

# Chronyx Threat Timeline

## Buyer Proof Summary

Public-safe product proof pack generated from uploaded Cybstyx Phylaxis master guide and package inspection data. This is source-based buyer collateral, not a live-customer runtime certification.

Event lake, threat timeline, correlation, case workflow, and investigation console.

Category	Native SIEM-lite / Event Lake
Responsibility	Organize logs, alerts, findings, and investigation milestones into reviewable timelines and cases.
Standalone boundary	Timeline analysis continues locally; SecOwl outage only affects central visibility and command.
Authentication	Local RBAC with MFA; optional Eidon SSO; collector or service authentication for event intake.
Linked applications	Optional SecOwl adapter, Tekmerion evidence, Keraunix response, and event sources such as Phylax, Orama, Phragma, Dolion, Nyxara, and Topora.

### Source Evidence Snapshot

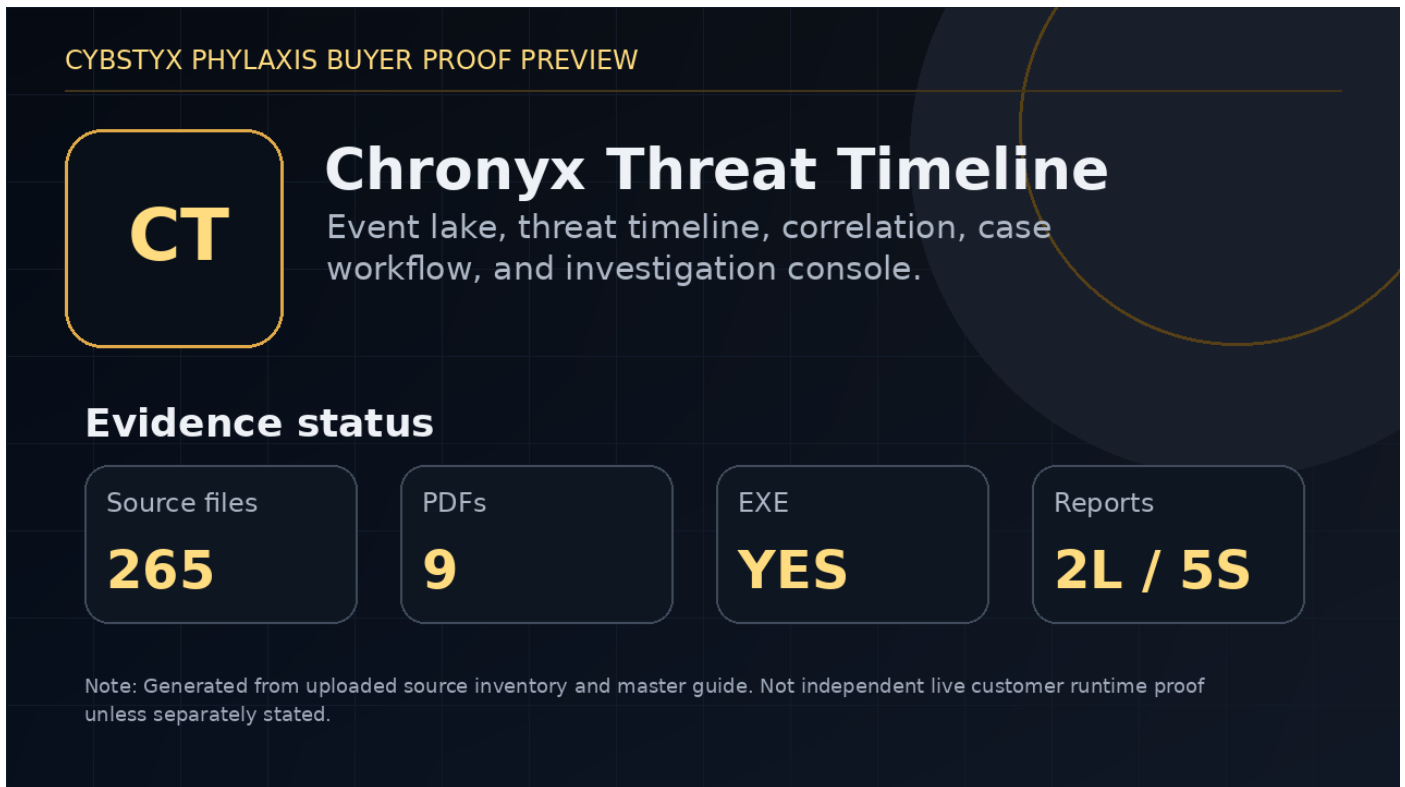
Source files inspected	265
PDF documents in package	9
Executable evidence found	YES
Live/self-test reports referenced	2 live / 5 self-test
Language profile	Python, JavaScript, Go, Java, PowerShell
Database/configuration modes	sqlite-native-local, postgresql-schema-ready

### Core modules

<ul style="list-style-type: none"><li>• Event intake and collectors</li><li>• Syslog, file, and CSV import</li><li>• Detection rules and IOC watchlist</li><li>• Attack story builder</li><li>• Case management, retention, and executive reports</li></ul>
---

## Visual Proof Preview

The image below is a generated buyer proof preview based on the uploaded source inventory and master guide. Use the separate contact sheet and MP4 preview for visual sales review.



Recommended buyer usage: share this pack as a source-backed capability and readiness brief. For production procurement, pair it with a live demo, customer environment scope, licence term, deployment checklist, and signed acceptance test.