Incident response in minutes

Today's challenges

Organizations today face unrelenting cyber threats from numerous attack vectors that necessitate swift and effective incident response when a malicious event has been discovered. However, this is often easier said than done. Conducting a comprehensive threat assessment and responding to attacks is challenging, time-consuming, and very resource-intensive.

Current situation: Sifting through alerts and conducting forensic analysis

Organizations continue to find themselves overwhelmed with alerts, necessitating the prioritization of potentially or yet-to-be-triaged severe threats. Meaning, the security operations center (SOC) or incident response (IR) teams are responsible for determining the severity of an attack and then conducting extensive forensic analysis.

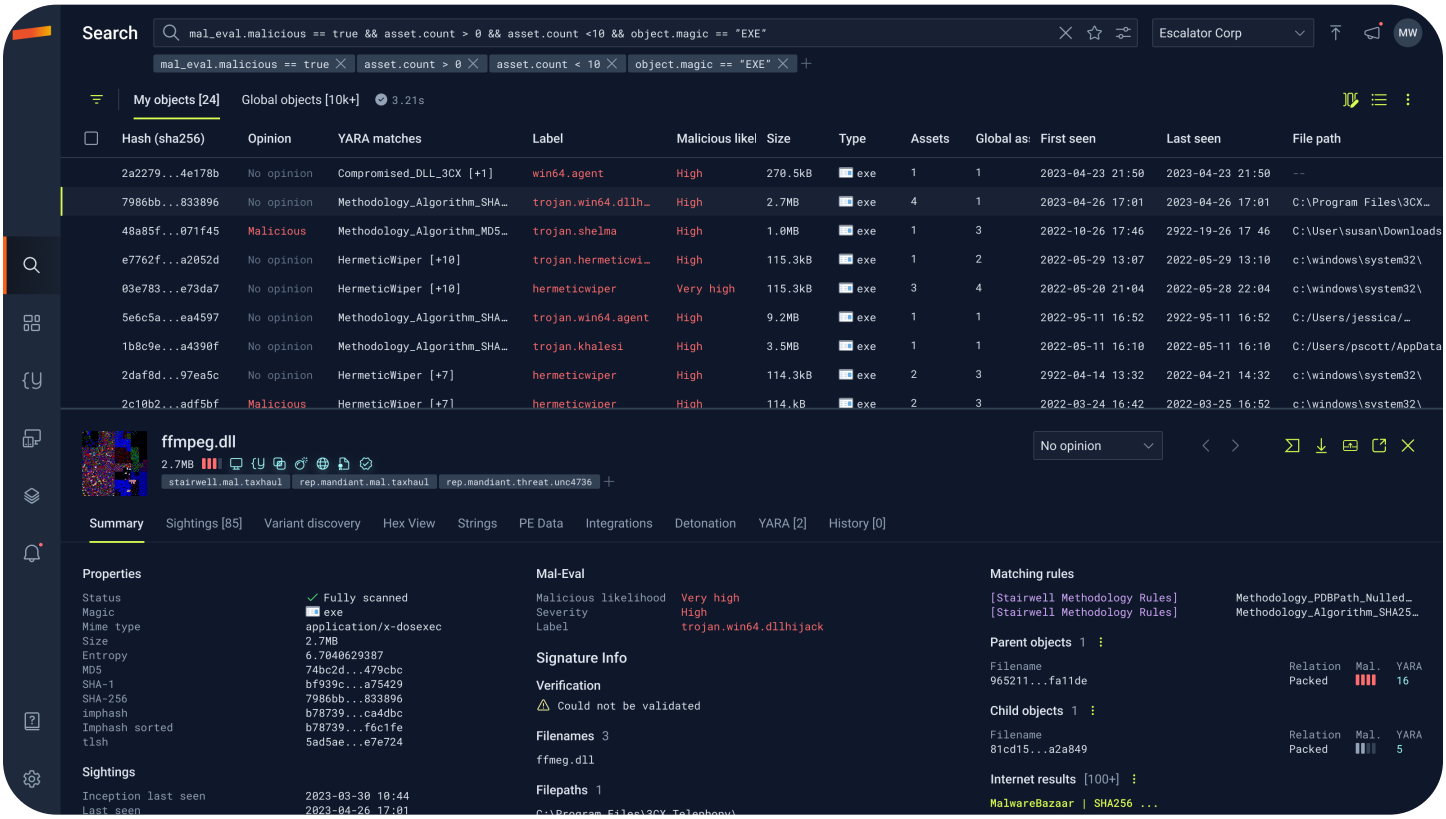
These efforts demand significant time, resources, and skilled personnel capable of researching across the different systems and networks involved. The time needed to collect and harvest details from impacted assets is also a major hurdle, often taking days to weeks, and is further hampered due to retention limitations. Consequently, security teams are unable to obtain comprehensive digital forensics and evidence, hindering their ability to understand the full extent of an attack.

Incident response in minutes

Accelerating threat assessments in seconds with Stairwell

The Stairwell platform is transformative for security teams as its data and evidence-based capabilities quickly help address the challenges of threat hunting and incident response assessments. Stairwell takes a whole new approach by ingesting every executable or executable like file written to disk, retaining them indefinitely, and running both static and dynamic analysis – all so your teams able to get digital forensic assessments in seconds to minutes, not days to weeks.

This unique approach leaves an attacker with no place to hide and empowers SOC and IR teams to swiftly determine the presence of a threat within their environment, both from the past and the present. What used to take days to manually correlate data, sift through logs, and reference intelligence feeds is now accomplished in minutes.



Stairwell allows the evidence to drive immediate action

1. **Threat detection and assessment in seconds**: Stairwell drastically reduces the time required to assess breaches and threats; instead of days or weeks, organizations can

obtain forensic analysis and results within seconds or minutes. This enables swift decision-making and minimizes the potential damage caused by an ongoing attack.

2. **Evidence-based analysis for effective response**: Stairwell's neural net-powered analysis and YARA scanning provide evidence-based verdicts, equipping teams to respond promptly to new and previously unknown threats or compromises. By automatically running comprehensive analysis on each ingested piece of malware, new threat alert, or threat intelligence, organizations gain a high degree of certainty regarding their exposure and impact.
3. I**mmediate access to digital forensics and evidence**: Stairwell overcomes the challenges associated with collecting and harvesting digital details from impacted customers. By retaining every executable or executable like file written to disk indefinitely, organizations have access to historical data, enabling them to conduct in-depth forensic analysis. This eliminates the limitations imposed by traditional forms of retention, allowing for comprehensive investigations that can span days, months, or even years.
4. **Empower analysts to quickly understand and respond:** With Stairwell, analyst teams are able to comprehend, analyze, and respond swiftly to potential threats. By automating the analysis and assessment process at the binary level, valuable time and effort are drastically reduced, enabling analysts to quickly mitigate threats and focus on proactive threat hunting, implementing proactive defense measures, and making strategic decisions.
5. **Automated & ready for future assessments:** Stairwell's platform serves as a foundation for all malware and threat analysis. By having a comprehensive repository of relevant files, organizations can leverage this valuable dataset for retrospective analysis, proactive threat identification, and continuous improvement of their security posture.

The Stairwell platform addresses the challenges posed by cyberattacks and significantly reduces the associated costs of conducting full-scale threat assessments. By automating the process and providing near-instantaneous results, organizations can reduce breach detection and assessment timelines, enhance their incident response capabilities, and save costs by allocating resources more effectively.

Stairwell offers transformative capabilities that enable organizations to respond swiftly, mitigate risks, and bolster their overall security posture. To learn more, visit www.stairwell.com.