

securonix SYNQ

TURN THREAT INTEL RESEARCH INTO RESPONSE-READY INTELLIGENCE WITHOUT BREAKING ANALYST FLOW.

Executive Summary

Securonix SynQ eliminates the friction between threat research and operational action. By embedding intelligence extraction, enrichment, and investigation workflows directly into the browser, SynQ helps security teams move from research to decision in minutes by improving analyst efficiency, accelerating response, and strengthening organizational readiness.

Securonix SynQ ensures threat intelligence doesn't stall in tabs, notes, or inboxes. Every insight becomes actionable, traceable, and reusable, supporting a SOC that is both Breach Ready and Board Ready.

The Customer Challenge

Research is fast.

Operationalization is not.

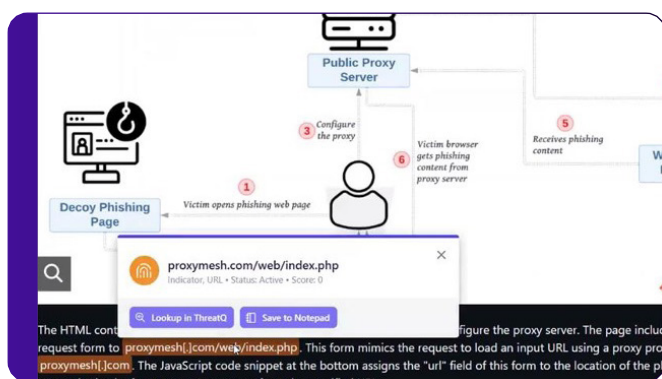
Security teams consume massive volumes of threat research every day—but turning that information into action is slow, manual, and inconsistent.

The Impact:

- ✘ Analysts lose hours to copy/paste workflows
- ✘ Intelligence quality varies by analyst and tool
- ✘ Context is lost between CTI, SOC, and IR teams
- ✘ Leadership lacks visibility into intelligence-driven decisions

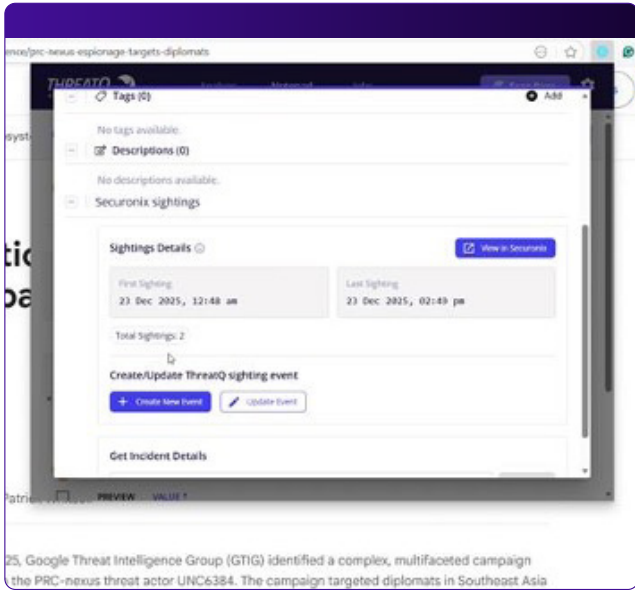
The result is delayed response, duplicated effort, and avoidable risk.

Analysts waste hours copying indicators from blogs, reports, and internal notes into security tools only to repeat the same lookups, enrichment, tagging, and relationship mapping across multiple systems. This drags investigations, splinters collaboration, and pushes critical decisions out. Now is the time to unify and automate this workflow to move teams from intake to insight in minutes, not days.



The Solution

Securonix SynQ brings ThreatQ context directly into your browser workflow by automatically extracting indicators and TTPs from the page you're viewing, then letting you enrich and operationalize them in bulk. Securonix SynQ correlates your findings into ThreatQ Investigations, so your research becomes decision-ready intelligence, while also providing visibility into threats within the customer's Securonix environment, including historical lookups to find evidence of prior sightings.



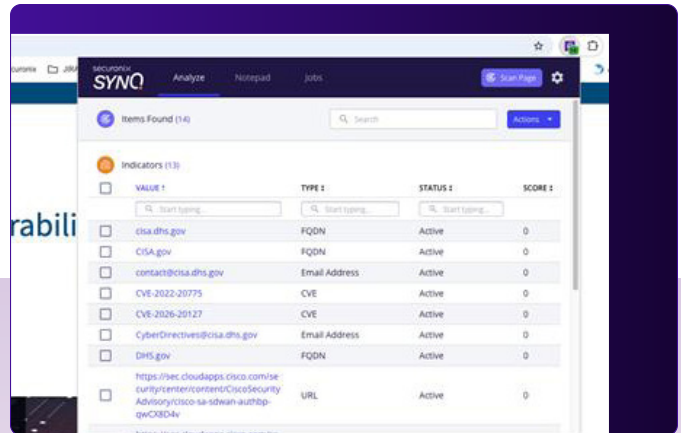
Core Business Value and Benefits

- ✔ **Less busy work, more consistency**
Bulk tagging, enrichment, and imports cut copy/paste and standardize capture.
- ✔ **Faster, higher-confidence decisions**
Scoring and provenance surface signal, reduce noise, and speed prioritization.
- ✔ **Better collaboration and continuity**
ThreatQ sync preserves relationships and timelines across SOC, CTI, and IR.
- ✔ **Stronger operational memory and reuse**
Link indicators and reports to build reusable, searchable intelligence for retrospectives.
- ✔ **Clearer visibility into work in progress**
Job tracking shows status and results, boosting auditability during fast investigations.

Core Capabilities

Auto-Extraction and Highlighting: Scan web pages (or background scan) to surface key entities like IOCs, threat actors, and ATT&CK techniques and tactics for quick validation.

- ✔ **Hover Context Preview:** Hover highlighted items to see ThreatQ score, status, sources, tags, and related events without leaving the page.
- ✔ **Bulk Lookups and Actions:** Run bulk IOC lookups and apply bulk actions like import, tagging, adding attributes, and enrichment in one pass.
- ✔ **Threat Visibility & Historical Evidence:** Visibility into security threats within the customer’s Securonix environment, including historical lookups to identify and validate prior sightings/evidence.
- ✔ **Inline Indicator Management:** Update indicator details like status and score, attributes, tags, sources, and descriptions directly in the extension without tab-hopping.
- ✔ **Investigation and Report Operationalization:** Capture reports and artifacts, relate entities, and sync into ThreatQ Investigations for collaboration and structured intelligence.



Why Securonix SynQ?

BREACH READY. BOARD READY.

SynQ is not another browser tool. It is an extension of the Unified Defense SIEM—bridging open-source research, curated intelligence, and SOC execution.



Book a demo and turn insight into response. Faster decisions. Fewer false positives. All within a Unified Defense SIEM, powered by Agentic AI.

Visit securonix.com or contact sales@securonix.com.