

## JOINT SOLUTION BRIEF

# Recorded Future and D3 Security

## Product Overview

D3 XGEN SOAR is the industry's #1 vendor-agnostic security orchestration, automation, and response (SOAR) platform, with 500+ integrations, low-code/no-code playbooks, and automated correlation of attacker techniques. Enterprise SOCs, MSSPs, and MDR providers around the world use XGEN SOAR to strengthen their security posture, validate threats, and systematically disrupt the kill chain.

## Joint Integration Description

D3 has an extensive list of Recorded Future commands, including:

- Retrieving alert notifications
- Retrieving risk lists for vulnerabilities, domains, hashes, IPs, and URLs
- Individual or bulk lookups of vulnerabilities, domains, hashes, IPs, and URLs
- Managing analyst notes from D3

The integration eliminates manual processing and improves response time by positioning Recorded Future's Threat Intelligence, Alerts, and Analyst Notes into XGEN SOAR's Event Pipeline and automated playbooks.

## Challenges Overcome through Integration

- Manual alert enrichment and triage
- Lack of visibility into threats and vulnerabilities
- High-risk incidents that require immediate response



## USE CASES

- Seamlessly enrich events from across your security infrastructure with Recorded Future intelligence to immediately assess risk without manual lookups or screen switching.
- Query Recorded Future for vulnerability intelligence and then trigger a D3 playbook to manage outstanding vulnerabilities.
- Reduce threat detection and prevention time by up to 93% with automated response. D3 can ingest Recorded Future alerts, extract IOCs, and orchestrate the appropriate response, such as blocking IPs and URLs, scanning for malware, and quarantining affected endpoints.

## BENEFITS

- Block threats quickly and confidently
- Identify and manage risky IOCs
- Do more enrichment and triage with less SOC resources
- Improve the speed of searching and investigation
- Dramatically improve visibility of threat actors and their methods

**Integrations**

Search Integration Commands

- Case Management (19)
- Data Enrichment (44)
- Email & Messaging (28)
- Endpoint Protection (45)
- Forensics & Malware Analysis (18)
- Identity Management (9)
- ITSM (40)
- Network Security (37)
- Other (24)
- Security Optimization Platform (1)
- SIEM (50)
- Threat Intelligence (27)
- Vulnerability Scanner (9)

**Connection Parameters**

Configure what parameters are available for your connections.

Field Name	Display Name	Field Type	Is sensitive data
System Connection Parameter			

**Connections**

Add your credentials and API keys for the accounts you wish to connect.

Connection Name	Site	Status	Active	User Permissions
Site Group: By sites				

**Commands**

Set up the commands that are available for this integration.

Command Name	Display Name	Description	Implementation	Status
Group: System Commands				
checkDomainReputation	Check Domain Reputation	Check domain(s) risk level	System	Live
checkFileReputation	Check File Reputation	Check file(s) risk level based on file hash(es)	System	Live
checkIPReputation	Check IP Reputation	Check IP address(es) risk level	System	Live
checkUrlReputation	Check URL Reputation	Check URL(s) risk level	System	Live
checkVulnerabilities	Check Vulnerabilities	Check vulnerabilities' risk level	System	Live
deleteAnalystNotes	Delete Analyst Notes	Deletes a list of analyst notes by given note IDs.	Python	Live
Event Intake	Fetch Event	Return Event(s) from the platform based on specified criteria(s)	System	Live
getAnalystNotes	Get Analyst Notes	Returns a list of analyst notes by given notes ids.	Python	Live
getDomainRiskList	Download Domain Risk List	Search domain for the risk	System	Live
getHashRiskList	Download Hash Risk List	Search Hash for the risk	System	Live
getIPRiskList	Download IP Risk List	Search IP address for the risk	System	Live
getRules	Get Rules	Search Alert Rules	System	Live

+ New Investigation Dashboard Monitor Configuration Reporting And Analytics Case Management Event Playbook Viewer

**Integrations**

Search Integration Commands

Recorded Future (24)

- Check Domain Reputation (From v2 to v2)
- Check File Reputation (From v2 to v2)
- Check IP Reputation (From v2 to v2)
- Check URL Reputation (From v2 to v2)
- Check Vulnerabilities (From v2 to v2)
- Delete Analyst Notes (From v2)
- demo
- Fetch Event (From v2 to v2)

**Recorded Future** Built-In

Recorded Future predicts future events by scanning sources on the internet and extracting, measuring

**Connection Parameters**

Configure what parameters are available for your connections.

Field Name	Display Name
System Connection Parameter	

**Connections**

Add your credentials and API keys for the accounts you wish to connect.

Connection Name	Site	Status
Site Group: By sites		
StansRecFuture	Security Operations	Passed 01/13/2022

### ABOUT RECORDED FUTURE

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

### ABOUT D3 SECURITY

D3 Security's XGEN SOAR platform is the only SOAR platform that combines automation and orchestration across 500+ integrated tools with the proactive response capabilities of MITRE ATT&CK. D3's codeless playbooks automate enrichment and remediation tasks, while making it easy for anyone to build, modify, and scale workflows for security operations, incident response, and threat hunting. For more information, visit [D3security.com](https://D3security.com).