Logz.io

Detection Strategy Guide

July 2025

Product Overview

Logz.io is a cloud-native observability platform that helps businesses monitor and secure their applications and infrastructure. It combines open-source tools like the ELK Stack (Elasticsearch, Logstash, and Kibana) and Grafana to provide a unified platform for log management, metrics monitoring, tracing, and security analytics.

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 **investigative-only**. This means no alerts from the SIEM are ingested, but the SIEM can still be used by us for investigation telemetry. Therefore we strongly recommend you set up this integration in Workbench to increase the available investigative support.

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 Logz.io

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

Logz.io detection rules support	No, this SIEM integration is categorized as investigative-only.
Detection rules written by Expel	No. Expel does not write any detection rules

	for SIEM integrations.
Investigative support through Workbench	Yes.
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.