Threat intel operationalized

So much intel, how to make it actionable?

Organizations often consume an average of 5-7 threat intelligence and malware feeds, then attempt to apply them to multiple systems used by different teams to try and thwart attacks. This has led to fragmentation and hindered the ability of security teams to leverage intelligence effectively, creating gaps or bottlenecks to assess and address an attack. As a result, organizations face difficulties in making threat intelligence actionable and operational across their entire organization. This all hampers timely prevention, detection, and response to threats, leaving organizations vulnerable and unaware of an attack taking place.

Stairwell's game-changing approach

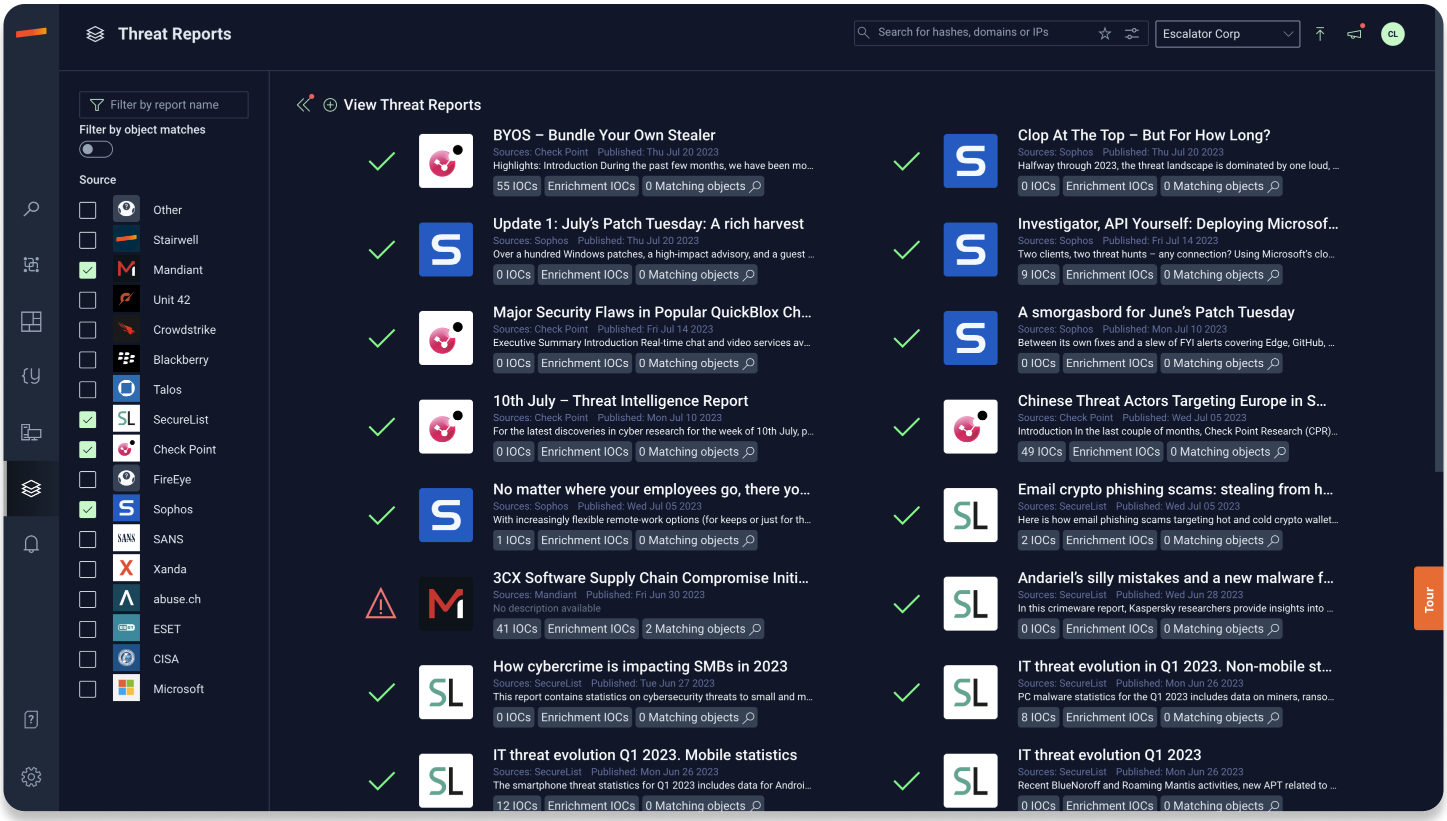
Stairwell revolutionizes the operationalization of threat intel by ingesting and storing every executable or executable-like file written to disk in perpetuity. Stairwell provides organizations with unprecedented analysis and threat detection capabilities at the source – files.

© 2023 Stairwell, Inc. All rights reserved

Threat intel operationalized

This unique approach allows Stairwell to automatically analyze indicators of compromise, an entire threat feed, or multiple threat feeds within seconds, providing immediate insights into the presence of threats in an organization's environment, past or present.

The analysis is done on a continuous basis. Every time a new threat feed or report is ingested, your security team is able to automatically ascertain if your organization has been impacted by new forms of malware or any variants. This is done by our cloud-based neural network, which is able to quickly discover both known and unknown variants within your environment.



Source

- ☐ Other
- ☐ Stairwell
- ☑ Mandiant
- ☐ Unit 42
- ☐ Crowdstrike
- ☐ Blackberry
- ☐ Talos
- ☑ SecureList
- ☑ Check Point
- ☐ FireEye
- ☑ Sophos
- ☐ SANS
- ☐ Xanda
- ☐ abuse.ch
- ☐ ESET
- ☐ CISA
- ☐ Microsoft

✓ **BYOS – Bundle Your Own Stealer**
Sources: Check Point Published: Thu Jul 20 2023
Highlights: Introduction During the past few months, we have been mo...
55 IOCs | Enrichment IOCs | 0 Matching objects

✓ **Update 1: July's Patch Tuesday: A rich harvest**
Sources: Sophos Published: Thu Jul 20 2023
Over a hundred Windows patches, a high-impact advisory, and a guest ...
0 IOCs | Enrichment IOCs | 0 Matching objects

✓ **Major Security Flaws in Popular QuickBlox Ch...**
Sources: Check Point Published: Fri Jul 14 2023
Executive Summary Introduction Real-time chat and video services av...
0 IOCs | Enrichment IOCs | 0 Matching objects

✓ **10th July – Threat Intelligence Report**
Sources: Check Point Published: Mon Jul 10 2023
For the latest discoveries in cyber research for the week of 10th July, p...
0 IOCs | Enrichment IOCs | 0 Matching objects

✓ **No matter where your employees go, there yo...**
Sources: Sophos Published: Wed Jul 05 2023
With increasingly flexible remote-work options (for keeps or just for th...
1 IOCs | Enrichment IOCs | 0 Matching objects

⚠ **3CX Software Supply Chain Compromise Initi...**
Sources: Mandiant Published: Fri Jun 30 2023
No description available
41 IOCs | Enrichment IOCs | 2 Matching objects

✓ **How cybercrime is impacting SMBs in 2023**
Sources: SecureList Published: Tue Jun 27 2023
This report contains statistics on cybersecurity threats to small and m...
0 IOCs | Enrichment IOCs | 0 Matching objects

✓ **IT threat evolution Q1 2023. Mobile statistics**
Sources: SecureList Published: Mon Jun 26 2023
The smartphone threat statistics for Q1 2023 includes data for Androi...
12 IOCs | Enrichment IOCs | 0 Matching objects

✓ **Clop At The Top – But For How Long?**
Sources: Sophos Published: Thu Jul 20 2023
Halfway through 2023, the threat landscape is dominated by one loud, ...
0 IOCs | Enrichment IOCs | 0 Matching objects

✓ **Investigator, API Yourself: Deploying Microsof...**
Sources: Sophos Published: Fri Jul 14 2023
Two clients, two threat hunts – any connection? Using Microsoft's clo...
9 IOCs | Enrichment IOCs | 0 Matching objects

✓ **A smorgasbord for June's Patch Tuesday**
Sources: Sophos Published: Mon Jul 10 2023
Between its own fixes and a slew of FYI alerts covering Edge, GitHub, ...
0 IOCs | Enrichment IOCs | 0 Matching objects

✓ **Chinese Threat Actors Targeting Europe in S...**
Sources: Check Point Published: Wed Jul 05 2023
Introduction In the last couple of months, Check Point Research (CPR)...
49 IOCs | Enrichment IOCs | 0 Matching objects

✓ **Email crypto phishing scams: stealing from h...**
Sources: SecureList Published: Wed Jul 05 2023
Here is how email phishing scams targeting hot and cold crypto wallet...
2 IOCs | Enrichment IOCs | 0 Matching objects

✓ **Andariel's silly mistakes and a new malware f...**
Sources: SecureList Published: Wed Jun 28 2023
In this crimeware report, Kaspersky researchers provide insights into ...
0 IOCs | Enrichment IOCs | 0 Matching objects

✓ **IT threat evolution in Q1 2023. Non-mobile st...**
Sources: SecureList Published: Mon Jun 26 2023
PC malware statistics for the Q1 2023 includes data on miners, ranso...
8 IOCs | Enrichment IOCs | 0 Matching objects

✓ **IT threat evolution Q1 2023**
Sources: SecureList Published: Mon Jun 26 2023
Recent BlueNoroff and Roaming Mantis activities, new APT related to ...
0 IOCs | Enrichment IOCs | 0 Matching objects

Stairwell automatically operationalizes your threat intelligence

1. **Automated ingestion of intelligence**: Stairwell eliminates the need for manually piecing together different intelligence feeds by automatically ingesting and parsing all sources of threat intelligence. Advanced logic and analysis is conducted with the ingested intelligence against every relevant file written to disk, quickly identifying malicious files or variants and providing your security team with the evidence and information needed to take immediate action.

© 2023 Stairwell, Inc. All rights reserved

2. **Enhanced detection and response capabilities**: With Stairwell, organizations can significantly improve their detection and response capabilities as the analysis and details conducted are instantaneous and at the binary level. By operationalizing threat intelligence, security teams are able to identify threats with evidence-based analysis and take proactive measures to mitigate an attack.
3. **Comprehensive historical and evidence-based analysis**: Stairwell's perpetual storage of executable or executable like files provides organizations with an unprecedented historical dataset for analysis. This empowers security teams to conduct retrospective investigations, identify patterns, and gain insights into past threats based on the latest threat intelligence received. By leveraging this comprehensive historical analysis, organizations can enhance their threat hunting capabilities and implement preventative measures.
4. **Increased efficiency and cost savings:** By automating threat intelligence, Stairwell creates a common source for analysis and evaluation with respect to intelligence and threats. This saves your organization valuable time and resources, drastically reducing the manual effort usually required to analyze and correlate multiple intelligence sources.

Stairwell's groundbreaking approach addresses the challenges associated with operationalizing threat intelligence across your organization. By automating the analysis of files at the binary level and integrating intelligence feeds, Stairwell empowers organizations to swiftly identify threats and respond effectively with evidence-based artifacts.

With enhanced detection and response capabilities, comprehensive historical analysis, and increased efficiency, organizations can stay one step ahead in the ever-evolving landscape of cyber threats. To learn more, visit www.stairwell.com.

© 2023 Stairwell, Inc. All rights reserved