Sublime connector for OpenCTI

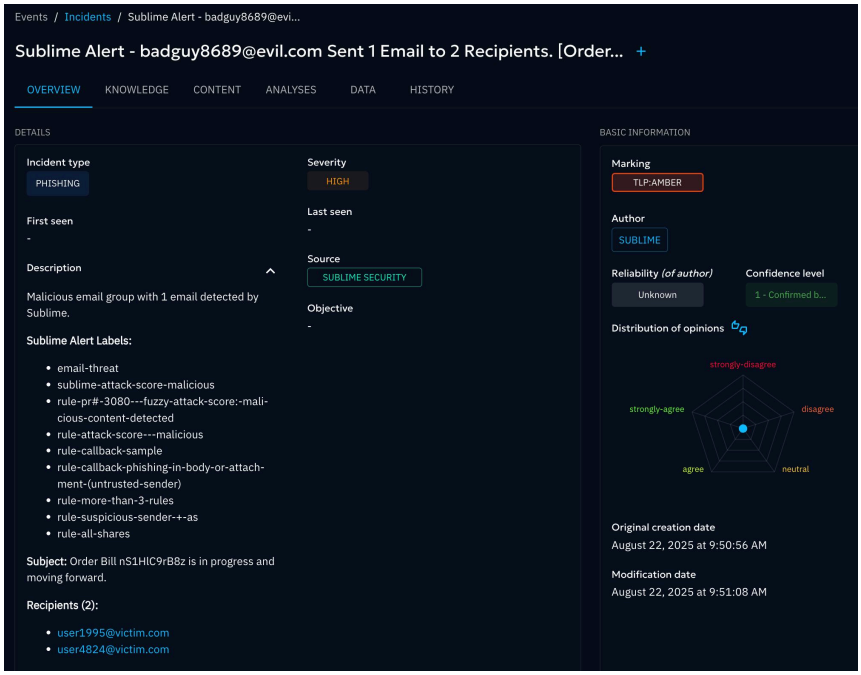
With Sublime and OpenCTI working together, security teams gain what matters most: clarity, context, and control over the threats targeting their organization.

Email threats don't stay in the inbox

Attackers use email as an entry point and then move laterally to exfiltrate data or deploy malicious payloads. Security teams that manage email detections in isolation can't answer these questions:

- **Are these malicious emails part of a broader campaign targeting multiple entry points?**
- **Do these indicators appear in endpoint, network, or other telemetry?**
- **Are there overlaps with known adversary infrastructure or publicly disclosed attacks?**

Without connecting email signals to the broader security stack, teams are left doing manual data correlation and attackers are given room to hide.



Sublime email threat intelligence + OpenCTI

The Sublime connector for OpenCTI feeds email threat intelligence directly into your centralized threat intelligence platform, where it correlates with existing security telemetry, like network logs, endpoint data, SIEM alerts, and threat feeds. This creates a complete, contextualized view of threats targeting your organization, without manual work.

© 2026 Sublime Security, Inc. All rights reserved

Enrich, correlate, and operationalize email data

Sublime → OpenCTI

Sublime continuously detects and analyzes malicious email activity, extracting indicators and metadata that's automatically ingested into OpenCTI for enrichment and correlation.

OpenCTI → security stack

With all threat intelligence centralized in OpenCTI, organizations can operationalize insights across their environment to feed detections into SIEMs, SOAR platforms, EDR tools, and other security controls.

STIX2 export format	100% automated ingestion	OpenCTI6.9.2+ LOTS-based QR attacks	Zero LOTS-based QR attacks

The power of unified intelligence

Centralized email intelligence

Sublime detections are automatically ingested into OpenCTI, enriching your threat intelligence platform with high-fidelity email threat data.

Automated indicator sharing

IOCs like URLs, domains, IP addresses, email addresses, and attachment hashes are exported in STIX2 format and immediately ingested for correlation.

Cross-platform correlation

Email-based threats can be analyzed alongside endpoint telemetry, network logs, SIEM alerts, and external threat feeds, enabling deeper investigation and faster response.

Expanded threat visibility

Security teams gain a unified view of campaigns spanning multiple attack vectors – not just email.

Sublime + OpenCTI gives you the full security picture so attackers have nowhere to hide.

Start using the Sublime connector for OpenCTI today:
https://hub.filigran.io/cybersecurity-solutions/open-cti-integrations/sublime

Book a live demo to see it in action: https://sublime.security/demo

© 2026 Sublime Security, Inc. All rights reserved