DATA SHEET

Active Threat Detection

Catch the Threats that Other Tools Miss

No matter how good your security team – or how powerful your security tools – there are indicators of threats going unnoticed on your network, right now. After a breach, retrospective analysis almost always shows that there were small signals that, when added up, could have been the warning you needed. They become evidence of the clues you missed. They are hard lessons in how to improve cyber defenses.

In the age of constantly escalating threats, rampant data theft, and devastating ransomware, you need faster detection and proactive response. You need

- 277: Average number of days it took for organizations to contain a breach in 2022.
- $1.12M Average savings of containing a breach in 200 days or less (Cost of a data breach 2022 | IBM)

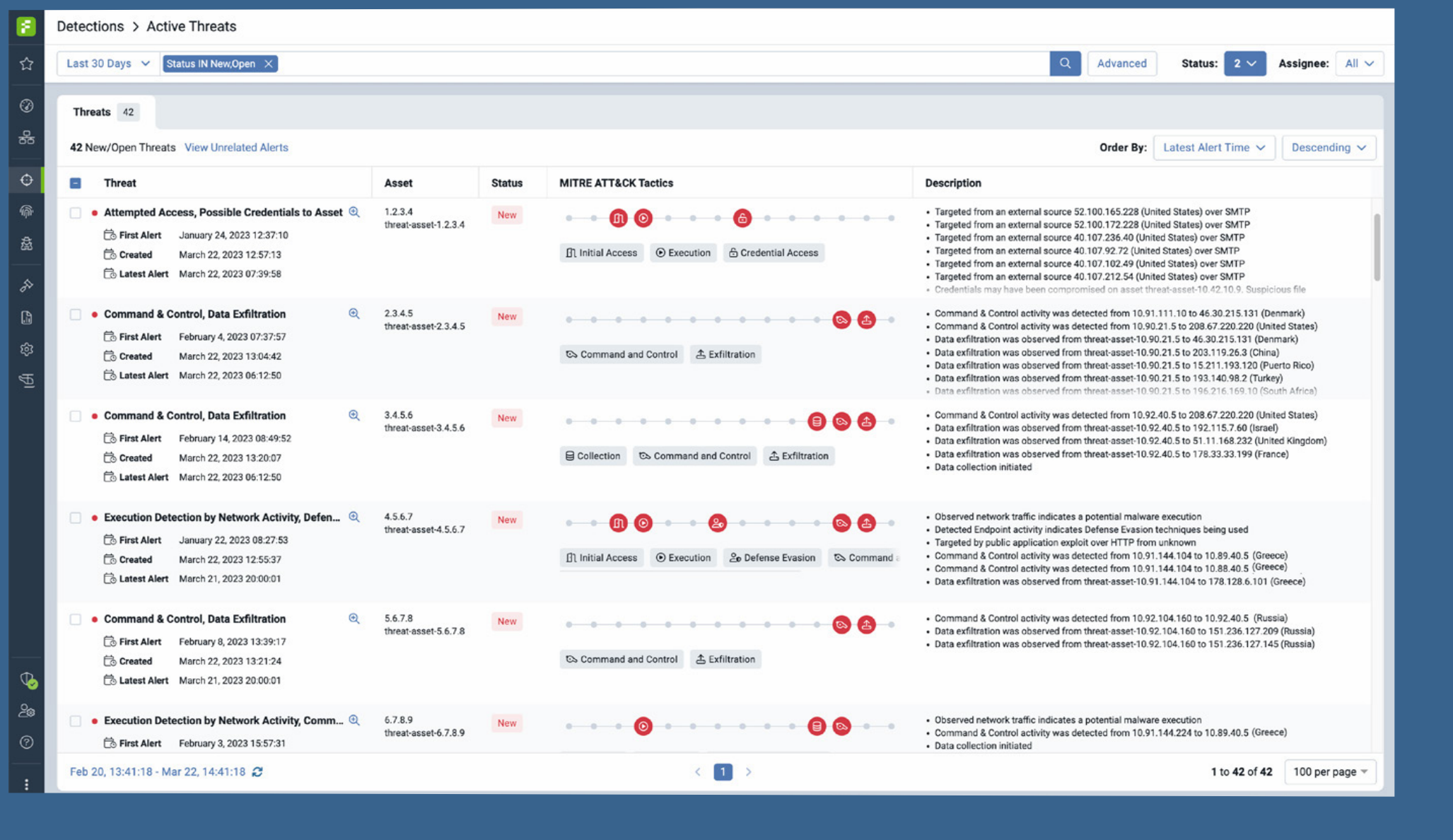
What is Active Threat Detection?

This groundbreaking, proactive threat detection and hunting technology now available in Fidelis Network® and Fidelis Elevate® correlates weak signals that often go unnoticed, drawing strong, evidence-based conclusions – automatically. Using proprietary algorithms developed by Fidelis Security's expert threat hunters, Active Threat Detection improves the speed and accuracy of your threat hunting – often finding threats that other systems miss – so that you can shut the door on would-be attackers.

Master the Hunt with Active Threat Detection

The last thing a security analysts needs is another alert vector adding noise. Alerts can contain thousands of entries, only some of which (if any) present indicators of credible threats. Active Threat Detection reduces the noise and draws strong conclusions. This is the clarity that analysts need for faster, more efficient, and accurate threat hunting. With Active Threat Detection, you can:

- Correlate weak signals across multiple phases of an attack and generate actionable detections.
- Find threats that might otherwise go unnoticed.
- Cut through the noise to determine credible threats quickly and accurately to your network.
- Map threats to MITRE tactics and techniques automatically.
- Operate within detailed workflows.
- Determine the best course of remediation based on expert recommendations.



How Active Threat Detection Works

Active Threat Detection is an integral part of the Fidelis Elevate framework. Active Threats correlate data from Fidelis Network, Deception, Endpoint, and Sandbox alerts

Detect and Correlate Weak Signals

Active Threat Detection surfaces high-confidence conclusions by aggregating data across alerts and assets and mapping findings to known attack techniques. Each conclusion represents an Active Threat to the network. It filters out noise and false positives, giving analysts dependable and actionable insights into the status, location, and impact of the threat. These findings help analysts quickly attend to malicious or highly suspicious activity in their networks.

Evaluate Findings Against Known Attack Vectors

Tracking the techniques, tactics, and protocols (TTPs) used by cyber adversaries is a full-time job. Active Threat Detection does the work for you by automatically correlating signals using the MITRE ATT&CK framework. This eliminates tedious and error-prone threat hunting exercises. The Active Threat workflows provided through Fidelis Elevate tell the complete story of the threat and offer evidence and guidance for investigation and remediation.

Proactively Secure Systems with Greater Confidence

Security teams can act swiftly and with greater confidence, relying on actionable conclusions. Each conclusion provides evidence of each threat signal, including stage of attack, involved files and systems, attack TTPs, and descriptions. Responders and threat hunters can drill in deeper to discover and remediate security weaknesses. And with intelligence that learns and grows, your cyber defenses become the foundation for true cyber resiliency, keeping your valuable assets and data safe, no matter what comes next.

Put Active Threat Detection to Work

Active Threat Detection is an integrated part of the Fidelis Elevate platform. Fidelis Elevate is an active and open eXtended Detection and Response (XDR) platform designed to enable proactive cyber defense. Fidelis Elevate delivers contextual visibility and rich cyber terrain mapping across the full threat landscape. These insights enable security teams to continually tune defenses and neutralize threats before they can damage business operations. They also form a foundation of intelligence to keep you ahead of the next attack.

Learn more about Fidelis Elevate, or sign up for a free demo today to see how your security teams can see more, and stop more, with Active Threat Detection, only from Fidelis Security.

About Fidelis Security®

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.

Contact us to learn more

www.fidelissecurity.com/contact
or scan the QR Code