Elastic Security

Detection Strategy Guide

June, 2025

Product Overview

Elastic Security is a security information and event management (SIEM) solution built upon the Elastic Stack (Elasticsearch, Logstash, Kibana). It provides a centralized platform for collecting, analyzing, and visualizing security data, which enables organizations to detect, investigate, and respond to cyber threats in real-time. Elastic Security offers features like automated threat detection, correlation rules, and machine learning for improved security insights.

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 **out-of-the-box (OOTB) detection rules**. This means we leverage your SIEM's OOTB rules to map the SIEM alerts to our own ingestion criteria, but we do not yet support any custom rules you may have in place.

OOTB rules are still 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

While some vendor technologies are still subject to threshold levels of alerting, some libraries of OOTB rules have already been reviewed and are promoted to Expel Alerts at severity levels commensurate for the projected balance of severity, volume/occurrence, and impact. 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 Elastic Security

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 Elastic Security, ask your Sales or Support rep for the most recent download (not all SIEM rules are visible on the Detections page in Workbench).

Elastic Security detection rules support	Yes.
Detection rules written by Expel	No. Expel does not write any detection rules for SIEM integrations.
Custom rules support	No.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query Logs ■ Query User ■ Query IP ■ Query Domain ■ Query Host ■ Elastic Triage
Hunting support	No. Hunting is not currently available for this integration.

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.

Use Cases Not Supported

Use Case	Description	Reason
AWS detections	Elastic AWS Detections	These detections are being indexed. We have a direct poller with AWS to provide coverage for your AWS environment.