swish elastic

Case Study

Swish and Elastic enable the U.S. Coast Guard to strengthen and scale its cybersecurity program for threat detection, security incident management, and compliance.

Introduction

Executing concurrent civilian and military roles within the Department of Homeland Security (DHS), the U.S. Coast Guard (USGC) has a multi-faceted array of responsibilities. They serve as a law enforcement organization, a regulatory agency, a member of the U.S. Intelligence Community and a first responder. USCG is the principal federal agency responsible for maritime safety, security, and environmental stewardship in the U.S. ports, inland waterways, 95,000 miles of coastline and on the seas. Their mission is critical to national security.

The Problem

Executive Order (EO) 14028 is a directive to improve the nation's cybersecurity investigative and remediation capabilities. Memorandum M-21-31 was issued to address the requirements in Section 8 of the EO, specifically for logging, log retention and log management with a focus on ensuring centralized access and visibility for the highest-level enterprise Security Operations Centers (SOCs) within each agency.

The USCG's SOC had many defensive cybersecurity measures already in place but in accordance with M-21-31 needed to further strengthen threat detection, security incident management, and compliance for their 65,000+ endpoints across hundreds of locations.

Additional USCG Challenges:

- **difficulty in rapidly detecting, alerting and investigating threats**
- **proprietary code with limited configuration options**
- **out-of-date solutions unable to meet the current cybersecurity threat landscape**
- **high costs related to operations and maintenance**

> “M-21-31 defines a standard set of event logging requirements that all agencies must follow. This enable agencies to collect the same types of data consistently, making it easier to analyze and share information across agencies, one of the main goals of EO 14028.”

The Solution

Swish was awarded a contract under the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigations (CDM) program to provide the U.S. Coast Guard with advanced security information and event management (SIEM) capabilities. Swish’s deep knowledge of the Coast Guard’s SOC environment and cybersecurity expertise prompted the USCG to make the move to Elastic, a leading cybersecurity partner for active threat management and incident response through real-time data analysis and extended detection and response (XDR). Elastic’s limitless ingestion, flexible analysis, and innovative agent coupled with its open-code framework provide the USCG with a powerful weapon against advanced persistent threats.

65,000+

endpoints across hundreds of locations

Summary

Today, the status quo is not sufficient when it comes to cybersecurity. Adversaries are relentless and constantly evolving their tactics and techniques to find and exploit the smallest vulnerabilities and IT hygiene missteps. Government agencies must be continually evolving in their policies, practices, and solutions against the ever-changing security landscape. Like many government agencies, USCG saw the need to expand their security practices in accordance with M-21-31 and they needed expert and experienced partners to accomplish that. Swish, with a dedicated cybersecurity practice within the company’s Center of Excellence and Elastic, being used as part of a critical strategy for visibility into the security posture of millions of endpoints, together provide a solution that meets USCG’s requirements for an expanded cybersecurity program.

About Swish

Swish is a provider of technology solutions and engineering services to the U.S. Federal Government with a focus on high-quality outcomes for customers. Since 2006, Swish has delivered high-performance solutions and services to the Federal Government market ensuring that customer’s digital service capabilities, performance, and security exceed expectations and requirements. Swish is a Service-Disabled, Veteran-Owned and HUBZone certified Small Business.

swishdata.com

swish