D3 SOAR is an award-winning platform for security orchestration, automated investigation, and incident response. Think of it like connective tissue for the SOC—D3 ingests events from across the security infrastructure, assesses their criticality, and triggers incident-specific response plans.

Through its integration with Sentinel, D3 can act as the security operations hub for cloud environments or hybrid environments that include on-premise systems. D3 integrates with the Microsoft Azure stack and 260+ other security tools in order to ingest data and orchestrate response actions across any system, whether it be cloud or on-premise. Sentinel data can immediately be correlated against other sources and turned into automation-powered workflows that quickly shut down threats.

**BENEFITS**

- Improved cloud security
- Faster security actions across the Azure stack and 260+ other tools
- Deeper investigation of alerts
- Centralized security operations on a single platform

**SECOPS CAPABILITIES**

- Ingest Sentinel alerts for advanced orchestration, investigation management, and full-lifecycle incident response
- Orchestrate actions across Azure endpoint protection, cloud firewalls, and other tools to secure your cloud environment
- Intelligently correlate events and adversary techniques using the MITRE ATT&CK matrix
- Enhance journaling and case management, for handling, tracking, and reporting on the full incident response lifecycle
WHAT IS THE MITRE ATT&CK MATRIX?

The MITRE ATT&CK matrix is an evolution of the intrusion kill chain, which was developed by Lockheed Martin in 2011 to describe the steps that an adversary is likely to take during a cyber attack. ATT&CK specifically focuses on aiding post-compromise detection, and instead of phases, breaks attacks down into 12 “tactics” (what the adversary is trying to accomplish), each with a number of “techniques” (the specific methods they might use to achieve that goal). Some tactics have dozens of associated techniques, so the ATT&CK matrix acts as a deep database of adversary behavior, based on real world cybersecurity incidents and detailed research.
OPERATIONALIZE THE MITRE ATT&CK MATRIX

Uniquely among SOAR platforms, D3 incorporates the MITRE ATT&CK matrix for intelligent correlations and “intent-based” response. Because D3 can ingest alerts, query data, and orchestrate actions across security tools, using D3 effectively operationalizes ATT&CK across the entire security infrastructure.

Simply put, the process works like this:

1. When an alert is ingested (or manually pushed) into D3 from Sentinel or any other tool, D3 strips out all the indicators of compromise, such as IPs, hashes, and user IDs.

2. D3 then identifies the techniques (as defined in the ATT&CK matrix) used in the event and searches for traces of related events that may be part of the same attack, based on those indicators.

3. D3’s dashboards can be used to track instances of each ATT&CK technique and identify vulnerabilities.

By using D3 to place each event in the context of a larger kill chain, users know exactly where to look for signs of compromise and understand what the adversary is likely to do next, giving them the best chance to disrupt the attack before it succeeds. This insight into adversarial intent is why we call this methodology “intent-based response”, as opposed to “event-based response”, which treats every alert as an isolated event.
CHALLENGE

Phishing, malware, and brute force attacks can upend your security team by requiring analysts to gather contextual data and resolve the threat while dealing with screen switching, data silos, and a lack of up-to-date information. Analysts spend too much of their time completing mundane tasks, which leads to longer dwell and remediation times, plus increasing boredom and human error.

SOLUTION

By combining Sentinel for cloud-based threat detection with D3 SOAR for incident enrichment and response, you can automatically escalate real threats to incident status in D3 and assess their criticality through data enrichment and MITRE ATT&CK matrix correlation. D3 can then trigger an automated response playbook or guide human analysts efficiently through manual steps, all within a single window.

BENEFIT

When Sentinel alerts trigger D3’s automated workflows and full-lifecycle playbooks for incident response, analysts no longer have to manually coordinate dozens of triage and response tasks. Response occurs in seconds, not hours. The full incident lifecycle, including timelines, evidence, and compliance obligations, can be viewed in a single, audit-friendly platform.
CHALLENGE

More and more companies are moving their systems and servers to cloud services like Microsoft Azure, but many retain a hybrid environment, with some systems still hosted on-premise. This hybrid model creates an issue around security, because the company is left managing two sets of security tools—one in the cloud and one on-premise. During a cybersecurity incident, adversaries don’t necessarily care where your servers are. If an attacker compromises multiple user credentials, they will start moving throughout your systems with little regard for which is cloud and which is on-premise.

SOLUTION

D3 can integrate with Sentinel, the rest of the Azure stack, and the on-premise stack to create a single SecOps interface for the entire hybrid environment. Sentinel and D3 users can enrich alerts with threat intelligence, identify MITRE ATT&CK techniques, run automation-powered playbooks to respond to incidents, and much more—across cloud and on-premise systems simultaneously.

For example, in a phishing attack that resulted in compromised user credentials, an analyst using D3 could disable the user’s access in Azure Active Directory, query Sentinel for additional data, search across Office 365 mailboxes for more instances of the phishing email, and remove the malicious attachment from computers using the on-premise EDR tool.

BENEFIT

Having D3 SOAR integrated with both Sentinel and an on-premise SIEM can reduce your work—and your risk—by half. Because of the ability to monitor and act across your entire hybrid environment, you won’t lose sight of incidents that move between environments, and you’ll always be able to execute your entire response without having to switch between tools.
EASY DEPLOYMENT

D3 SOAR is a flexible solution with SAAS and on-premises deployments. Sentinel customers can leverage D3’s playbook library which automate security actions and orchestrate IR. Prebuilt integrations, playbooks and reports provide rapid time-to-value, while D3’s unique dynamic data structure ensures agility.

ENHANCED SECURITY INVESTMENTS

D3 SOAR is connective tissue for the SOC, meaning your organization’s existing technology investments can only benefit from its implementation. Feature-rich integrations and a powerful abstraction layer makes harnessing the power of all your tools easy—simply drag and drop new playbooks into reality, no coding required.

GET CONNECTED

CONNECTED—the D3 Partner Program—provides resellers, distributors, system integrators and consultants with the support they need to sell into new accounts, and enhance existing ones. D3 is used by the world’s most targeted organizations for threat investigation, incident response and case management.

Get CONNECTED today.