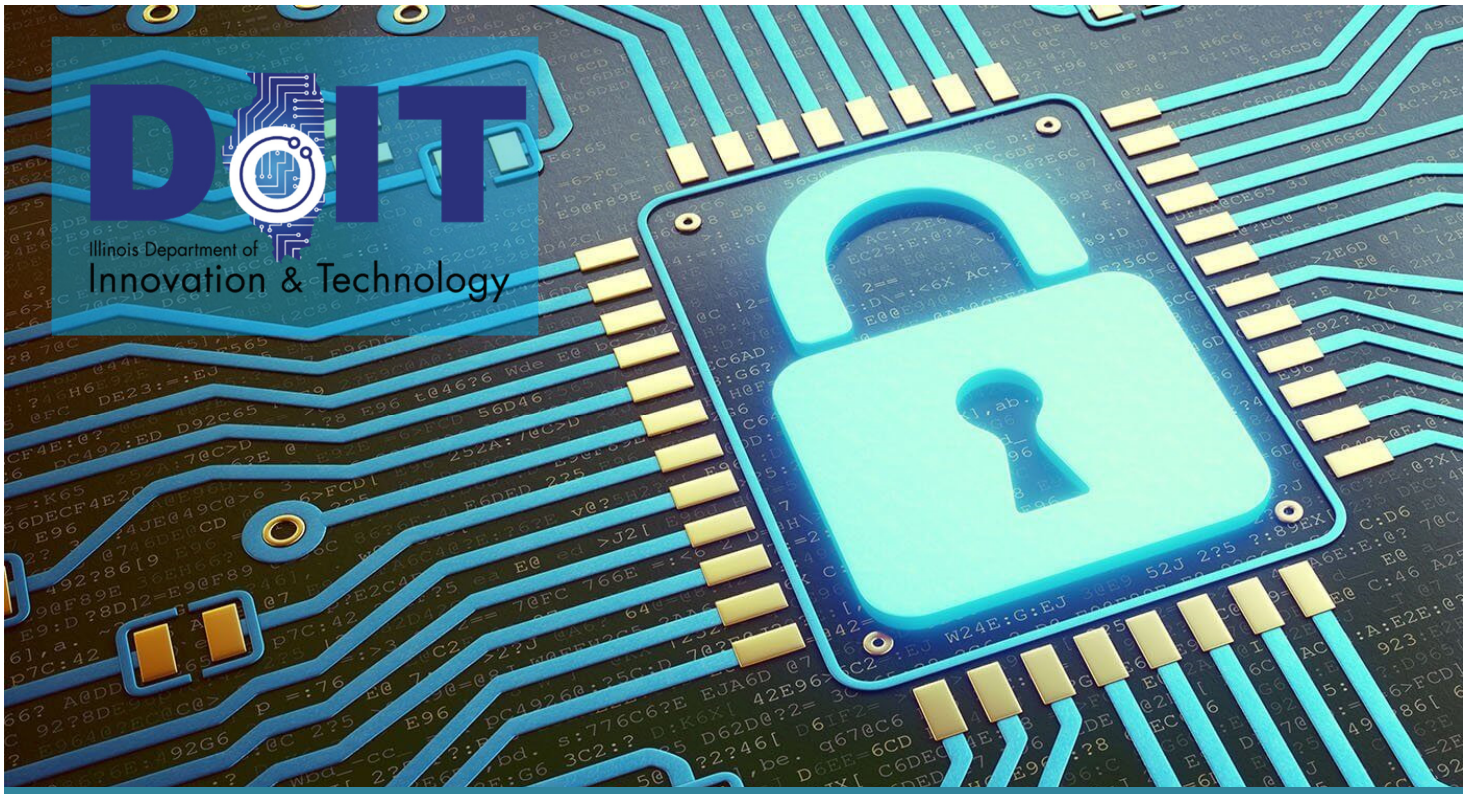

Security Operation Center (SOC)

NASCIO Award Category
Cybersecurity
State of Illinois

Chris Hill, Chief Security Officer
Department of Innovation & Technology
Chris.Hill@illinois.gov

Initiation Date: July 2016
End Date: December 2017

Executive Summary

The creation of a centralized Security Operation Center (SOC) has been a major success story for the Department of Innovation & Technology (DoIT) and the Division of Information Security. Information Technology is a critical infrastructure key resource that is integral to all functions of government. Having a centralized security team dedicated to ensure that State of Illinois information technology resources are safe and functional is essential to all operations of the State. The SOC has increased the State's ability to detect the occurrence of an event and contain the impact, which increases resiliency and decreases the effect on services provided by the State of Illinois.

The development of the SOC supports many goals and objectives of the Illinois Cybersecurity Strategy and transformed many ways in which Illinois previously handled security on our network and provided a view into operations. This increased visibility also supports many other business processes and programs already in place.

The Creation of a Security Operation Center

Concept

Background

Prior to 2016, Cybersecurity was handled by over 60 individual state agencies, boards or commissions that serve millions of Illinois citizens and employ approximately 50,000 employees. Cybersecurity efforts existed within a "silo" at the agency, board or commission level. Each siloed team had their own monitoring/response procedures and owned a small part of the response process. IT Security tools were distributed throughout the enterprise and security was viewed as primarily a compliance and response function. With the appointment of a new Chief Information Security Officer (CISO) and the issuance on January 25, 2016, of Executive Order 2016-01, a new state agency, the Department of Innovation & Technology (DoIT) was created and has the responsibility for the Information Technology (IT) functions of all agencies, boards and under the jurisdiction of the Governor. These two acts laid the foundation for centralizing security efforts under one agency to pool best practices and talent across the State of Illinois.

One of the first priorities of DoIT, the CISO and the DoIT security team was to collaborate with the National Governor's Association to create a State of Illinois Cybersecurity Strategy. The Strategy is organized around five goals:

1. Protect State of Illinois Information and Systems
2. Reduce Cyber Risk
3. Best-In-Class Cybersecurity Capabilities
4. Enterprise Approach to Cybersecurity
5. A Cyber Secure Illinois

Each of the above goals is supported by numerous objectives and actions plans. The achievement of many of those objectives relied upon the establishment of a Security Operation Center (SOC).

The SOC focuses on:

Security Monitoring

- Provides real-time alerting and remediation of unauthorized security events
- Creates a common operation picture of the security posture of the State network

Incident Response

- Addresses and manages the aftermath of a security breach or attack
- Handles situations in a way that limits damage and reduces recovery time and cost

Establishment of the SOC

When the State of Illinois CISO and the DoIT security team began their efforts for creating a Security Operation Center (SOC), they determined the existing capabilities. As previously mentioned, prior to 2016 Illinois agencies, boards and commission were operating as individual silos with limited resources and limited lines of communications.

The security team began by assessing our state and determining what tools existed and what gaps were throughout the State. Then a detailed proposal was created that provided what an ideal state for a SOC would be that included: what role a SOC would play; how it would interface with the existing environment; and what the roles and responsibilities of the staff would be.

A maturity model was established to move from current state to ideal state. This maturity model had 3 tiers of maturity. As of December 31st, 2017, Illinois is at Tier Two.

	Tier One	**Tier Two**	**Tier Three**
Goal	Use the SOC for monitoring and basic incident response	Place most capabilities in the SOC to streamline and improve coordination between protection controls, detection technology and incident response processes.	Bring advanced capabilities such as hunting and red teaming, within the SOC to shift from reacting to incidents to proactively discovering emerging threats and unknown vulnerabilities.
SOC Capabilities	Focus mostly on basic threat monitoring capabilities, such as intrusion prevention, intrusion detection, and event monitoring.	Expand the SOC's capabilities to include advanced incident response capabilities and basic threat intelligence.	Own most event correlation and proactive discovery capabilities, such as next generation endpoint, artificial intelligence, advanced analytics.
Steps to reach this Tier	*Bridging existing capabilities to Ideal State of Illinois • Creating detection and mitigation tools from scratch to perform initial response triage, • Conduct in-depth file system investigations, • Remotely remediating compromised assets, • Purchasing an incident response case management system with ticketing application for cybersecurity incidents and that provides continuity during incidents, metrics, & trend analysis.	*Created a Standardized and Repeatable Processes for: • Formal Incident response plan • Incident Response playbooks • Standard Operating Procedures • Metrics- weekly, monthly quarterly, annual • Information Security Analyst training plan	*Increasing to 24/7 coverage. *Emphasis on automation • Automated detection, investigation, mitigation, and documentation processes with little or no human interaction • Intelligence sharing with security partners and ingestion of current threats

Significance of the SOC creation

With the establishment of the SOC, for the first time ever, the State has been able to have clear visibility into malicious activity occurring on the State's network. The SOC has been instrumental in improving the overall security posture of the State by:

- Actively detecting and responding to security incidents
- Gathering metrics related to:
    - Attack vectors
    - Expose weaknesses in our environment
    - Improve incident response times
    - Determine click rates vs report rate
- Access to 24-hour reporting capabilities
- Tailoring security training efforts to quickly address and mitigate the effects of phishing campaigns
- Creating a cohesive approach for integrating threat intelligence products
- Gaining access and visibility into firewall logs

This initiative was innovative in nature as it was created with minimal funding, partnerships and during the midst of a technical transformation in state government. Not only does it increase security for the state, but it also serves as a value-added proposition for those agencies undergoing technology consolidation. For agencies, boards and commissions that have been operating in a security silo with little money, expertise and technology to secure their data and systems, the SOC serves a center of expertise previously not available to agencies, boards and commissions in an enterprise manner.

The tiered approach to the creation of the SOC described in the above information, assures successful implementation and training. The ideal state outlines a path for growth for employees. As the SOC has grown, it has allowed for further integration of other programs within DoIT's Division of Information Security. The Security Awareness program works closely with the SOC to be reactive in the development of material and training to better inform and equip state employees to be a part of the solution and to detect and stop malicious activity directed at our employees and further security eyes and ears throughout the organization. The goal is for all state Employees to be force multiplier of the SOC and part of the solution.

Impact

The SOC has greatly impacted the overall security of data, systems and the population they serve in the State of Illinois. Our society runs on information. If our ability to access, trust and protect data is compromised, our ability to serve the citizens of Illinois is negatively impacted.

Since the creation of the SOC, the security division has seen an overall 64 percent decrease in incident response time. This saves the state money in a variety of ways:

- Loss of employee downtime and lost productivity costs the state on average is $20 per hour for BOTH the employee affected the employee fixing the problem. This is cumulative total of $40 per hour.
- Potential loss of data. According the latest Ponemon Institute research, the average data breach cost $225 per record compromised, with the cost of a data breach in the US at an all-time high of $7.35 million.
- The SOC has been working with 68 agencies, board and commissions and other constitutional offices to receive their firewall logs. At of the end of 2017, Security has received 55 of the 68 logs. This increased visibility into the network traffic can help stop a breach before it happens.
- The SOC has moved the State of Illinois from reactionary posture to a defensive posture and are poised to provide offensive threat hunting.

The creation of the SOC is bringing value beyond financial and even outside of its original scope. The SOC has enabled the Division of Information Security to measure the effectiveness of employee awareness training through pro-active phishing campaigns in collaboration with the Department of Homeland Security. On January 1, 2018, HB 2371 took effect and states that all State of Illinois employees under the Governor receive annual Cybersecurity Awareness trainings. Cybersecurity Awareness training was fully implemented in 2017, a year before the bill was signed. State employees are our first line of defense, by continued training and communication this helps to increase our security on all levels.

A tool that is available to employees is the Phish alert “button” that is embedded in all incoming emails. If an employee feels an incoming email is a scam/phishing, with a click of a button an email is sent to the SOC team that is dedicated to security monitoring and incident response for follow-up and monitoring. Thus, living the “OneDoIT” motto, at all levels throughout the DoIT organization working toward one common goal of security awareness. This collaboration has been able to measure and improve training efforts as well as determine weaknesses in detection and reporting that help fine tune automated detection technology and response capabilities. This is a value-added proposition that was not planned for.

- The partnership between the SOC and Security Awareness Training has given the State visibility into the click rate of users, ratio of report-to-clicks, average time to first click and average time to first report.
- This valuable information enables training with a new ratio of reports-to-click as 2.0. Pre-SOC this was unmeasurable as there was not a method in place to track metrics. From Tier 1 to Tier 2 the ratio moved to 1.11. Tier 3’s SOC implementation goal will be a 2.0 ratio of reports-to-

click. This ratio increase could result in millions of dollars of saving if an incident was reported and stopped prior to it becoming a breach.

The SOC is revealing a strong need for a more automated approach to security incident response. This discovery supported the Division of Information Security's decision to work with the Engineering section to deploy products capable of communicating threat intelligence across state environment. This results in cost saving to the State of Illinois by using only products that work together and consolidated licensing costs for applications. The term "security fabric" describes this system of shared threat intelligence, incident response management and integrated tools across our many platforms. Taking this fabric approach allows the state security tools to learn from each other and reduce security risk, which helps to achieve other goals within the Cybersecurity Strategy. The fine tuning and training of these tools helps create a tighter weave to the security fabric to get the best benefit. The SOC is integrating existing technologies with new technologies to improve the security posture of the state.