Sublime Security

Detection Strategy Guide

August 2025

© 2025 Expel, Inc. CUSTOMER SENSITIVE - DISCLOSURE MUST BE AUTHORIZED.

Product Overview

Sublime Security provides a modern, programmable email security platform. It allows security teams to write their own custom detections as code to protect against sophisticated phishing and business email compromise (BEC) attacks that bypass traditional security controls.

Expel's MDR for Email integration with Sublime Security will ingest alerts generated by the Sublime platform that have been marked as Unreviewed by Sublime. We will apply our own detection logic and correlation engine to these alerts, as well as leverage Sublime's built-in email analysis tools, investigating potential threats and escalating confirmed malicious activity for remediation. This allows you to leverage Sublime's powerful, customizable detection capabilities with Expel's 24/7 monitoring and response.

Detection Strategy for Email Integrations

Detection

Expel integrates directly with email security providers and uses their data to quickly identify and investigate email and identity-based attacks to:

- generate Expel alerts for investigation
- provide enriched context to a threat
- offer decision support for incident scoping and severity identification

Expel consumes email security provider events through a mix of raw log analysis and security alert processing, which pass through our detection engine to identify signs of post-exploitation activity. When a threat is detected, our automated response bot takes action by enriching evidence fields with first- and third-party threat intelligence. Additional bot actions query a wide span of technologies in order to directly arm analysts with key pieces of investigative information and related events.

Email security providers do not provide full-body email text to Workbench analysts, but rather the alert data provided by the email security providers' devices. Full-text analysis of user-submitted emails is offered via Expel's Managed Phishing service offering. When events are promoted to Expel alerts, additional workflows are used to query to enrich the event with context.

© 2025 Expel, Inc. CUSTOMER SENSITIVE - DISCLOSURE MUST BE AUTHORIZED.

Response

Email alerts are useful to identify and mitigate email threats such as phishing, business email compromise (BEC), and malware. Additionally, telemetry from other integrations with Expel is used to correlate activity across the kill chain to paint a more comprehensive picture of an attack beyond the email threat surface. For example, for an onboarded EDR or network security device, Expel can correlate the observation of a malicious attachment in the email security provider with the downloading and execution of that attachment in these integrations. If no other integrations are onboarded, analysts will use the context from the alert as well as Expel-internal enrichment sources (file/IP/URL lookups) to make the best determination of an alert.

To learn more about our overall approach to detection strategy, see About Detection Strategy in the Help Center.

What We Support for Sublime Security

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for Sublime Security, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ Sublime Security Defend
Supported platforms	■ Sublime Security Defend
Supported event log sources	■ Flagged and unreviewed message groups containing rules at low, medium, high, or critical severity
Sublime Security detection rules support	Yes.
Detection rules written by Expel	Yes.
Auto remediations	Yes. Expel supports automatic execution of some remediation actions for this integration when you follow our setup guide to update the permissions in your vendor device, and then enable the auto remediation in Workbench. The available auto remediations for this integration include:

© 2025 Expel, Inc. CUSTOMER SENSITIVE - DISCLOSURE MUST BE AUTHORIZED.

	■ Remove Malicious Email To enable auto remediations for your environment, see Enable an Auto Remediation in Workbench in the Help Center.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query Raw Logs ■ Retrieve Rules ■ Message Insights ■ URL Analysis
Hunting support	No. Hunting is not currently available for this integration.

Additional Details and Common Questions

Console Access

A vendor 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.

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).

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events 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

© 2025 Expel, Inc. CUSTOMER SENSITIVE - DISCLOSURE MUST BE AUTHORIZED.

action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.

© 2025 Expel, Inc. CUSTOMER SENSITIVE - DISCLOSURE MUST BE AUTHORIZED.