NASCIO State IT Recognition Awards

Cybersecurity Category

State of Maine

Using Security Information and Event Management (SIEM) Technology To Advance State Missions

Contact Information:

Project Manager: Matthew A. Keene

Title: Senior Cyber Security Analyst – Team Lead

Agency: Office of Information Technology

Address: 51 Commerce Drive

City: Augusta

State: ME

Zip: 04333-0145

Phone: 207-624-9519

Email: matthew.a.keene@maine.gov

Project Initiation: June 2015

Project Completion: December 2015 (phase 1)

Executive Summary

Maine's Office of Information Technology (OIT) is the state's centralized IT organization responsible for delivering safe, secure, and high-performing networks and systems to state agencies to enable daily performance of their missions for the citizens. OIT has over 450 IT professionals providing services for all Executive Branch Agencies and their 12,000 state employees, all ultimately serving Maine's 1.3 million citizens.

In recent years, Maine has focused on bolstering enterprise security, but didn't have all the pieces in place to accomplish that mission. About a year ago, Maine began evaluating different solutions to execute on its enterprise security mission, which meant providing deep enterprise security for the infrastructure and applications that they were responsible for. Log aggregation, big data analytics and rapid incident response were key requirements.

Within any security circle, there is set of best practices known as the SANS Top 20 Security Controls, which was a driving force in Maine's enterprise security mission. Through the use of its new enterprise security platform, Maine is now able to aggregate information across its environment, oversee its inventory of authorized and unauthorized devices across its network, and monitor the use of administrative privileges to track any potential insider threats.

The platform also enabled Maine to conduct maintenance, monitoring, and security analysis of its audit logs, and establish a platform to monitor state directory activity. Another crucial capability the state now has is enhanced incident response and management. By implementing this new platform, Maine was able to successfully knock out 25 percent of the SANS Top 20 recommendations, which was a monumental achievement for the state in only a period of five months

The Splunk platform Maine chose allows the state to aggregate disparate information and bring all of that into one centralized place so they could start adding security intelligence across the state.

Project Narrative/overview

When initially assessing the state's IT landscape, Maine could immediately discern a deficit of the right enterprise security tools and technologies. Maine also saw a challenge in trying to find a solid anchor for an information security plan to move the state's IT mission forward.

Maine needed a tool to aggregate all logged information coming off of servers, network devices, applications, user activity and then collect all of that to paint a picture as to what's going on within the environment. With such a tool, Maine would be able to find indicators of compromise and arrive at meaningful security analytics. Like many other states, Maine's government was running into the challenge of having a very large footprint, with a very limited number of tools and resources to manage that properly.

Another challenge Maine was looking to tackle was achieving NIST 800-53 and IRS publication 1075 compliance. These compliance standards require the state to enable logging of system information, aggregation of the log information, and monitoring for actionable security events. This platform for log aggregation and correlation provided the foundational elements required to implement a robust incident response program.

Driven by the SANS Top 20, Maine began deployment by looking across its entire environment to gain an understanding of what capabilities existed that could be leveraged, as well as what types of capabilities needed to be enabled to move the mission forward. Knowing it had compliance initiatives to adhere to, Maine's major business objective was to drive a higher return on investment for the state by developing a shared security platform for all agencies and divisions within the state.

When deployment kicked off and Maine begun efforts to stand up the new platform, departments from Maine's Office of Information Technology gathered together to help identify the correct data logs so the security team could start ingesting this information into the tool. Once that process was underway, state security dashboards began to populate with data points, which allowed the state security team to make fact based security decisions. From there, Maine was able to identify where it was going, what it needed to focus on and where it could improve from an alerting, reporting and dashboard perspective. The deployment then began to gain major momentum and value as the solution began to mature.

"Once the team was able to gain that visibility into the environment, they were really able to identify what success looked like from a deployment standpoint," said Jim Smith, Chief Information Officer, Maine Office of Information Technology.

Concept

The Office of Information Technology of Maine maintains an inventory of over 600 applications, many of which are built on older technologies. Modernizing applications or migrating to newer, modern, and flexible platforms requires time and money, and can expose vulnerabilities. Over

time, with the pressure to continually lower costs, many state governments have deferred investments in their IT infrastructure. This lack of investment has resulted in a less flexible, more expensive, and higher risk cyber environment.

Additionally, agencies have often invested in single point solutions such as multiple imaging systems, and licensing systems, instead of enterprise solutions. This is often driven by the timing of federal funding, but has resulted in a hodge-podge of expensive boutique solutions. Multiple solutions, with multiple technologies, require more expensive resources to maintain them, further reducing economies of scale.

In an environment of budget constraints, increased efficiency is more important than ever. With that in mind, Maine wanted to become more proactive in monitoring, alerting and having the ability to execute items for specific security events in a swift manner. Maine also sought access to reports and dashboards that would enable the state to visualize anomalies and trends, and uncover suspicious events more quickly.

After assessing its chief needs, it became clear that Maine needed Security Information and Event Management (SIEM) technology, as well as cyber analytics tools to achieve its enterprise security mission. Paired with its initial assessment, Maine was also looking to the SANS Top 20 Security recommendations to guide the process of where it should be focusing efforts.

Increasing cybersecurity measures, visibility, and rapid response were the overarching motivations behind Maine's decision to implement a SIEM technology. With that in mind, Maine's approach was to leverage the Splunk Enterprise Security platform as a shared model across the state. The new platform was completely scalable and had the ability to be deployed statewide, which is significant because other state agencies can lean on the platform to fulfill their compliance and security obligations.

Significance and Impact

Before deployment, there were no solutions in place within the state of Maine to achieve enterprise security results of this magnitude. "Prior to deployment of this platform, accomplishing any of these results with the speed and agility we have seen, was almost impossible," said Matt Keene, Senior Security Analyst with the State of Maine.

With the platform, Maine was able to quickly build a scalable architecture for security analytics and incident response. Additionally, Maine was able develop a shared security model so all agencies across the state could achieve security and compliance needs with limited staff and budget. Maine felt that the platform had an effect similar to "a rising tide lifts all of the boats in the harbor," and was a significant technology deployment and success story that you don't see often in state government, said Kevin St Thomas, Enterprise Security Officer, State of Maine, Office of Information Technology.

Only five months into deployment, the most significant feat thus far has been developing a foundational security architecture for security analytics and incident response. This platform has

allowed the state to address the lack of a robust security budget and to monitor more of the state's systems with less security staff.

Since consolidating its technology in 2005, Maine has made great strides in centralizing client and infrastructure services. This has resulted in more stable, secure and cost efficient services to agencies. For example, the state IT workforce has 80 less full time employees than before the consolidation. Maine continues to work with agency partners, outside partners, and other government organizations, to minimize risks related to cybersecurity, business continuity and disaster recovery to ensure stable, cost-effective platforms, and provide technical solutions through project management best practices.

Since the adoption of the SIEM solution, Maine has been able to continuously monitor the state's security posture, prioritize and act on incidents, rapidly investigate threats, and handle multi-step investigations. Additionally, Maine has reduced its incident investigation time by 80 percent and limited the threats that they are responding to by 30 percent. That percentage is also expected to increase as the solution matures within OIT.