SOLUTION BRIEF

# Fortinet and D3 SOAR Security Solution

## Broad, Integrated, and Automated Solution for Security Orchestration and Automated Incident Response Across the Security Infrastructure

### Executive Summary

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 Solution Description

D3 SOAR is an award-winning platform for security orchestration, automated investigation, and incident response. Think of it like connective tissue for the security operations center (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 following illustration.

### Joint Solution Components

- Fortinet FortiGate, FortiManager, FortiSIEM, FortiAnalyzer, FortiClient, FortiClient EMD, FortiSandbox, FortiMailvf
- D3 SOAR

### Joint Solution Benefits

- Orchestrate FortiGate's firewall policy management and indicator of compromise (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

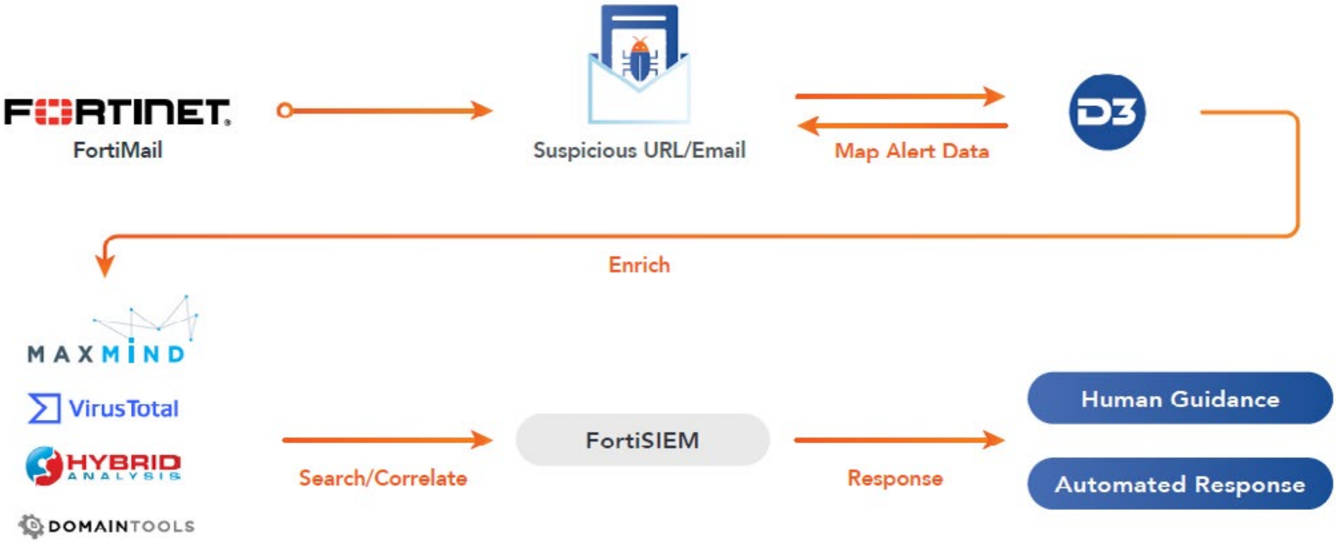

Figure 1: Automated BEC enrichment and response.

## D3 SOAR

DefendEdge, a Cyber Security company focused on building solutions that will protect your data, infrastructure, reputation, and customers against cybercrime. Our proprietary platform SiON is designed to be the most accurate and effective artificial intelligence platform in human behavior to help clients predict, detect, identify, and respond to human identity access threats in corporate networks.

### Joint Use Cases

- Alarm enrichment and response
- Automated business email compromise (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.

FORTINET

www.fortinet.com

September 20, 2021 1:45 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 3:FA-SB-nfv-d3-092021:FA-SB-nfv-d3-092021

401316-A-0-EN