Toward Automated Information Sharing California –

Cybersecurity Integration Center's approach to improve on the traditional information sharing models

Keith Tresh
Maxim Kovalsky

INTRODUCTION

On August 31, 2015, California Governor Jerry Brown signed Executive Order B-34-15, directing the establishment of the California Cybersecurity Integration Center (Cal-CSIC). The new center operates under the auspices of the Office of Emergency Services (OES), with the California Department of Technology, California National Guard, and the California Highway Patrol acting as the key partners in the coordination of cybersecurity related activities within the State.

In his Executive Order, Governor Brown tasks the Cal-CSIC with two primary missions: facilitate information sharing across the state and coordinate statewide responses to cyber incidents. Given the increasing threat from cyberattacks to the State government and all California governments, businesses, and citizens, the Cal-CSIC's mandate is immediate action to mitigate those risks. It takes significant planning and time to coordinate an incident response capability for statewide deployment, therefore, the immediate focus is to create and implement a statewide information sharing program.

The team faced a critical decision: Should the Cal-CSIC adopt a unidirectional information sharing model whereby the primary product is human-readable and addresses common threats and vulnerabilities, or take advantage of the mandate and experiment with a unique approach? The authors of this paper argue that for cyber threat information sharing to be effective it must be crowd-sourced, where partners agree to share technical details about suspected intrusions with all other participants and done at machine speed. They also reflect on the lessons learned from their experience implementing such a program.

Keith Tresh was appointed as the commander of the California Cybersecurity Integration Center (Cal-CSIC) by Governor Jerry Brown on October 6, 2016. His office is part of the Governor's Office of Emergency Services.

A retired Army colonel, Mr. Tresh is also a veteran C-level IT management professional and an educator with a passion for information assurance and awareness. He served in the Army for more than 33 years, including a combat tour in Iraq from 2005-2006. Among his many assignments, he was the J6 for the California National Guard from November 2006 to June 2011.

Keith holds a Master of Science degree in Computer Information Systems from the University of Phoenix and a Master of Science in Strategic Studies from the Army War College. Mr. Tresh lives and works in Sacramento with his wife Coco and his children – Justine, 30, Austin, 24, Hunter, 22, and Kristina 18.

Given the decentralized nature of California state government networks, where each agency and department is responsible for managing—and securing—its infrastructure, historically, information about cyberattacks on one entity was not readily shared with other organizations. Before the establishment of the Cal-CSIC, there was not an organization positioned to share security information and expertise with all California governments, whether state, local, or municipal, higher education, utilities, and the private sector.

Cal-CSIC's unique value

The Cal-CSIC builds and expands upon the existing partnerships of the California State Threat Assessment Center (STAC) which is collocated with the Cal-CSIC.[1] In collaboration with federal agencies, fusion centers, local and municipal governments, and other information sharing organizations, the Cal-CSIC gains access to and disseminates information about existing and emerging cyber threats. While processing, analyzing, and disseminating information on opportunistic cyber threats to California entities was an important start, the Cal-CSIC acknowledged early on that it needed to produce actionable data and products.

Information that brings the most value to Cal-CSIC's partners reflects the threat's current posture, profile, and intent. This information is a "live broadcast" about cyber incidents that are unfolding across California. Given the Cal-CSIC's position at the intersection of federal and state government entities, it has the right resources to accomplish this ambitious goal. This "broadcast" enables the Cal-CSIC to develop an early warning system, where the collective can prevent attacks through the use of the data it gains from the first victim of the attack. Finally, to keep pace with the speed at which attackers change their infrastructure and techniques,

Maxim Kovalsky is a Senior Manager in Deloitte's Cyber Risk Advisory practice. With over ten years of experience in technology and cyber security, Maxim's work at Deloitte has focused on security intelligence and operations strategy and implementation projects across multiple sectors. He has led engagements in areas covering cyber security program assessments, threat monitoring and detection, cyber incident response, and threat intelligence.

Prior to joining Deloitte, Maxim directed cyber threat intelligence research at Flashpoint, where he supported clients in the healthcare, retail, and financial services sectors. Before that, Mr. Kovalsky worked for the Federal Bureau of Investigation, providing operational and intelligence support to complex cybercrime investigations. Mr. Kovalsky is a reservist in the US Army and a member of the Cyber Threat Fusion Cell within the Army Reserve Cyber Operations Group.

the Cal-CSIC has to process, correlate, and share information as close to machine speed as possible.

The added strategic benefit of an efficient sharing of tactical information requires the development of a holistic picture that describes the threat landscape facing a broad set of California entities. Understanding the threat holistically, as well as the trends in cyberattacks can allow state leaders and business owners to formulate a rational model for resource allocation.

Challenges with traditional information sharing models

At the beginning of the Cal-CSIC's development, a critical decision faced the team. Should the Cal-CSIC adopt a commonly implemented information sharing model where most of the burden to produce threat and vulnerability notifications rests with the center? To determine an answer to this question required an understanding of the challenges inherent in the traditional model and a new vision for how to improve. The following challenges were identified in the very early stages of planning and design of the Cal-CSIC's future state.

Alerts Take too Long to Produce. Given the speed at which attackers change tactics and infrastructure, production and dissemination of human-readable reports frequently result in the information recipient getting data that is no longer relevant or actionable. There is a benefit in detecting a previously unnoticed intrusion based on that information, but it has little preventative value.

Free Rider Problem. In addition to delays associated with manually sharing cyber threat data from an incident, the model is plagued by the free rider problem.[2] Stemming from economic theory, the free rider problem occurs when absent a precise definition or enforcement of rules, members of a community use a public good or service without contribution. The problem is exacerbated when members decrease their contributions because they believe that others are riding free, which leads to the eventual depletion of that good. Voluntary and manual contributions in the context of information sharing suffer from a similar problem, wherein partners may be reluctant to share information due to resource constraints, or fear of appearing vulnerable.

Operationalization Challenges. Consumers of shared information frequently struggle to understand how it is relevant to their operating environment. The recipient grows weary after parsing so many notifications that do not apply to their agency. Unparsed cyber threat products often end up in email folders that are rarely checked. In addition to email fatigue, there are challenges associated with operationalizing information for those events that are deemed relevant. If the message contains an attachment with a list of threat indicators, for example, someone on the receiving end must be tasked with parsing out that data; someone else has to enter that data into reference lists for alerting or blocking within security technologies. Given the acute cybersecurity talent shortages within the public sector, the few resources capable of accomplishing those tasks are likely stretched too thin to take on additional responsibilities.

Lack of Trust. Participation in information sharing organizations is often hampered by the lack of trust of members in the conduit of shared information. Partnership candidates fear that the information shared by them will expose their organizational deficiencies or question their capabilities to defend against cyber threats with ramifications to influence over critical decisions, careers, budgets, and the projected image of the entity.

The envisioned solution

Solving for the four mentioned deficiencies above with traditional information sharing models requires the reduction of human involvement in the sharing, receipt, and actions taken on threat information. In other words, sharing information—both from center to the hubs, and from the hubs to the center—has to be as close to machine speed as possible. At its core, the model has to be supported by a technology that allows the Cal-CSIC to receive attack telemetry from partners, aggregate the relevant data, and disseminate it to threat detection and mitigation tools for automated ingest and action.

The envisioned solution architecture, depicted in Figure 1 below, started out with deploying a threat list integration server within the partners' network technology environment. This virtual machine pulls new threat indicators from the Cal-CSIC's threat intelligence cloud at periodic intervals and organizes the data by indicator type. The Security Event Information Management (SEIM) system is configured to ingest this data and alert security analysists of any positive correlations. In step 2 of this layer, potentially malicious events that meet Cal-CSIC's criteria are minimized to ensure that no attributable or personally identifiable information leaves the agency, and are forwarded to a local security event collection server, which in turn, submits these events to the Cal-CSIC's security event reporting platform. Newly observed indicators are then shared with the rest of the partners through the threat intelligence platform, as depicted in step 6 of the diagram.

SECURITY EVENT INFORMATION MANAGEMENT (SEIM) SYSTEM

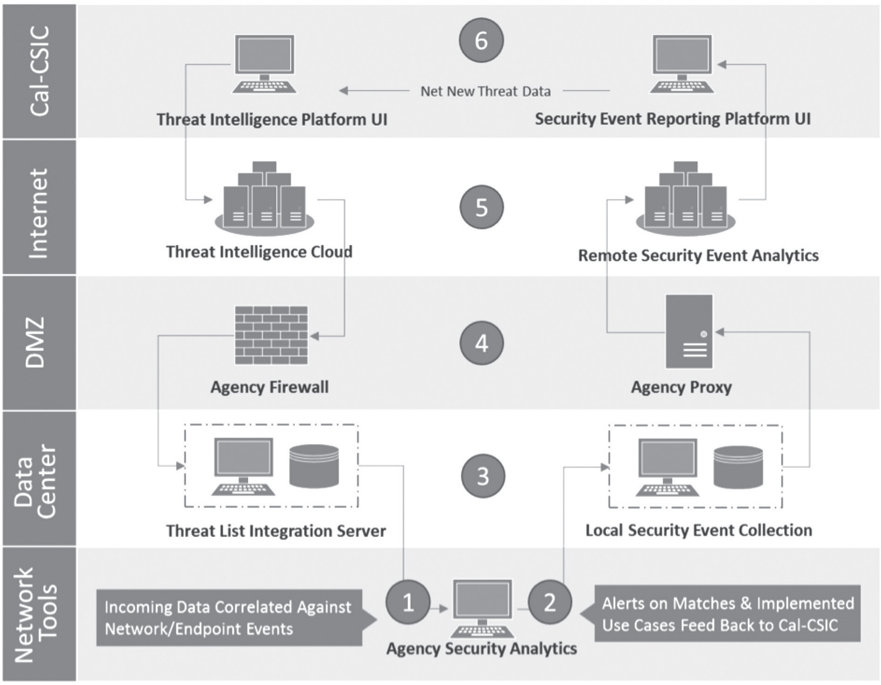
Cal-CSIC
Internet
DMZ
Data Center
Network Tools
6
Threat Intelligence Platform UI
Net New Threat Data
Security Event Reporting Platform UI
5
Threat Intelligence Cloud
Remote Security Event Analytics
4
Agency Firewall
Agency Proxy
3
Threat List Integration Server
Local Security Event Collection
Incoming Data Correlated Against Network/Endpoint Events
1
Agency Security Analytics
2
Alerts on Matches & Implemented Use Cases Feed Back to Cal-CSIC

Figure 1. Solution Architecture

To alleviate the burdens associated with the initial integration, the Cal-CSIC provides direct support to partners to configure their threat detection and mitigation tools to leverage a common data model. This enables partners to alert on or block correlated internal events that are generated by the Cal-CSIC-shared data without additional human intervention.

Once the threat intelligence integration technology was implemented, the Cal-CSIC established unidirectional automation to share attack data out to partners. This process is depicted in step 1 of Figure 1. Unidirectional sharing dramatically enhances the speed at which attack data is shared and implemented for preventative and detective purposes. Automation also addresses the operationalization challenges because indicators are ingested directly into the security devices, relieving a human operator from the task of taking manual steps to act upon each portion of received data.

However, unidirectional indicator sharing has its limitations. It does not address the free rider problem nor the lack of trust. To overcome these challenges, the Cal-CSIC partners have to agree to abide by a set of core requirements to receive the benefit of the Cal-CSIC's crowd-sourced threat intelligence. Participation is always voluntary which strengthens the trust amongst participating members. Automation of the sharing process serves as an enforcement mechanism while increasing the speed at which other partners receive the valuable information.

The Cal-CSIC and its partners have a shared understanding of the model through clearly defined parameters of information that is subject to sharing through a common data model. Practically, this requires walking potential partners through the process and then formalizing the relationship by a mutually signed Memorandum of Understanding (MOU). To mitigate privacy concerns and protect civil liberties, the Cal-CSIC clearly defines the data elements: information attributable to a specific organization or its users is not shared with Cal-CSIC's other partners.

To support the common data model, the Cal-CSIC has a defined matrix of threat detection use cases and criticality ratings that contain information relevant to the Cal-CSIC partners. Each of the use cases requires a level of visibility into the environment necessary to detect the malicious activity in question. For example, to detect account sharing, which may indicate a compromise of credentials, the use case requires the collection and processing of Windows and Linux event logs. An example of this particular use case is shown in Figure 2 below. A roadmap for onboarding the necessary log sources is developed with each partner early in the onboarding process, and progress throughout onboarding is monitored.

ID	USE CASE NAME	USE CASE DESCRIPTION	ANTICIPATED LOG SOURCES	EXT IOC TYPE	BASE QUERY
TA-010	Potential account sharing detected from distinct source address	Detect and alert on internal apps and authentication to those apps for the same user, from different sources in X amount of time	WIN Logs (login events etc.) Server (WIN/UNIX) Asset (Office Information etc.)	N/A: All internal network events	Sourcetype= <windows_logs> | eventstats count (<src_ip>) as TotalSource by <UserID> | where TotalSource > <threshold>

Figure 2. Account Sharing Use Case

Once the threat detection use cases are deployed, and an alert is generated that meets the established criticality threshold of the relevant attack data and context, it is automatically forwarded to the Cal-CSIC. The Cal-CSIC then analyzes and shares this attack data back out to the partners which creates a multiplier effect where one partner's successful detection of an attack can lead to prevention and detection across the other partner entities.

Testing the solution during a pilot

The Cal-CSIC's strategic goals are ambitious, and the Cal-CSIC understands that to pioneer an advanced information sharing model requires hiring able staff, developing the processes to onboard new partners, and deploying the information sharing technologies. The Cal-CSIC also appreciates that their operations cannot happen in a vacuum and that the integration model needs to be tested by partners for viability. As a result, the Cal-CSIC decided to develop its information sharing program through a pilot. Three partners, the California Department of Corrections and Rehabilitation, the Governor's Office of Emergency Services, and the California Franchise Tax Board participated in the six-month pilot and provided feedback throughout the process to enable the Cal-CSIC to get the program up and running while simultaneously identifying enhancement areas to facilitate future partner onboarding.

Several challenges were encountered early in the process. For information sharing to have value, the partner receiving the attack data must have security tools that are configured to accept and act upon the data. Once the Cal-CSIC began working directly with each partner on the technology integrations, it became clear that the Cal-CSIC would need to assist the partners to configure their existing threat detection technologies to both send and receive the relevant alert data. The Cal-CSIC has overcome this challenge by assigning a security engineer to work with each of the partners to implement new threat detection use cases or to enhance existing logic.

Valuable lessons were also learned from the perspective of relationship management and continual partner engagement. Initially, the Cal-CSIC sought an executive sponsor within each partner entity to drive the Cal-CSIC integration within their organization. However, throughout the pilot, the Cal-CSIC understood that the formal role of the leader who facilitated the Cal-CSIC integration was not the determining factor in the success of the integration. While it is important that the leader clearly communicates to the staff the benefits to the organization, when it comes to resource allocation to accomplish the required tasks, it is the involvement of middle management who champion the integration that assures the success of the partner onboarding. This is a valuable lesson learned because it demonstrates that either an executive or a middle manager can champion the Cal-CSIC integration. This enhances the scalability of the Cal-CSIC because middle managers are often closer to the resources and security tools than executives, and can personally conduct or oversee the integration.

Opportunities for improvement

As the Cal-CSIC moved from planning, to pilot, to the operationalization of the program it has identified several areas for improvement across the state's security posture and within the Cal-CSIC. Through a series of conversations with potential partners, it became clear that many state entities perceive emerging security technologies as the panacea to cybersecurity risks. Advanced security tools, however, often provide little value when deployed with default configurations. They require a team of professionals with security engineering skills to continuously configure and customize these tools to both reflect the reality of the local environment and the dynamics of the threat landscape.

The Cal-CSIC also observed that the model deployed during the pilot is useful for entities with existing Information Technology and security programs, and ones that have visibility into their respective environments. However, it would not be effective for an entity that had little to no visibility or security infrastructure to consume the shared information. For these entities, the Cal-CSIC recognizes that an alternative model is required. This additional model entails the Cal-CSIC deploying and managing sensors at the partner entity.

Finally, as the Cal-CSIC scales to incorporate partners from across local and state agencies, tribal governments, utilities and other service providers, academic institutions, and non-governmental organizations it is clear that the volume of data that the Cal-CSIC will ingest and share will require a big data processing platform. The scale of the Cal-CSIC's technology stack must match the scope of the Cal-CSIC's mission. Additionally, the Cal-CSIC must implement further automation and data analytics that will enable rapid analysis of the received security data.

CONCLUSION

An information sharing model that is easy to implement is likely ineffective. Although automatic bidirectional information sharing requires more time and expertise on the front-end than in a traditional information sharing model, it creates sharing mechanisms that are both more responsive to today's threat landscape, and are more effective in preventing and detecting those threats. These benefits are multiplied by the speed at which this information can now be shared, which imposes high costs on the attackers by rendering the staging infrastructure useless in a brief period.

The authors of this paper do not argue that while the Cal-CSIC's approach was unique in the state government sector, it is not the only model to effectively counter emerging cyber threats. Other states, for example, have moved down the path of consolidating networks into an enterprise environment to gain direct visibility into malicious events at the asset level, rendering technical information sharing superfluous.

For other state governments operating with a federated organizational structure similar to California's, the Cal-CSIC's pilot demonstrates the feasibility of leveraging bidirectional information sharing to increase the cybersecurity posture of the state as a whole.

NOTES

[1] "State Threat Assessment Center," Governor's Office of Emergency Services, http://www.caloes.ca.gov/cal-oes-divisions/state-threat-assessment-center, accessed on May 10, 2018.

[2] Russell Hardin, "The Free Rider Problem" The Stanford Encyclopedia of Philosophy, May 21, 2003.