California Department of Technology
STRATEGY INNOVATION DELIVERY

Statewide Security Operations Center as a Service (SOCaaS):

TRANSFORMING CYBERSECURITY ACROSS CALIFORNIA

California Department of Technology (CDT)
California Government Operations Agency

Award Category: Cybersecurity

Project Dates: Fiscal Year 2021-2022 - Present

Conrad Long
Office of Information Security, Security Operations Chief
916.898.4559 (office) ● conrad.long@state.ca.gov

Executive Summary

In today's rapidly evolving digital landscape, cybersecurity threats loom large, especially for government entities responsible for safeguarding sensitive data and ensuring the continuity of essential services. Enter the California Department of Technology (CDT) Offi ce of Information Security (OIS) with an audacious and groundbreaking initiative: **Security Operations Center as a Service (SOCaaS)**

.

Launched in Fiscal Year 2021-2022, this visionary project is designed to transcend traditional boundaries, extending robust, scalable, and cost-eff ective security monitoring and threat detection services beyond the executive branch to all public sector entities, including critical infrastructure.

IDEA

Transforming California

Enhanced Protection of Sensitive Data and Services	SOCaaS provides strong cybersecurity measures to protect sensitive data and critical public services from cyber threats, ensuring that Californians' personal information is safeguarded against breaches and unauthorized access.
Improved Public Trust and Confidence	By implementing cutting-edge security measures, SOCaaS helps to prevent service disruptions and data breaches. This enhances the public's trust in state and local government entities, ensuring that Californians feel more secure in their interactions with government services.

Cost Savings and Efficiency	The initiative has led to significant cost savings for the state, which can now be redirected to other important public services and infrastructure improvements. This efficiency optimizes government spending and ensures that resources are utilized effectively for the benefit of all Californians.
Accessibility to Advanced Cybersecurity Resources	SOCaaS now extends its services to all public sector entities, including smaller local governments that may lack the resources and expertise for advanced cybersecurity measures. This ensures that all Californians benefit from the same level of protection, democratizing cybersecurity resources.
Faster Response to Cyber Threats	The advanced tools in SOCaaS enable quick detection and response to cyber threats, reducing downtime and maintaining essential services for Californians.
Educational and Community Benefits	SOCaaS promotes cybersecurity awareness and education, benefiting schools, universities, and the general public by building a more informed and vigilant community, better prepared to handle and prevent cyber threats.

Implementation

Addressing Critical Cybersecurity Challenges

SOCaaS stands as the unwavering protector against the ever-growing threats state and local government entities face.

Prior to SOCaaS, many entities struggled, lacking the resources and expertise to combat advanced cyber threats. Adhering to the State Administration Manual (SAM) and the Cal-Secure roadmap presented formidable challenges. SOCaaS rises to meet these challenges head-on, offering continuous security monitoring, incident detection, and response services at no cost to participating entities.

This initiative bridges cybersecurity gaps, ensuring that entities of all sizes have access to state-of-the-art security tools and expertise.

Why SOCaaS Matters

The vision behind SOCaaS is as powerful as it is inspiring: to safeguard the state's public sector, critical infrastructure, and sensitive data from the constant threat of cyber-attacks. The stakes are high—potential consequences include data breaches, service disruptions, and loss of public trust.

SOCaaS strengthens the state's cybersecurity capabilities through centralized security monitoring, utilizing cutting-edge Security Information and Event Management (SIEM) and Security Orchestration Automation and Response (SOAR) tools. This centralized approach boosts efficiency and effectiveness and delivers significant cost savings. In its inaugural year, the new SIEM platform cut costs by $1.7 million, with annual savings projected to soar to nearly $5 million. Moreover, the streamlined onboarding process has revolutionized efficiency, reducing the timeframe from 6-9 months to a mere 45-90 days.

Impact

A Vision Realized

SOCaaS represents cutting-edge innovation, with its decentralized multi-tenant SIEM architecture leveraging the power of cloud-native solutions and software-as-a-service tools.

This pioneering approach enhances scalability and reduces operational costs. By integrating automation and machine learning capabilities, SOCaaS ensures high-fidelity incident notifications and enriched data for forensic analysis and threat hunting, ultimately enabling faster, more effective threat detection and mitigation.

The project's success serves as a shining example of how a centralized approach to cybersecurity can bring significant benefits in terms of cost savings, efficiency, and improved security posture.

- **Total Customers:** Skyrocketed from 18 to 76 in just ten months.
- **Cost Savings:** SOCaaS has delivered a staggering $40 million annual cost savings to the state budget.
- **Automation and Process Improvements:** These have empowered OIS to handle the surge from 4 customers to 75.
- **Advanced Log Management Service (OIS/ALM):** Innovative log management has cut SIEM costs by 25-60%, saving the state data center around $600k annually.

76	57	$40,000,000
Total customers	New customers in 10 months	Annual cost savings

Stepping into the Future

This groundbreaking solution is dedicated to future-proofing the state's cybersecurity infrastructure against emerging threats.

The SOCaaS project is crafted for long-term sustainability, with continuous improvement efforts and regular stakeholder engagement ensuring its ongoing effectiveness. Future plans include further enhancements to the SIEM architecture, incorporating emerging technologies, and expanding the service to additional entities. The substantial cost savings, improved security posture, and enhanced service delivery justify the project's initial and ongoing investments.

SOCaaS embodies a transformative initiative that greatly enhances cybersecurity for California state public sector entities. Through innovation, collaboration, and a focus on efficiency and effectiveness, SOCaaS has established a new standard for statewide cybersecurity solutions. The project's significant impact, cost savings, and alignment with key priorities make it a deserving candidate for the NASCIO State IT Recognition Award.