Statewide Security Operations and Intelligence Center

Executive Summary

California Department of Technology's (CDT) Security Operations Center (SOC) is the newly established, last line of defense that collaboratively tackles threats across State government.

The SOC is co-located with the CDT statewide data center and provides network protection and detection for all 100+ state entities utilizing the state's wide area network as well as IT resources managed by CDT. The SOC, which is staffed by state civil service, the California Military Department and private sector contractors, became fully operational July 2017. To compliment the SOC, the Network Protection Team (NPT) was also added. NPT augments the SOC by implementing technical controls and configurations that mitigate cybersecurity threats identified by the SOC and/or alerts from inspection points within the network of the state data center and/or CGEN network. The SOC and NPT together have prevented more than 100 security incidents across state entities and blocks 200 million plus malicious scans and targeted attacks daily.

Cyber adversaries have unlimited time and resources to target California from around the globe, with unlimited time to get lucky exploiting a potential vulnerability. California State government entities need to be as close to one hundred percent perfect to be able to defend against this ever-increasing global threat. The newly created CDT SOC defenses, backed by modern cloud-based and automation capabilities, effectively mitigate any frontline vulnerabilities. The outcome of this effort enables common statewide defenses to keep up with the threat as it advances and persists at a global scale. Through the SOC's cloud-backed security technology and advanced automation, California is able to use large-scale compute resources to enable our security workforce to be highly effective against cyber adversaries.

Concept

The *Vision 2020 California Technology Strategic Plan* foresees one digital government securely delivered by a dynamic workforce and delivering secure, effective and innovative technology to the people of California.

The California Department of Technology (CDT) Office of Information Security (OIS) is responsible for ensuring a variety of imperative controls that protect California's sensitive data. This includes ensuring the confidentiality, integrity and availability of State systems and applications; promoting and protecting privacy as part of the development and operations of State systems and applications; and developing and implementing information security policies, standards and guidelines. OIS is responsible for coordinating the activities of State agency information security officers for the purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy standards and policies; and enhancing state agencies risk management and privacy programs. The CDT Security Operations Center (SOC), provides protection against, detection of and response to malicious activity targeting the California Government Enterprise Network (CGEN) and IT resources managed by CDT. One hundred eleven state entities, as well as some counties and local jurisdictions, use CGEN.

Significance

The accelerated pace of the shifting cybersecurity landscape, and the unprecedented agility and evolution of cyber threats, pose an ever increasing danger to the state's information assets. CDT's OIS is statutorily responsible for ensuring the confidentiality, integrity, and availability of state systems and applications by developing and maintaining state information security policies and standards, and providing direction to the State to ensure the protection of the its digital assets. This scope covers over 140 distinct State entities, including State agencies, departments, as well as boards and commissions. One significant aspect of meeting this responsibility has been the establishment of a SOC, which is the first of its kind in the State of California.

The initial concept of the CDT's SOC was expeditiously established in July 2017. It began as an 8 to 5 operation that expanded to full 24/7/365 operation beginning November of that year. The scope of the SOC's monitoring capability, includes the entire California Government Enterprise Network (CGEN, which is the State government-wide area network, or WAN). It also includes the consolidated State data centers operated by CDT, which hosts a large number of California's mission-critical government applications systems, including public safety, health services, revenue collection, budget management and other vital services on which constituents and government programs rely. The complexity involved is significant in that the IT assets involved include Windows servers, Linux services, AIX and Solaris servers, zLinux, mainframe, desktops, storage systems, firewalls, routers, and many other data center devices.

This entire effort falls within Goal 4 of the California Information Technology Strategic Plan that states.

Secured Information:

Public sector leaders must secure the trust and gain the confidence from consumers of government services and information if the state is to effectively serve its constituents. To engender trust, the state must safeguard sensitive data through strong privacy and data security practices. Further,

state entities must be prepared to operate during times of disruption (natural disasters, unplanned outages, and other events).

Additionally, by leveraging data resources and analytical capabilities, the state can convert data it already collects into actionable information to make informed policy decisions, administer programs, reduce costs, improve outcomes, and better serve constituents. By making IT systems and transactions secure, state entities ensure that Californians can leverage technology with confidence to access the services and information they need.

Objective 4.1

- Protect sensitive data through robust security and privacy programs.
- Implement and monitor compliance with security and privacy policies, standards, and practices.
- Provide accountability where compliance failure has exposed sensitive data to avoidable risk.
- Raise awareness of information security risks and train and educate state technology users.
- Implement next generation security tools.

Impact

The SOC is staffed by a combination of State civil service staff as well as members of State active duty military staff in a unique blend of the two staffing sources. Current staffing levels total twenty (20) monitoring staff, which is planned to grow further in Fiscal Year 19/20, plus ten (10) support staff who implemented the new and complex technologies that provide uninterrupted monitoring, threat intelligence and alerts to deter malicious cyber actions. The NPT is a matrixed team consisting of security staff and individuals from CDT's Network Engineering groups whom together are responsible for implementing and holistically managing network protection safeguards across the state data center and the California Government Enterprise Network CGEN network. The primary benefit of bringing the security and network teams together was to ensure that security safeguards within CGEN didn't compromise the availability of network services supporting mission critical systems for the state. In turn, this team ensures changes within CGEN does not create vulnerabilities that could be exploited.

Implemented technologies include security analytics, security operation workflow management, intrusion detection/protection, security focused packet capture, vulnerability scanning, and Artificial Intelligence based network analytics, incident management, web access protections, endpoint protection, and communication and coordination technologies. These require constant and active management and tuning to ensure that they are aligned to detect the most current malicious threat profiles based on multiple sources of threat intelligence. Additionally, incidents must be rapidly detected, dissected, and remediated by both SOC and NPT staff; in addition to IT security staff across the state. To illustrate the efforts involved, through the first three months of operation in FY 17-18, these efforts resulted in 7,330 events processed by SOC staff and 34,948 total events generated from CGEN, which resulted in nine confirmed and reported security incidents. As one can imagine recent results are even greater in scope.

Between 2018 and 2019, the SOC responded to and mitigated hundreds of events indicating malicious activity. Some of the activity include attacks related to ransomware, malspam, botnets, Distributed Denial of Service (DDoS), and account takeovers. The impact from such activity was

minimized to prevent largescale adverse impacts. The potential of damage if unmitigated may have resulted in direct or indirect costs to the State in the orders of 80-100 million dollars annually. The processes and activities conducted by the SOC significantly reduce the amount of time a potential attacker can reside on a network and to reduce the opportunity for largescale adverse impact an attacker is able to cause California. Additionally, the NPT through automation and architectural changes have been able to reduce the time to mitigate Distributed Denial of Service (DDoS) attacks against CGEN resources from which in past may have taken hours across CGEN

The SOC establishes partnerships and cyber threat intelligence processes in order to receive and scale the defenses in a collaborative manner. These partnerships are led by the Governor's Office of Emergency Services (OES) California Cybersecurity Integration Center (Cal-CSIC). This allows the SOC to gain intelligence indicators from other partners at the Federal, State, and Local levels to maximize the SOC's defensive policies. This also allows the State SOC to share threat indicator information to other organizations collaborating with the Cal-CSIC.

The SOC monitoring and protection capabilities are embedded within the statewide network and offer all entities the following services:

CALIFORNIA GOVERNMENT ENTERPRISE NETWORK (CGEN)	STATEWIDE DATA CENTER	CALIFORNIA CYBERSECURITY INTEGRATION CENTER (CAL-CSIC)
• CGEN Edge Detection • CGEN Edge Protection • Distributed Denial-of-Service (DDoS) Protection • Initial Incident Response • Network Forensics	• Unified Integrated Risk Management platform • Endpoint Protection • Email Threat Detection • Network Threat Detection and Prevention	• Complex Incident Response Coordination • Statewide Cyber-Exercise • Threat Information Sharing • Prioritize and Communicate Threats

It is believed that these efforts are unique within state government and represent a model that can be utilized elsewhere to raise the level of cyber security protections that are needed across state governments.