Fortinet and D3 SOAR Security Solution

Broad, integrated and automated solution for Security Orchestration and automated Incident Response across the Security Infrastructure

Security Operations and Incident Response teams are overwhelmed by the thousands of alerts that come in from numerous security tools every day. Combine this with the well-known cybersecurity skills and resources gap, and you have a perfect storm for analyst burnout and serious cyber threats slipping through undetected. Organizations need solutions that can aggregate alerts from numerous sources, help them identify which alerts represent real threats, and enable them to quickly respond.

D3 Security and Fortinet recently established a technology partnership to address the above challenges to help organizations centrally manage alerts and orchestrate rapid actions that harness the full power of the Fortinet Security Fabric.

Joint Solutions Description

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.

Robust out-of-the-box integration with all Fortinet tools provides security teams with seamless security incident and data breach response. Workflow and reporting silos, manual and repetitive work, and cost and complexity are eliminated with a security fabric that truly unifies prevention, detection, enrichment, and response.

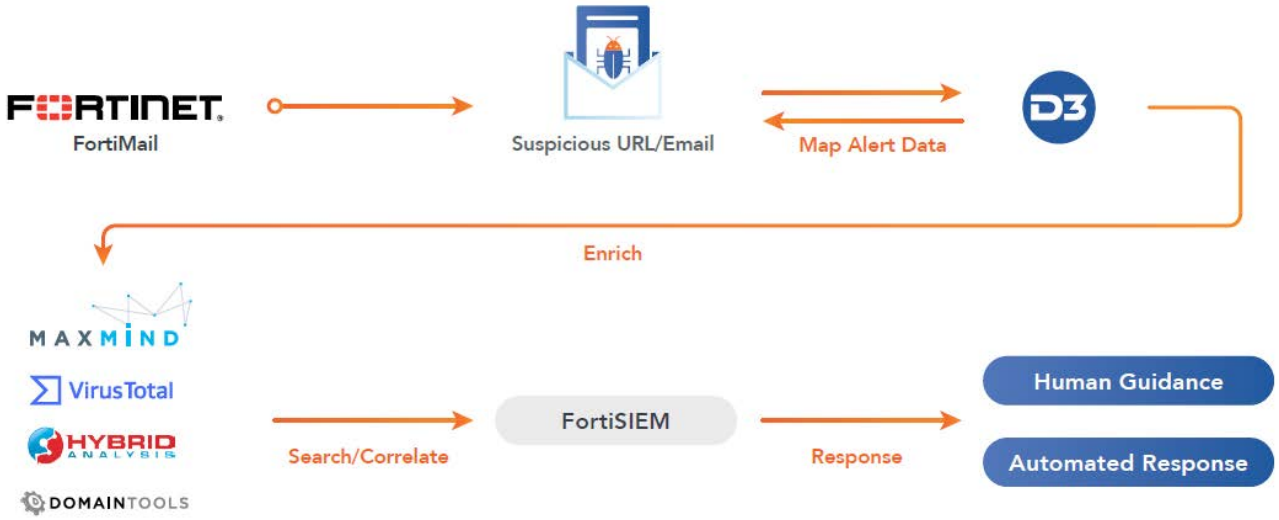
Key Features:

- 200+ integrations, 400+ actions
- Visual playbook editor
- Dynamic data structure
- Investigate case management

The functionality of the joint solution is summarized in the illustration below.

Joint Solution Benefits

- Orchestrate FortiGate's firewall policy management and IOC blacklisting with a full range of actions from across your security infrastructure
- Seamlessly integrate FortiSandbox's malware analysis and reporting outputs into adaptable incident response playbooks within D3
- Automatically ingest, triage and respond to alerts from FortiManager, FortiSIEM, FortiMail, FortiClient, FortiAnalyzer and FortiGate
- Orchestrate across Fortinet and third-party tools to improve analyst impact, efficiency, decision-making and review



Automated BEC enrichment and response

D3 SOAR

D3 SOAR—a full-lifecycle orchestration, automation, and incident/case management solution, which integrates with 200+ security tools to enact automation-powered response playbooks, enable deep investigations, and ensure compliant procedures.

Fortinet Products D3 SOAR Integrates with

- FortiGate
- FortiManager
- FortiSIEM
- FortiAnalyzer
- FortiClient
- FortiClient EMS
- FortiSandbox
- FortiMail

Joint Use Cases

- Alarm enrichment and response.
- Automated BEC enrichment and response.
- Automated network traffic investigation.

About D3 Security

D3 Security's orchestration, automation, response and case management solutions are the foundation of the world's most advanced security operations, including over 20 percent of the Fortune 500. D3 seamlessly facilitates collaboration within the security operations center and across departments through a flexible platform that streamlines incident management, orchestrates human and machine processes and documents all actions taken to assure that organizations meet industry requirements and compliance reporting standards.

Learn more at www.d3security.com

February 6, 2019 9:14 PM

123456-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2018:Collateral-Refresh-2018:Solution-Brief-Template:sb-template-gray Folder:sb-template-gray