D3 SECURITY x zscaler™

D3 SECURITY AND ZSCALER

NEXT-GENERATION SECURITY ORCHESTRATION AND AUTOMATED INCIDENT RESPONSE

Every day, security teams are facing an overwhelming number of alerts, each with IOCs and hashes that require investigation. Analysts end up spending their time switching between tools, copying and pasting data, and manually coordinating response actions. When combined with the challenges of cloud security and the growing attack surface, analysts don't have enough time and attention to detect and resolve genuine threats.

D3 SOAR and Zscaler solve this problem by integrating cloud security tools with powerful automated incident response. When alerts come in from a SIEM or other source, D3 can automatically query Zscaler to get information about IOCs, retrieve sandbox reports, and orchestrate changes to black/whitelists. The result is a streamlined and well-informed incident response workflow, all from a single interface.

D3 NEXTGEN SOAR

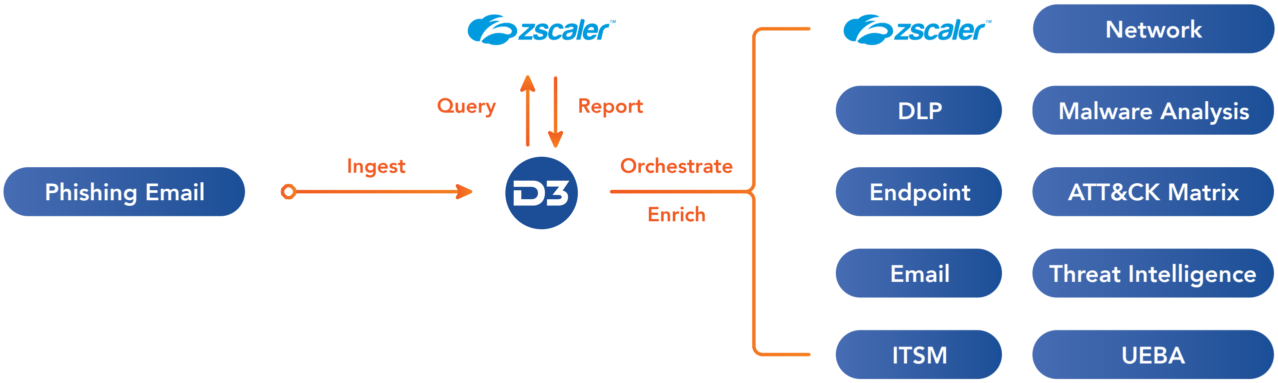
D3 SOAR helps teams to improve their security posture, quickly validate threats, and systematically disrupt the kill chain. Easily and quickly adopted by security teams of any size, D3 NextGen SOAR provides 260+ out-of-the-box integrations, a comprehensive playbook library, low-code/no-code playbook builder, automated correlation of attacker techniques, powerful link analysis, full-lifecycle case management, and detailed reporting.

BENEFITS

- Improved speed and quality of investigations through D3's integrations with Zscaler and 260+ other solutions
- Dramatic MTTR reductions through streamlined analysis and orchestration
- Streamlined workflows by managing black/whitelists directly from D3

SECURITY OPERATIONS CAPABILITIES

- Enrich security alerts with Zscaler information about IOCs, which can then be automatically integrated into D3's playbooks and incident reports
- Retrieve sandbox reports from Zscaler to identify malicious files
- Orchestrate Zscaler operations such as updating blacklists and whitelists from D3 playbooks



USE-CASE

SPEAR-PHISHING RESPONSE

CHALLENGE

Phishing is a cheap and effective way for adversaries to target your organization. Most breaches still begin with some form of social engineering because human error is inevitable. Organizations need quick and effective ways to respond to potential phishing incidents without wasting analysts' precious time.

SOLUTION

D3 can monitor phishing inboxes and create an event in D3 SOAR by pulling suspicious email content and attachment(s). The IOCs are then automatically checked against Zscaler for contextual information. Using APIs, D3 can automatically get Zscaler's sandbox detonation results for new unknown files. D3 will also search SIEM logs for suspicious network flows occurring on the involved endpoints and automatically enrich external IPs and URLs. If an IOC's reputation is malicious, a response playbook will be triggered to quarantine endpoints, block IPs and URLs, and add the IOC to a blacklist in Zscaler.

OUTCOME

By integrating D3 with Zscaler, you can create a complete phishing response workflow that automatically incorporates all the information you need to quickly separate harmless emails from threats and respond accordingly.

ABOUT D3 SECURITY

D3 Security's Next-Generation SOAR platform combines the proactive analysis of MITRE ATT&CK with rapid, end-to-end automation, orchestration and response. Using D3's advanced capabilities, SOC operators around the world have expanded the speed and scale of their security operations, while strengthening their ability to identify suspicious behaviors, conduct efficient investigations, and remediate critical threats.

ABOUT ZSCALER

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler cloud-delivered services securely connect users to their applications and cloud services, regardless of device, location, or network, while providing comprehensive threat prevention and a fast user experience. All without costly, complex gateway appliances.

D3 SECURITY

www.d3security.com

SALES CONTACT

1-800-608-0081 (Ext. 2)
sales@d3security.com

FOLLOW US