IDC

Observability Case Study:

Interview with the CISO of the Asset Management Group at a Financial Asset Management Organization in the U.S.

ASSOCIATED WITH THE WHITE PAPER:

Network Intelligence and Insights: Driving Performance, Protection, and Productivity in Observability

AUTHORS:

Christopher Kissel

Mark Leary

Business Scenario

This case study focuses on the commercial real estate division of a global asset management company that includes several business divisions. Asset management for this division includes activities relevant to the safety and maintenance of property in addition to activities around preparing property for preferred insurance premium. The division also is responsible for complying with the necessary regulatory jurisdictions.

How Network and Security Operations (NOC/SOC) Are Managed

The CISO has ultimate decision-making authority for purchases and process and interestingly is responsible for data privacy for all departments within the Asset Management group. The NOC and the SOC are separate entities; however, they do share the same reporting platforms and the same KPI. From the CISO's perspective, the NOC/SOC fall under the purview of the IT department while OT - the HVAC systems, security cameras, lighting systems and so forth - are managed separately. **Read on...**

Where Observability Fits In

While there is a separation between IT and OT, the NOC/SOC operations are somewhat conventional. The CISO has set aside an organizing principle for the hundreds of properties that the company manages. For every property and division, the CISO sets up a checklist/questionnaire of 60-70 criteria. The company has a weighting system and frequently updates the internal metrics. Important metrics include protocols around proving safety in the facility, a checklist for completion of environmental, social, and governance (ESG), and inventory of software and applications. Worth noting, in cybersecurity, the internal metrics include vulnerabilities detected, mean-time-to-detect, and alerts processed.

For cybersecurity, the CISO has had a conventional EDR (Crowdstrike), SIEM (Splunk), and SOAR (Demisto, now Palo Alto Network Cortex XDR) stack with which he was very satisfied. The ARMIS OT platform is used to identify devices based on logs coming from proprietary OS. ARMIS offers visibility and support for wireless protocols such as ZigBee and BACnet that are used for short range communications especially in lighting and physical security systems. Observability is used to track anomalies to port activities and devices that need to be reset (they will make a callout to the device through the last connected port).

The CISO said that in security, 78.2% of alerts deploy a playbook which initiate an automated response. There does appear to be a difference between the first automated response and a fully automated response. The CISO reports only 30% of alerts are fully addressed through automation.

Culturally, the company has not gone the last mile in automation. Instead of forcing a multifactor authentication (MFA) request, the SOC has a 15-minute dimmer switch where if an alert is not investigated, the user is then asked to reauthenticate back onto the network.

Opportunities to Enhance Operations with a Greater Commitment to Observability

There are two counter influences within the organization. First, there are central principles and practices that guide the management of each property. However, even in this case, each property is at a different IT maturity level. Second, the network, security, and OT environments are well-tooled with redundancies. The tooling includes privilege access management, CASB, and the OT and cybersecurity stack previously described.

There are two specific places where observability can help with a better IT and security posture. Property management requires a mix of monitoring several types of devices. Even esoteric devices such as digital signage must be accounted for. An IP address observability platform based on the identification of devices through logs, network intelligence, and behaviors can help to get rogue devices under control.

Second, the CISO would like to see greater capabilities in "block and detect." The best way to do that is to receive machine-readable data from observability platforms. Enhanced session data can be used to create YARA rules. YARA rules are designed to recognize patterns of behavior in malware enabling teams to look for novel threats as well as dangers to the existing network. YARA rules can be then ported onto AV and firewalls to keep intruders out and deny employees from accessing malicious domains. At its best, observability reduces the noise between an indicator of compromise (IoC) and actionable content that can affect everything from faster detection, better forensics of past events, proactive blocking, and automated responses.

A strong observability platform is more than just logs. Logs do tell a specific story, but the context of events is as potent as the logs themselves. One example is a port override. Through an SSH command, the adversary can create an override over Port 443 showing the lowest possible encrypted session. However, perimeter tools will look to see that the session is encrypted and quit monitoring ingress/egress. It is the tracing of the session in this case that sees the attempted obfuscation.

Last and importantly, in 2023, businesses must be agile. The property management company needs technology that includes insights into DevOps environments such as Red Hat OpenShift, Docker and Kubernetes, as well as visibility into cloud and virtual environments.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200