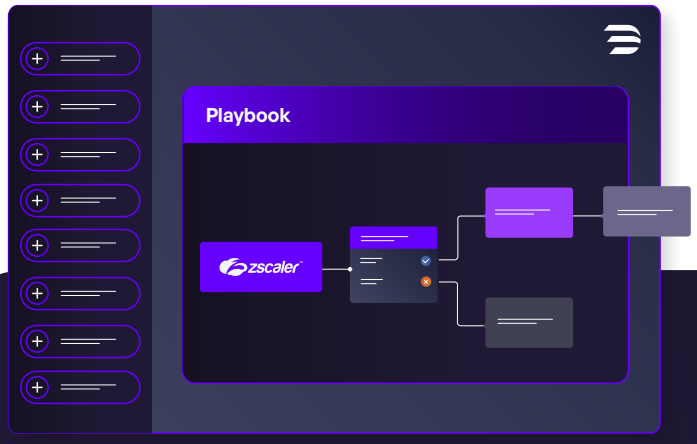
D3 x zscaler

D3 SMART SOAR — INTEGRATION WITH ZSCALER

POWERFUL AND STREAMLINED NETWORK SECURITY AUTOMATION

D3 is the leading independent provider of security orchestration, automation, and response (SOAR) software. D3 Smart SOAR integrations are expertly designed, built, tested, and maintained by D3's team, enabling users to ingest data and orchestrate lightning-fast actions across the environment.

The Zscaler Platform enables fast and secure off-network connections and local internet break-outs for all your user traffic, without appliances. Integrating Zscaler with D3 Smart SOAR enables rapid orchestration of firewall actions to protect users, endpoints, and data, no matter where they are. Threat intelligence and uncovered IOCs can be turned into Zscaler updates via automated play-books, with no screen-switching or manual data entry required.



BENEFITS

- Automate network security actions to reduce MTTR
- Ensure consistent application of policies across integrated tools
- Triage threats with D3's Event Pipeline
- Increase the quality of investigations

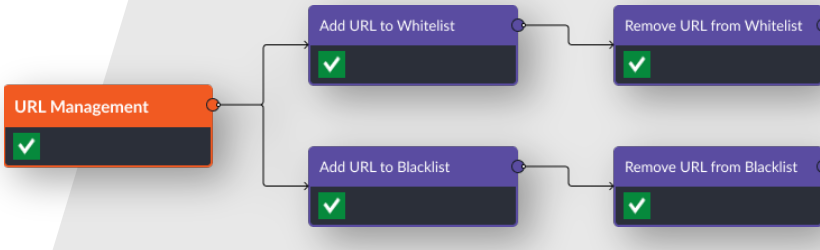
INTEGRATION FEATURES

- Orchestrate Zscaler operations from Smart SOAR playbooks, including updating Allowlists and Denylists
- Retrieve sandbox reports from Zscaler to identify malicious files
- Automate bulk updates, such as blacklisting all URLs from a threat intelligence report
- Assign URLs to Zscaler categories from Smart SOAR

D3

USE CASE #1:
Automated URL Management

The integration of Smart SOAR with Zscaler greatly simplifies the task of managing URLs. By using commands such as “Add URL To Blacklist,” “Add URL To Whitelist,” “Remove URL From Blacklist,” and “Remove URL From Whitelist,” security teams can automatically add or remove URLs from their blacklist or whitelist. This automation significantly reduces the time spent managing URLs and enhances the organization’s protection against malicious web content.

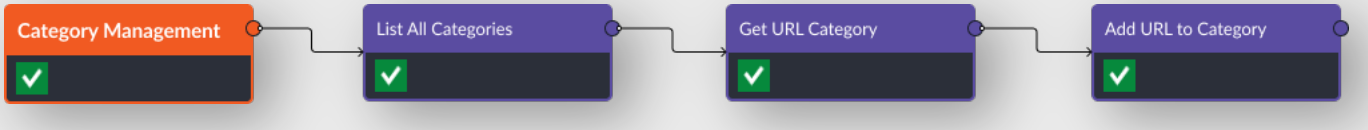


USE CASE #2:
Sandbox Analysis

When suspicious files are detected, Smart SOAR can automatically send them to Zscaler for sandbox analysis using the “Upload File to Sandbox” command. The subsequent sandbox report, obtainable with the “Get Sandbox Report” command, provides detailed insights into the file’s behavior, helping analysts determine its potential threat level.

USE CASE #3:
Comprehensive Category Management

Smart SOAR’s integration with Zscaler also simplifies the process of managing URL categories. Security teams can use the “List All Categories” command to get an overview of all existing categories. The “Get URL Category” and “Add URL to Category” commands further streamline category management by allowing analysts to add URLs to specific categories and retrieve the categories of given URLs, respectively.



USE CASE #4:
Effective Allow and Deny List Retrieval

The “Get Blacklist” and “Get Whitelist” commands provide an easy way for security teams to retrieve their complete blacklist and whitelist. This capability simplifies the review and management of these critical security assets, ensuring that all entries are up-to-date and valid.

1-800-608-0081 D3Security.com sales@D3Security.com