D3 SECURITY

D3 SOAR CASE STUDY

MSSP

APAC-BASED MANAGED SECURITY SERVICES PROVIDER

40-ANALYST CYBER SECURITY INCIDENT RESPONSE TEAM

~50 CLIENT ORGANIZATIONS

THE BACKGROUND

This Asia-Pacific-based MSSP ("The Client") provides outsourced IT and managed security services to energy, finance, government, manufacturing, and telecom organizations. Its security operations center (SOC) manages day to day security operations, while its 40-analyst computer security incident response team (CSIRT) is responsible for incident remediation for approximately 50 clients.

The SOC and CSIRT teams operate from two sites, each with its own primary SIEM. The main reason for supporting multiple SIEMs is to offer flexibility to its clients.

Going into the project, The Client already had a SOAR solution in place, but it could not meet their automation, reporting and scalability needs.

THE LIMITATIONS OF THE EXISTING SOAR SYSTEM INCLUDED:

Insufficient reporting capability. The platform lacked different exportable formats and was not customizable for detailed analysis.

Could not consolidate incidents when multiple alerts were triggered at the SIEM level. The resulting duplication slowed analysts down and prevented them from seeing a complete view of the threat.

Did not support the right third-party tool and platform integrations.

Lacked enhanced playbook functionalities, especially around automation.

THE EVALUATION

D3 was selected after a head-to-head proof-of-concept evaluation against Demisto (now known as Palo Alto Cortex XSOAR).The Client ultimately selected D3 as the SOAR vendor that was best suited to achieve its project goals.

KEY ELEMENTS OF THE IMPLEMENTATION

Integrations with The Client's two SIEMs, as well as other key tools such as Palo Alto, Fortinet, Checkpoint, Meraki, Sophos, Cynet, and Darktrace

40+ incident response playbooks for SOC and CSIRT use cases

Task management based on three client subscription levels.

Automated, continuous check ins with an internal threat intelligence database

Multiple methods to build playbooks—both manual and codeless

Seven customized reports that the client previously had to create using Excel

THE SOLUTION

D3 SOAR is now at the heart of The Client's CSIRT operations, bringing automation, effective response, and detailed reporting to the MSSP. Some of the key outcomes of the project were:

CODELESS PLAYBOOKS

D3's codeless playbooks could be made quickly and easily (even by Tier 1 analysts), which increased profit margins by eliminating complex scripting procedures and empowering analysts with a codeless playbook builder.

INCREASED PROFITS

Profitability of The Client's Level 3 (Remediation/ EDR) service was greatly enhanced, in large part due to D3's integration with all three of The Client's firewalls (PAN, Fortinet, and Checkpoint).

MITRE ATT&CK

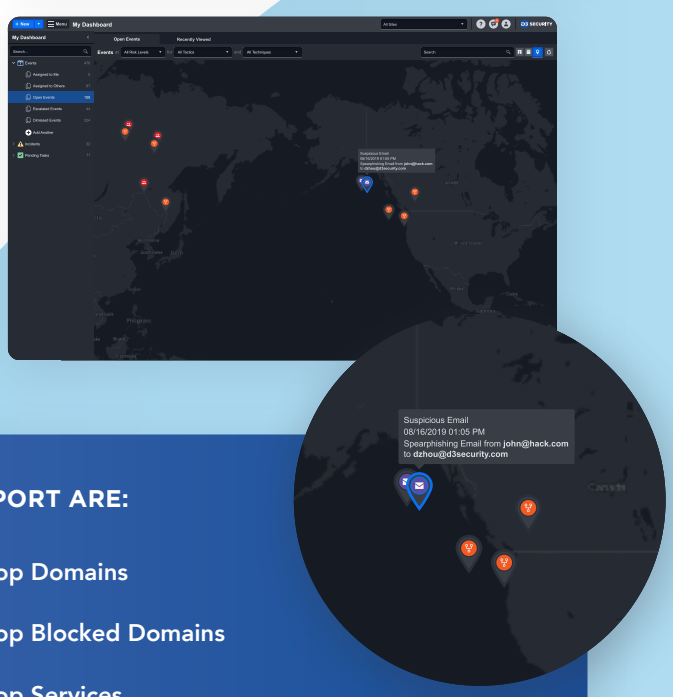
Enablement of high-value MITRE ATT&CK services based upon the increased visibility of adversaries and APT groups in D3.

AUTOMATED REPORTS

Automated metric generation and report distribution to key stakeholders, with no analyst effort required.

ENHANCED RETENTION

Enhanced data compliance capabilities, including retention of full incident documentation for six months.



THE SEVEN KEY SOC REPORTS D3 WILL SUPPORT ARE:

- Top Source/Destination IP
- Top Ports
- Geo Location of Event
- Top Alerts & Incident Types
- Top Domains
- Top Blocked Domains
- Top Services

FINAL METRICS AND COMMENTS

NUMBER OF AUTOMATED PLAYBOOKS

HOURS PER WEEK PER ANALYST SPENT ON TIER 1 TASKS

> The D3 SOAR Platform has scaled effectively to help automate and orchestrate security operations and incident response across multiple SIEMs, three teams of analysts, and dozens of blue-chip level customers."

CSIRT Leader

> With D3's metrics and reporting, we are able to define and achieve SLAs that are more relevant to our clients' business goals than simplistic, time-based SLAs

CSIRT Leader