Splunk

Detection Strategy Guide

June, 2025

Product Overview

Splunk's analytics-driven SIEM also includes real-time security monitoring, advanced threat detection, forensics, and incident management. Splunk Enterprise Security (ES) is a SIEM that provides insight into machine data generated from security technologies. It streamlines all aspects of security operations and is suitable for organizations of all sizes and expertise. Adaptive Response is both an initiative and a framework within Splunk Enterprise Security that connects a community of security vendors to improve cyber defense strategies.

Detection Strategy for SIEM Integrations

Detection

SIEM technology provides us with a helpful detection "backstop" for event telemetry. The detections are not authored by us, so how we ingest and action on the SIEM's alerts depends on the SIEM's category.

This SIEM integration is categorized as supporting both **out-of-the-box (OOTB) detection rules** and **custom detection rules**. This means we may leverage either OOTB or custom rules to map the SIEM alerts to our own ingestion criteria.

Your OOTB and custom rules are both subject to our evaluation and will be accepted based on:

1. **Fidelity** - the detection rule should have an alert volume that suggests high fidelity (for example, an average weekly alert volume less than 10 generally suggests the rule has high fidelity)
2. **Redundancy** - the detection rule name, description, and query should not duplicate (or suggest a duplication of) alerts that would surface through a direct API integration with a non-SIEM technology
3. **Evidence** - the detection rule must provide us with an adequate number of artifacts to action upon (two or fewer artifacts suggests insufficient information for our SOC analysts)
4. **Scope** - the detection rule name, description, and query must align with your service and should not be written for a different category of service

If we are unable to support your custom rule because it does not meet the criteria above, we will let you know so that you can make modifications and resubmit it to us.

For accepted custom rules, we will provide you with a report that details our projected level of support. Contact your Sales or Support rep for more details.

Response

SIEM telemetry provides additional information that can be useful for us to disposition alerts. With the exception of investigative-only SIEMs, we will follow our normal event triage process and create an Expel Alert that is sent to our SOC analysts for analysis. We may also run queries against your SIEM logs to search for additional types of data, which we use to enrich our alerts with additional context.

What We Support for Splunk

To see a comprehensive list of the most up-to-date SIEM rules and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for Splunk, ask your Sales or Support rep for the most recent download (not all SIEM rules are visible on the Detections page in Workbench).

Splunk detection rules support	Yes.
Detection rules written by Expel	No. Expel does not write any detection rules for SIEM integrations.
Custom rules support	Yes.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ List sources ■ Query Logs
Hunting support	Yes. Hunting is available for this integration to customers who purchase this option. Contact your Sales or Support rep for help understanding the hypotheses and objectives for each hunting technique. For a full list of techniques by integration, see Hunting Techniques in the Help Center.

Additional Details and Common Questions

Console Access

A SIEM alert does not typically include all of the contextual timeline activity surrounding the event of interest. Because this integration does not allow us to get all necessary data via the API, we will ask you for a certain level of console access during onboarding. Granting it is optional, but is strongly recommended.

The level of access that we require is meant to support essential triage and research activities, and to help us determine the vector and extent of attacker activity for an identified threat. At minimum, we will ask for visibility into alert data, timeline events recorded, and live response/real time response shell (if applicable).

Historic Volume

We use historic volume to determine projected SIEM alert volume, which helps us decide whether or not a particular detection is appropriate to send to our SOC. We target 30 days as the ideal period of time to check on volume, and two weeks as the minimum. This gives us the confidence we need to properly evaluate incoming SIEM alerts in a way that does not flood the SOC with benign activity.

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain SIEM alerts as needing an immediate verification or notification, and bypasses the normal internal event triage process. The alerts subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.