CALIFORNIA
EMPLOYMENT DEVELOPMENT DEPARTMENT

Award Category: Cybersecurity
Project: Fraud Prevention
Project Dates: State Fiscal Year 2024 – 2025 - Present
Contact: Douglas Leone
Douglas.Leone@edd.ca.gov
Chief, Cybersecurity Division

EXECUTIVE SUMMARY

The California Employment Development Department (EDD) faced the critical challenge of protecting vast amounts of sensitive Californian data amidst a rapidly escalating threat landscape. Recognizing the limitations of traditional security measures, EDD embarked on a strategic initiative to build a proactive, intelligence-driven security posture.

The core idea was to establish a holistic framework encompassing a robust Security Operations Center (SOC), advanced threat detection and response capabilities Managed Detection and Response (MDR) and Extended Detection and Response (XDR), proactive fraud prevention, comprehensive device visibility, and enhanced identity proofing for critical systems managing millions of logins.

Implementation involved a strategic roadmap centered on adopting Elastic Cloud. Key phases included a rigorous technology selection process that chose Elastic for its anomaly detection, threat hunting, scalability, and cost-effectiveness; a successful migration to Elastic Cloud; the critical centralization of data from diverse sources onto the Elastic platform; the integration of AI/Machine Learning for expedited anomaly detection; the consumption of multi-layered threat intelligence; and the enterprise-wide deployment of Elastic Agent for centralized data ingestion. A strong emphasis was placed on knowledge transfer and building internal expertise.

This initiative has yielded significant positive impacts. Due to real-time visibility and AI-powered analysis, EDD has achieved enhanced threat detection and response with reduced Mean Time to Detection (MTTD) and Mean Time to Response (MTTR). Data retention and compliance have been significantly improved, meeting strict 7-year requirements and streamlining compliance efforts for over 850 billion logs through data normalization. Analyst's productivity has increased substantially thanks to Elastic's intuitive interface and AI assistance. Application performance monitoring has been strengthened, providing developers with crucial insights. Furthermore, enhanced data accessibility has fostered improved collaboration across divisions, and efforts are underway to optimize costs.

EDD is committed to maintaining and enhancing this strengthened cybersecurity posture through a dedicated internal team, continued partnership with Elastic, continuous process improvement, and integrated budget allocation. By leveraging Elastic and fostering a collaborative security culture, EDD has set a commendable standard for safeguarding sensitive information and managing risk.

IDEA

The California EDD encountered a pressing challenge: protecting sensitive information for millions of Californians, including Personally Identifiable Information (PII) and federal tax data, in an ever evolving and increasingly complex threat environment. The rise in malicious actors' capabilities highlighted the urgent need for EDD to bolster its security and risk management strategies proactively. Acknowledging the shortcomings of traditional security methods, EDD has set out to develop a holistic and integrated approach. This vision focused on establishing a robust SOC, improving threat detection and response capabilities through MDR/XDR frameworks, implementing proactive fraud prevention strategies, gaining a clear understanding of its device landscape, and enhancing identity proofing mechanisms—particularly concerning login security for critical systems like MyEDD with over 71 million logins. This initiative aimed to transition from reactive

tactics to a forward-thinking, intelligence-driven security framework, ensuring the confidentiality, integrity, and availability of vital services and data. The widespread nature of this challenge, faced by organizations managing large volumes of sensitive information across multiple sectors, underscores the significance and potential impact of EDD's approach.

IMPLEMENTATION

EDD set out on a strategic roadmap to achieve its cybersecurity vision, with Elastic chosen as a cornerstone technology. This initiative involved collaboration among key stakeholders, including the Cybersecurity Division (CSD) and potentially the Product Development Division (PDD), all under strong leadership and a spirit of teamwork.

The implementation process was conducted in several key phases:

- **Technology Selection:** After a thorough evaluation, Elastic was selected for its robust anomaly detection and threat hunting capabilities, its scalability to handle vast datasets—including meeting the challenge of 7-year data retention requirements—and its cost-effectiveness. This decision, spearheaded by CSD, required overcoming initial hesitations about adopting newer SIEM solutions.
- **Infrastructure Migration:** A significant effort was put into migrating from an on-premises technology stack to Elastic Cloud. This transition, aided by Elastic's professional services, involved creating custom dashboards and establishing efficient methods for querying and utilizing data.
- **Data Centralization:** EDD strategically unified data from diverse technologies, including Salesforce, Amazon Web Services, Microsoft, Palo Alto, and Okta, all on the Elastic platform. This centralized view of data allowed for comprehensive security monitoring and analysis.
- **AI and Machine Learning Integration**: EDD integrated Elastic's AI Attack Discovery module in Q4 2024. This step harnessed AI and machine learning capabilities to contextualize and expedite anomaly detection, thereby enhancing threat detection accuracy and lightening the manual workload in the SOC.
- **Threat Intelligence Consumption:** EDD adopted a multi-layered approach to threat intelligence, incorporating feeds from existing security vendors and collaborating with trusted external partners (such as CAL-CSIC, CDT, CMD, MS-ISAC, CHP, and Law Enforcement) while also leveraging open-source intelligence (OSINT) resources.
- **Elastic Agent Deployment:** EDD launched an enterprise-wide rollout of Elastic Agent, which provided a centralized and secure means of ingesting logs, metrics, and endpoint telemetry. This enabled remote policy management and improved scalability.
- **Knowledge Transfer and Training**: EDD strongly emphasized building internal expertise by collaborating with Elastic's professional services. Through workshops and strategy sessions, they fostered a resilient and well-rounded security team poised to tackle future challenges.

IMPACT

EDD's strategic cybersecurity initiatives, particularly the implementation of Elastic, have had a significant positive impact throughout the organization:

Enhanced Threat Detection and Response: The adoption of Elastic, featuring AI Attack Discovery and real-time visibility, has notably expedited the triage process for investigations and incident response workflows. Analysts can now more effectively correlate events across different systems, resulting in reduced Mean Time to Detection (MTTD) and Mean Time to Response (MTTR).

The integration of AI Attack Discovery in Q4 2024 has improved the speed and contextualization of anomaly identification.

Improved Data Retention and Compliance: Elastic has empowered EDD to meet its strict 7-year data retention requirements for critical information. Additionally, by utilizing the Elastic Common Schema (ECS), data normalization and parsing have become more streamlined, enhancing compliance with NIST CSF and FedRAMP frameworks.

EDD successfully manages over 850 billion logs, ensuring long-term data availability for compliance and analysis.

Increased Analyst Productivity: Elastic's user-friendly interface, swift search capabilities, and AI-powered assistance have markedly boosted analyst productivity by minimizing manual log analysis and speeding up threat investigations.

The standardized data structures through ECS enable analysts to create reusable queries and visualizations, saving time and effort.

Strengthened Application Performance Monitoring: By leveraging Elastic's Application Performance Monitoring (APM) capabilities, developers gain vital insights throughout the development process, enhancing debugging efforts and application stability.

Developers now access meaningful dashboards that deliver real-time event collection and debugging information.

Enhanced Collaboration: The accessibility of information through Elastic dashboards has encouraged more excellent teamwork across various divisions within EDD, equipping staff and management with the data they need to meet their goals.

Cost Optimization: EDD is also focused on optimizing resource allocation and improving IT efficiencies through using Elastic, making strides towards reducing cloud computing costs.

Improved Security Posture: This comprehensive approach—including enhanced threat detection, proactive monitoring, and better incident response—has significantly strengthened EDD's overall security and risk management posture, better safeguarding the sensitive information of millions of Californians.

Maintenance and Ongoing Cost:

- EDD is committed to the continuous upkeep and enhancement of its cybersecurity posture, which includes:

- **Dedicated Internal Team:** A resilient and highly skilled internal team manages the day-to-day operations and optimization of the Elastic platform.
- **Ongoing Partnership with Elastic**: EDD maintains a valuable partnership with Elastic, gaining access to expert support, workshops, and strategic advice.
- **Continuous Improvement:** EDD is dedicated to improving its security processes continuously, with plans to further utilize AI Attack Discovery and expand the use of Elastic Agent.
- **Budget Allocation**: To ensure the sustainability of these critical security functions, ongoing costs associated with the Elastic subscription, professional services, and internal resources are integrated into EDD's budget.

By strategically rolling out Elastic and fostering a collaborative security culture, the California Employment Development Department has set a remarkable standard in strengthening its security and risk management framework, offering a commendable example for other organizations facing similar challenges.