Advanced Cyber Analytics Improves Pennsylvania's Cybersecurity Intelligence and Response Program

Commonwealth of Pennsylvania
John MacMillan, Deputy Secretary for Information Technology and
Chief Information Officer
209 Finance Building
Harrisburg, PA 17120
717-787-5440

Initiation Date: December 1, 2013
Completion Date December 30, 2014

Executive Summary

The Pennsylvania Office of Administration’s Office for Information Technology (OA/OIT) has implemented a comprehensive, advanced cyber analytics solution to aggregate and correlate data from a multitude of sources into a single platform in order to strengthen its identification and prediction capabilities for security- and cyber-related incidents.

State governments have become an even greater target for cybersecurity attacks in recent years. In addition to more attacks, there is significantly more data from various sources that needs to be compiled and analyzed as part of the investigation and response. Pennsylvania’s OA/OIT sought to implement a solution to improve upon the overall enterprise security posture and cyber security incident response capabilities, with the ultimate goal of safeguarding the commonwealth systems and upholding the commitment to protecting personally identifiable information (PII) from data leaks and fraudulent activity.

The integration of advanced cyber analytics has greatly improved the incident response process by providing enhanced visibility into potential and realized threats through a “single pane of glass” for extremely rapid response and action. The intelligence and correlation capabilities within the tool provide better visibility into the attack “kill chain” process, providing the means to effectively discover, predict and respond to cyber threats at rapid-fire speed.

In the year since the solution was implemented, the amount of data collected by OA/OIT has increased ten-fold. Thus, the time-saving benefit of this application is indispensable to mitigating and predicting cybersecurity attacks. With the security analytics platform in place, IT security incident responders are no longer burdened with the time consuming tasks of compiling and comparing separate data reports from different sources. Rather, their time now can be directly focused on analyzing a single report in real-time, determining if an incident occurred, a threat exists or an attack is imminent, and taking immediate action as necessary.

The project provided demonstrable results and drastically reduced the amount of time and human intervention required to identify, predict and mitigate cyber security incidents and cyber-attacks happening on the state network. Efficiencies in cyber incident response and user investigations have resulted in an annual realized cost savings of $617,706 for the commonwealth.

Adopting a security analytics solution has streamlined the overall incident response process and has resulted in better utilization of cyber security resources, more effective allocation of employee skills, and a more secure and resilient enterprise. The enterprise approach and implementation of the security analytics solution directly aligns with the governor’s priority for “Government that Works”, the CIO‘s IT strategic plan, the 2013 National Governors Association’s “Call to Action” for Governors and NASCIO State CIO Priorities for 2014.

Description of the Business Problem

Today’s cybersecurity threat landscape involves a growing number of sophisticated actors, advanced persistent threats and targeted breaches. State governments, which are tasked with safeguarding citizen data and confidential information, are an increasingly popular target. Hackers, nation states and cyber criminals use a wide array of advanced methods to steal data from organizations and break into government systems. In the rapidly evolving cyber threat landscape, it is no longer a matter of if a successful attack will happen, but when.

Strengthening the ability to identify and protect against and respond to security threats through a combination of human resources, robust controls, risk management strategies, intelligence reporting and response mechanisms are critical to the commonwealth’s continued protection. The need for quick and timely intelligence to provide the means to adequately respond to cyber incidents and provide an understanding of the adversary, while anticipating and predicting future potential attacks, has to be a top priority in today’s threat environment.

The Commonwealth of Pennsylvania has a multitude of enterprise security solutions and tools. While these solutions and tools are instrumental to the overall security posture, they provide little visibility into the “big picture” of what’s happening on the network – or what may happen in the future – without advanced intelligence and correlation capabilities. For example, the commonwealth has had a security information and event management (SIEM) solution in place for several years to correlate structured data and log information. However, it is no longer a match for the advanced threat actors because standard SIEMs provide little visibility into unstructured data or the identification of specific advanced attack patterns, nor do they offer genuine predictive capabilities.

In addition to the SEIM, OA/OIT regularly conducts computer forensic investigations of security incidents and suspicious system activity, as well as investigations at the request of state agency human resources departments. Existing security tools allowed for the collection of a multitude of data, however because this data was siloed into separate reports, it didn’t provide a full overview of the situation, significantly increasing investigation timelines.

When a security analyst was made aware of an inconsistency or red flag in a user’s activity, the first step in the investigation would be to construct a timeline of events in order to determine the scope of the incident. In order to create a timeline, an analyst would use various forensic tools to identify and collect the logs and metadata, organize them by type, and then import them into a spreadsheet. In some cases, the volume of data would exceed the capabilities of the spreadsheet. The security analyst would then have to manually review the data to determine if there was a security incident that required further action. This process could take as long as a week for just one suspected incident.

Over the past several years the number of external attacks on the state network increased, which in turn has increased the number of cyber security incidents requiring comprehensive investigations. The amount of data collected by OA/OIT has also increased dramatically, having grown by ten-fold in a single year.

In today's threat environment, attackers work with great speed and efficiency. However, increased incident activity and data requiring analysis threatened to drive time spent on investigatory processes in the opposite direction. Turning vast quantities of data into actionable information was a time-consuming and manual process. Analysts spent much of their time scouring through log files and running lengthy reports looking for traces of the attack. A lack of correlation to combine many data sources and/or source types into one clear and concise report in a timely manner proved increasingly problematic. OA/OIT quickly recognized there was a need to improve workflow and create streamlined and automated security processes to make better use of the rich data sets available.

Solution

Understanding that all data is potentially relevant to security, Pennsylvania took the initiative to implement a tool to connect disparate data sources to improve current processes for recognizing security events by analyzing the data collectively and quickly determining if there is a real threat.

After conducting research and evaluating different technologies, OA/OIT implemented Splunk Enterprise Security to enhance its advanced security analytics capabilities. Using this solution, Pennsylvania deployed a unique application that utilizes cyber intelligence and security analytics to correlate and aggregate multiple data sets into one system. The application compiles and compares all relevant data from log files, servers, workstations, internal network devices and access points and brings it all into a single, comprehensive real-time reporting console.

As with any new application, it was imperative to quickly showcase to leaders, stakeholders, personnel and security analysts that eliminating silos and sharing data between sources had both short-term and long-term benefits. When the new process was first presented to security analysts, there was hesitancy to adopt the application because they worried it would involve more work. Once they realized it offered them the ability to spend more time analyzing data instead of collecting and organizing it, the solution was wholeheartedly embraced.

Unlike standard SIEM tools that can only consolidate and correlate structured security log data, OA/OIT's advanced cyber analytics platform can capture structured and unstructured data from any log source, including business applications and processes. This “big data” cyber analytics approach finally provides the means to bridge cyber security to the business and create an empirical investigatory data set that can be used for future investigations, research and analysis.

The application takes Pennsylvania to a new level of cybersecurity intelligence. Security analysts are able to request information on a certain user, workstation or individual incident and obtain a full, single-pane visibility report in a matter of minutes (rather than days) in order to determine the necessary action. This upgrade provides a universal view of information, developed efficiently and delivered in real-time, to operate as a 'lens' into Pennsylvania's security posture.

Significance of the Project

Further maturing its overall enterprise security posture is one of Pennsylvania's top IT strategic goals. Advanced cyber analytics helps achieve that goal by allowing OA/OIT to rapidly identify and protect against cyber threats through a combination of robust controls, intelligent reporting and security management tools. The implementation of security analytics has provided the means to more effectively respond to cyber security attacks, identify and remediate IT security risks, and has provided a more efficient use of our cyber workforce resources.

Pennsylvania's governor has established a policy agenda based upon jobs that pay, schools that teach and government that works, with transformation, modernization and efficiency as key tenets to achieving better, more effective government. OA/OIT's enterprise approach and implementation of a security analytics solution directly aligns with these priorities.

The 2013 National Governors Association (NGA) “Act and Adjust: A Call to Action for Governors for Cybersecurity” provides strategic recommendations that states can immediately adopt to improve their cybersecurity posture. Pennsylvania's investment in a comprehensive advanced security analytics solution accomplishes several suggestions from the NGA paper, which include conducting risk assessments and allocating resources accordingly, implementing continuous vulnerability threat monitoring practices, ensuring compliance with current security methodologies and business disciplines and creating a culture of risk awareness.

Finally, the benefits seen from this application reinforce NASCIO's cybersecurity awareness best practices for data, intelligence, information sharing and gathering analytics.

Benefits of the Project

Overall, the advanced security analytics program has enhanced Pennsylvania's ability to quickly identify, respond to and remediate advanced cyber threats and incidents effectively. The application has dramatically reduced the time, effort and costs necessary to consolidate logs in order to conduct investigations and has clearly demonstrated several key quantitative, qualitative and innovation-related benefits.

Quantitative Benefits

- OA/OIT regularly receives requests from HR for investigations of log-on and log-off activities of users. Prior to the project, a security analyst needed to manually review local workstation event logs and calculate the time periods in question. A typical investigation could take up to 30 days due to all of the manual processes and calculations involved. The average salary for a commonwealth forensics investigator is $35/hour with an average cost of each investigation being $7,875. With advanced security analytics, investigations are now completed in less than 30 minutes. With 53 investigations completed to date, this translates into a **cost savings of $6,947.50 per investigation** or **$416,447.50 per year** based on the current caseload.

- The average time for analysis and investigation of a phishing incident routinely took up to 15 work hours to identify the source and the initial infection vector of the activity. During that time, the "business user" was without email capabilities. With advanced security analytics, the same investigation can be done in less than 45 minutes. These incidents equate to an individual cost of $525 per case. With 377 cases completed to date and time saved, this translates into a **cost savings of $498.75 per case or $188,028.75 per year** based on the current caseload.

- On average, the commonwealth processes 756 cyber security incidents per year. With the old system, the security analysts had to perform many manual tasks to identify the source IP, destination IP and system owner. This process used to take approximately 30 minutes per incident. With advanced security analytics, this work is accomplished instantly resulting in an **annual cost savings of $13,230**.

- Overall, the project has realized a **total annual cost savings of $617,706.25**.

Qualitative Benefits

- The solution has eliminated restrictive data silos and created a "single pane of glass" visibility, allowing data to be reviewed in real-time, which has improved cyber intelligence and incident response efficiency.

- OA/OIT utilizes this new process to identify security events, ask scenario-based questions in real-time, develop shareable reports based on discoveries and analyze all data to determine if there are any security vulnerabilities.

- With all data points in one place, security analysts have benefitted from increased network visibility and awareness which has saved time, improved productivity and boosted employee morale.

- Over the course of one year, the amount of data collected by OA-OIT has increased ten-fold. Thus, the time-saving benefit of this application is indispensable to mitigating cybersecurity risks.

- Overall, the enhanced monitoring, correlation and analysis of data capabilities across a multitude of platforms and sources has provided for a more robust cybersecurity posture for the commonwealth. Today, the solution implemented is utilized enterprise-wide. Agency information security officers have seen the value in its capabilities and are interested in additional services the platform can provide.

Innovation Benefits

Not only has this solution been beneficial in mitigating security events, OA/OIT is using this new intelligence platform to prepare for the future. Security analysts can now find new patterns and trends that were previously unknown or could only be identified through laborious and time-intensive processes. The ability to identify trends and patterns from the data to spot potential and future vulnerabilities has provided analysts and management with valuable insights and metrics to plan for future security-related budget cycles.

Continuous Improvement

OA/OIT's future plans include integrating the security analytics platform with other data sources including advanced persistent threat (APT) anti-malware technologies. Doing so will greatly expand the array of intelligence that will be used during investigations, further driving efficiencies and reducing costs.

This vision will ensure all aspects of processes are captured, from the time a computer is turned on or logged onto until the time it is logged off or turned off and everything in between. Interns from local universities have been brought on board to assist in coding and development to build additional custom queries which will assist in future cyber-incidents and investigations, driving efficiencies in operations even higher.

The inclusion of the advanced cyber analytics has taken the overall maturity level of the data intelligence lifecycle to a new level. With unstructured and structured data across many platforms collected, analyzed, integrated and correlated, the means for true optimization can be realized. The solution has created a one-stop-shop for preparing for, predicting, assessing, mitigating and preventing cyber-attacks, providing all this visibility through a single pane of glass.