SOLUTION BRIEF
HYAS Protect

HYAS Protect & Splunk SOAR Integration: Automated Threat Prevention Fueled by Infrastructure Intelligence

Automate Threat Defense with Real-Time Verdicts from HYAS Protect

Speed matters in cybersecurity. The faster you can detect, assess, and respond to emerging threats, the stronger your defense posture. With HYAS Protect integrated into **Splunk SOAR**, security teams can now automate domain-based verdict lookups and threat response actions using authoritative, infrastructure-derived intelligence — without analyst intervention.

HYAS Protect brings a proactive layer of DNS threat protection directly into your SOAR playbooks. By assessing domains and infrastructure in real time, assigning reputational verdicts, and identifying potentially malicious behavior based on communication patterns, HYAS Protect enables security teams to take decisive, automated action — all at machine speed.

This integration turns Splunk SOAR into a fully automated threat prevention engine, using HYAS Protect verdicts to triage, block, and escalate threats across your entire environment.

> “With HYAS Protect integrated into Splunk SOAR, security teams can now automate domain-based verdict lookups and threat response actions using authoritative, infrastructure-derived intelligence.”

Key Benefits of the Integration

Real-Time Verdict Lookups
HYAS Protect enables your SOAR workflows to automatically assess domains, IPs, and other infrastructure in real time. Every query returns a detailed reputation verdict, helping you identify high-risk threats and respond instantly.

Automation-Ready Threat Intelligence
HYAS Protect verdicts are generated based on dynamic, multi-variant communication pattern analysis — ensuring your SOAR system is operating on the most current, accurate infrastructure intelligence available.

Accelerated Playbook Execution
Eliminate the need for manual lookups and decision-making delays. HYAS verdicts can be used to trigger conditional actions in Splunk SOAR, streamlining workflows and cutting response time.

Preemptive Protection
With infrastructure-focused intelligence embedded into your SOAR playbooks, you can block threats earlier — before damage occurs — reducing risk across your organization.

Supported HYAS Protect Actions in Splunk SOAR

The HYAS Protect app for Splunk SOAR includes enrichment and lookup actions that can be integrated directly into automated workflows or run manually as part of investigations:

- **Query Domain Verdict**
- **Query IP Verdict**
- **Query Nameserver Verdict**
- **Query FQDN Verdict**

Each action retrieves real-time threat intelligence from HYAS Protect, providing reputation scores, risk classifications, and context to drive faster, more confident decisions.

Example Use Cases

Automated Alert Triage

Use HYAS Protect verdicts in your SOAR playbooks to automatically enrich indicators from incoming alerts and escalate or suppress them based on threat classification.

Malicious Domain Blocking

Create playbooks that automatically block domains with negative verdicts by updating firewall or DNS policies — reducing the risk of successful C2 callbacks or phishing.

Conditional Escalation

Use HYAS verdict results to trigger specific playbook branches. For example, escalate only if a domain is rated high risk, or notify analysts when a verdict is unknown or suspicious.

IOC Investigations

Leverage manual lookup actions within the SOAR console to quickly check the reputation of domains, IPs, or nameservers discovered during threat hunting or incident response.

How to Get Started

1. Download the App

Find the HYAS Protect App for Splunk SOAR on Splunkbase.

2. Install & Configure

Install the app and configure your HYAS Protect API credentials within your Splunk SOAR environment using the built-in setup instructions.

3. Build Your Playbooks

Integrate HYAS Protect verdict actions into your automated workflows to enhance triage, enrichment, and response across your organization, defending against threats.

About HYAS

HYAS is the world's premier provider of infrastructure intelligence, enabling organizations worldwide with unparalleled visibility, protection, and the necessary proactive intelligence to address cyber attacks, fraud, and all forms of digital risk. Independently tested with proven efficacy, HYAS Protect delivers business resiliency against all forms of cyber attacks, regardless of the attack vector or how the organization was breached.

Want to see it in action?
Contact us at info@hyas.com or visit www.hyas.com to learn more or schedule a demo.

HYAS Products

HYAS security solutions provide the visibility and observability needed to stay in control of your environment. HYAS solutions are easy to deploy, easy to manage, and integrate seamlessly into any security stack.

PROTECTIVE DNS

HYAS Protect

Protective DNS

Our protective DNS solution combines authoritative knowledge of attacker infrastructure and domain-based intelligence to proactively block malicious communication used by cybercriminals to conduct phishing, ransomware, and other forms of cyberattacks.

Explore HYAS Protect →

HYAS Protect
Executive Dashboard
Traffic Volume by Source Type
Protection Events by Type
Protection Events across Source Types

THREAT INTELLIGENCE & INVESTIGATION

HYAS Insight

Threat Intelligence & Investigation

HYAS Insight allows you to rapidly discover and investigate any IOC and related indicators. Identify and map out the complete cybercriminal campaign architecture and take a proactive stance against future attacks.

Explore HYAS Insight →

Recent Malware Infrastructure
Daily Detonation Volume by Malware Family
Distribution by Top Malware Tags
Distribution by Top C2 ASN Countries
12161
Total

Contact Us For a Demo

hyas.com/contact

HYAS

Protecting Businesses and Solving Intelligence Problems Through Detection of Adversary Infrastructure and Anomalous Communication Patterns

HYAS is a world-leading authority on cyber adversary infrastructure and communication to that infrastructure. HYAS is dedicated to protecting organizations and solving intelligence problems through detection of adversary infrastructure and anomalous communication patterns.

We help businesses see more, do more, and understand more in real time about the nature of the threats they face. HYAS turns meta-data into actionable threat intelligence, actual adversary visibility, and protective DNS that renders malware inoperable.

HYAS.COM / INFO@HYAS.COM
DUNS #24-735-0333