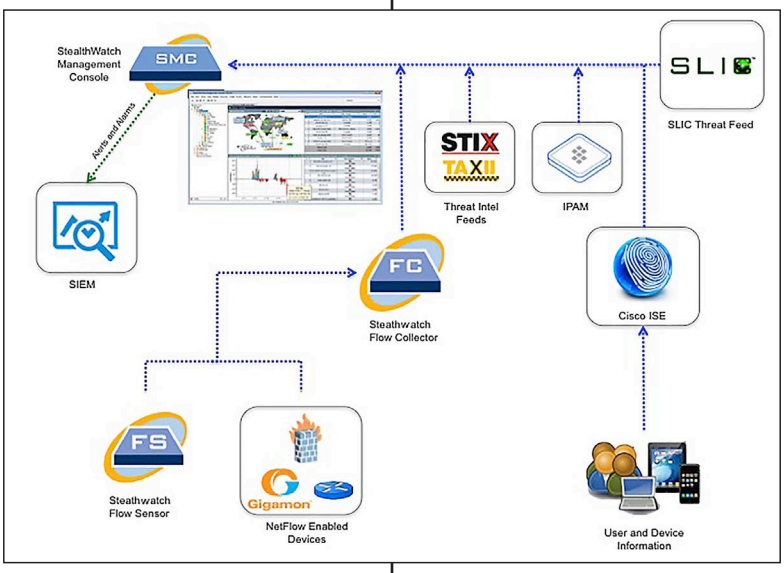
A For us, another requirement was the user attribution, and we were heading down the path of deploying Cisco ISE. This helped us fortify that decision, because we've integrated Cisco ISE with the Stealthwatch solution to provide that user attribution. This integration gives us the ability to easily search for a user within Stealthwatch. In the future, we're looking to automate some remediation decisions based on Stealthwatch rules. As an example, a client is going to a known bad site or exfiltrating a known high amount of data. We can send the client to a remediation VLAN where they will have less access to the network, get remediated, and then be returned to the production environment.

The integration of ISE and Stealthwatch has been extremely helpful in user attribution as well as deeper insight into the devices on the network. We are now able to get the username within the flows that we are reviewing. Device visibility has also improved with the addition of the MAC address, device operating system, as well as device manufacturer. These additions of the username and device info are directly from ISE integration.

Q You mentioned scalability was one of your top criteria. What is the scale and scope of what you're planning for from a deployment point of view; i.e., number of nodes on the network or users or locations.

A Erie Insurance has about 5,000 employees. We have approximately 18,000 independent agents and support staff. The agents aren't on our network, but they do interact with our systems. Our goal was to get as much coverage as possible within our network. We're doing about 20,000 flows per second that consist of all the traffic on the network, workstations to DMZ/Datacenter, DMZ/Datacenter to workstation, workstations to external, and DMZ/Datacenter to external. Right now, we're evaluating workstation-to-workstation traffic.

Q Wherever you had Gigamon capability, you're now forwarding that data to Stealthwatch? Or did you say, "Now, that we're using Stealthwatch, we also have to add other span ports" or more monitoring capabilities in addition to what you originally had?



A We're basically using Gigamon for the creation of SPAN sessions, the deduplication of traffic, then the creation of NetFlow. The NetFlow records are then forwarded to the Stealthwatch collector. We're also getting NetFlow from our firewalls (internal and external). This adds more user attribution for us, and it's making use of some NAT stitching capabilities from both firewall vendors. NAT stitching reduces the amount of flows we see. Stitching takes the public Internet IP address and our internal IP address and combines it into a single flow record. This enables us to see the actual host in question and not just a NAT address.

Q Walk us through the timeline between the point where you made the decision to use Stealthwatch and where you are today. How did you go about deploying and how long did it take?

A Like everything, the longest part is getting all the contracts and agreements in place. Once everything was in place, we deployed it pretty quickly. We did quite a bit of upfront testing with our existing technology and the Stealthwatch solution. Stealthwatch analyzed flows from Gigamon to ensure that we were getting what we wanted out of it into its lab environment, as well in our lab environment. A lot of the experts there went through and validated everything was working correctly, because at the time we were one of the first people to utilize the NetFlow creation from Gigamon. After we had all the t's crossed and the i's dotted, we were able to install it within a week. It was fairly straightforward: send the flows to the collector, set up all of the hardware as well as some of the virtual images.

Q To understand, Stealthwatch has three components; the management console, flow sensors, and flow collectors? Are the physical appliances on the collector side and you're able to run the console as a virtual software? How did that work?

A We're actually running the Stealthwatch Management Console as a virtual machine. We are running the flow collector and the flow sensor as physical hardware. We currently monitor our datacenter, various DMZs, campus, and all 25 branch locations. Stealthwatch has provided us insight into areas of our network that we did not previously have.

Q Who actually views the console and then does anything? Is that you as an architect? Is that operational? Is it multiple people?

A It's multiple people. The network team makes use of Stealthwatch as a replacement for a legacy tool that was no longer being utilized. They also use Stealthwatch for capacity planning, QoS policy development, and looking for top talkers during congestion.

Stealthwatch is primarily used by the InfoSec team and is one of the main tools when doing any type of investigation (DDoS, infection, data exfiltration, policy violation). In order for InfoSec to be successful, we have learned to ask ourselves four main questions when approaching a new process or technology:
1) What are our threats?
2) What do we want to monitor?
3) What can this do for Erie Insurance?
4) How does InfoSec respond?

What are our threats?

We understand our threats many ways. Some of the methods we are using consist of risk assessment and threat intelligence. We utilize various forms of threat intelligence. We subscribe to the Stealthwatch Labs Intelligence Center (SLIC) threat feed, are members of various information sharing groups, create intelligence from previous incidents, as well as utilize OSINT.

What do we want to monitor?

We make our monitoring decisions based off what the business deems to be important. For that we utilize internal Business Impact Analysis reports. We also monitor off existing policies, risky assets, anything with an Internet presence, and compliance/regulations.

What can this do for Erie Insurance?

This is where we measure ourselves; in this case we do self-assessments against both the CIS Critical Security Controls and the NIST Cybersecurity Framework.

How does InfoSec respond?

Our process consists of playbooks, which are outlines on how to handle an incident. We have playbooks for when we see known alerts as well as preemptive playbooks that we use to find bad things on the network. The playbooks are always evolving which helps us with measurement and drives future correlations. The playbooks help us bring some science to the art form of incident response.

Q As it relates to alerting or reacting to alerts, is the process that somebody's using the Stealthwatch console and starts going through alerts and investigating? Or are the alerts forwarded to the SIEM and you work through those alerts?

A It's a little bit of both. Some alerts we just go directly from Stealthwatch and we get them via email. All of the alarms that are triggered, we do send to the SIEM, so we can add that to any correlation searches that we may have in the future. We can look at those alerts in conjunction with other data like endpoint vulnerabilities or endpoint alerts. These alerts are also helpful with other investigations that may not source from Stealthwatch directly.

Q Based on where you are today and what you went through; knowing what you now know, is there anything you would have done differently or any lessons learned you want to pass along to other people who might follow you on this path?

A For lessons learned, I would definitely say to find a solution that provides enterprise reuse. It's going to be an easier sell to management if more than one team can make use of it. Find a solution that will consolidate and complement your existing processes and technologies. Make friends with your network team. When I started at Erie Insurance, there wasn't a lot of collaboration between the two teams and that was something I really wanted to change right away. We did that, and now with our great relationship, we make use of their technology, they make use of our technology, and it makes things operate a lot smoother. Make use of your self-assessments and the frameworks to help validate plans and show progress. For us, it is the CIS Critical Security Controls and the NIST Cybersecurity Framework. Lastly, ask your vendors how they stack up against your framework of choice. Make them prove to you why you should buy their solution.

Q On the "know-your-network side," you were trying to do user attribution, but, a lot of times along the path to trying to identify particular PCs and then particular users, people often run into, "We have problems in the way PCs are named or directories are structured" or other things. Did you have to work through those kinds of problems?

A A little bit. Our usernames aren't very humanly recognizable. It's not very easy for an analyst to look at a username and say, "Oh, that's Jamison." So, what we do is send the alert with our username to the SIEM, and that alert will populate with the actual person's name. This is done via LDAP queries to the user store that is needed. We do a couple of those things behind the scenes. Computer names are pretty easy for us, too. Cisco ISE will pull out the computer name, MAC address, and device manufacturer and place that information into the NetFlow records.

Q Since you're already using Stealthwatch in concert with ISE, are you doing active network access control and quarantining, or is that something an analyst would review an alarm and then make a decision?

A Right now, it would be an analyst who would view an alarm and make a decision. We are leveraging the 802.1x features of devices on the network as well, as a way to handle BYOD access. We are also making use of the posture assessment and device-profiling features. Our plan is to automate the response based off a given alarm or activity that is detected within Stealthwatch. We really utilize playbooks as our process.

Right now, we have a very good foundational set of playbooks around alerts that we're getting to know how to handle them. Our next iteration of what we're doing is further development into our proactive hunting playbooks. The goal is for an analyst to sit down at the beginning of the day and run through these set of plays. They go through it and try to find some potential bad things to help find some problems proactively. It encourages them to develop new correlation searches, new policy violations, and new dashboards.

Q On the operational side, is Stealthwatch administered with a full-time employee? Is the Stealthwatch person sharing it with an analyst job or some other security role?

A In our mid-sized environment, we have one full-time person dedicating half of their admin time to it – it takes probably half a full-time person to administer the tool, update, make enhancements, add more feeds as needed to keep on top of it to keep the solution running well. Analysts make use of it every day. Whenever I do an investigation, one of the first stops I make is to pull the flows for the assets in question from Stealthwatch.

Q I'll ask you about Stealthwatch support. As you were going along deploying, did you use their support to get going? And then, since you've been operational, have you used support from Stealthwatch during that phase?

A From my experience, the support is very responsive. One thing that I can tell that they focused on over the past couple of years is getting better at customer support and really building that capability. They're very willing to go out of their way to help you get an answer or a fix to your problem. We've even had instances of them being willing to dial in during our restrictive change windows, after hours, or on the weekends and make sure that things went well. Over the past few years, the Stealthwatch team has really improved their customer support and outreach with the customer community portal. The knowledge-based articles as well as the discussions are helpful for research. The onboarding of new employees has been made easier by the training that is provided for Stealthwatch. The training is on demand and available to Stealthwatch customers. Lastly, we are participants in the beta program. This allows us to test new code or features that we may want to turn on in the future in an environment that is not our production instance.

Q When did you first start the procurement?

A We started it about two years ago.

Q So, you started this before Cisco acquired Lancope. Any disruption when that happened or how'd the support and responsiveness work after they were acquired by Cisco?

A No problems. I think they are working together, but still do what they're good at. I have not seen any disruption from a customer-service standpoint.

Q Any features request or requirements that you've told the Cisco Stealthwatch team, "Hey, it'd be great if the product would do this."

A They're pretty good at staying up on the latest technologies and integrations. The biggest thing that I would like them to do is make sure that they stay vendor agnostic and continue to work with many vendors and different products.

Q Do you do any sort of network forensics-type analysis? Are you storing flow data or is it you're storing alarms and then away you go? Are you doing any sort of forensic storage of the network flows or pcaps?

A Another one of our requirements was retention. So, with our packet captures, we had less retention. We wanted to get at least 120 days of flow data, and we actually have over a year. So, that really helps us out when looking and digging through some things in the past to say, "If we were compromised by this six months ago, do we even know?" So, now we have the ability to go back and see, which is a huge help for us.

Q You do that through Stealthwatch or do you have another product integrated in to do that?

A Yes, that is accomplished with Stealthwatch. We have the ability to hold onto flows for about a year, so that's one of the major reasons we went with Stealthwatch was the fact that it met our retention needs. We didn't have to worry about open-source tools; they tend to have some scalability issues and data retention issues. Stealthwatch does a really good job in the databases and the compression that they use to store the flows. Another reason we went with Stealthwatch was if there's a hardware failure, we don't have to worry about building a new box, setting up the software on it, getting it all configured. They will just ship you a new one and you can apply all of your existing configurations via backups.

Q What are your plans for the future?

A Improved integration and automated actions with our SIEM, ingestion of intelligence feeds, and maturing our ISE deployment to take advantage of some of the interactions with Stealthwatch such as network access quarantining.