DATASHEET

Fidelis Insight™

The Engine Behind the Intelligence

Go Beyond Signatures and Feeds

Fidelis Insight delivers threat intelligence in several forms and serves as a key element combined with network sensors, endpoint agents and sandbox techniques into a single solution that automates threat detection and response.

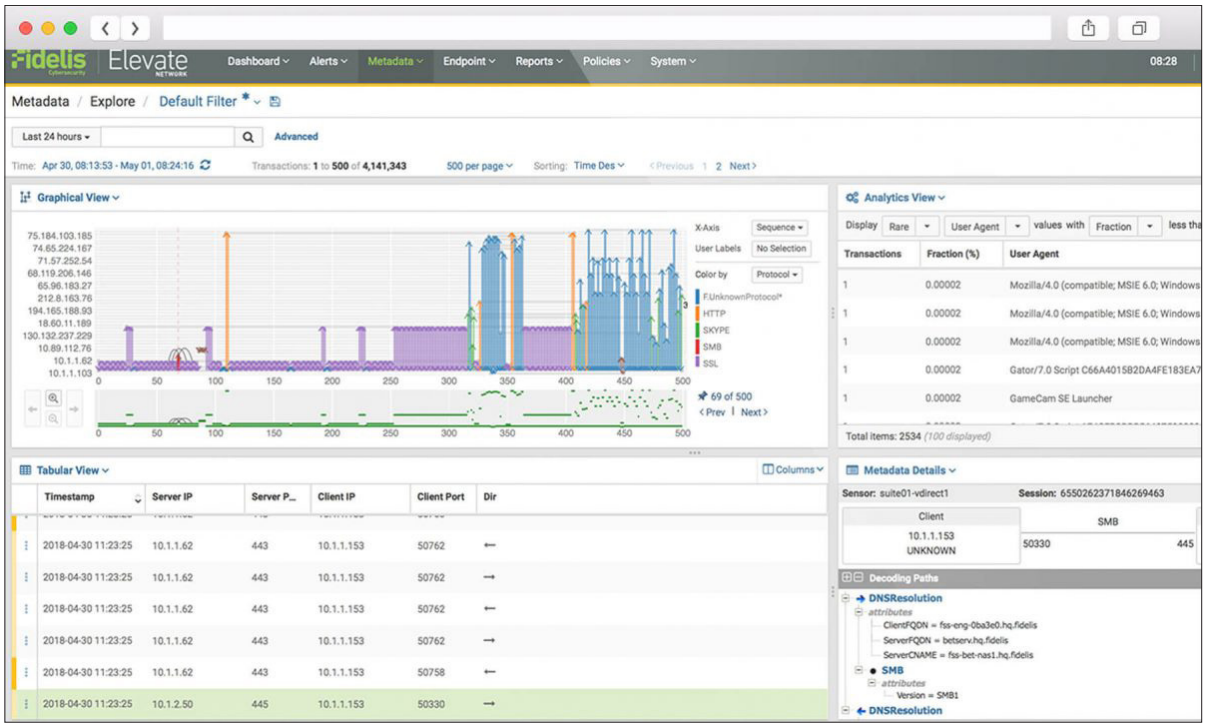
Curating Intel to Drive Detections

Fidelis Insight threat intelligence is sourced from various feeds and curated by the Fidelis Threat Research Team to drive the detection techniques used by Fidelis Network sensors and Endpoint agents.

Threat Intelligence

It is used in numerous ways across Fidelis products including:

- Policies, which include rules that enable the detection of threats, compliance with industry standards, and detection of data theft.
- The Malware Detection Engine which is included within the Fidelis Network sensors. This engine was built specifically to identify malicious files and malicious network behavior.
- Validation rules, which query endpoint events that correspond to every Fidelis Network alert so that analysts know whether the alert requires immediate attention or not.
- Fidelis Feeds, which cultivate data from several sources including Fidelis internal research, open source providers, Fidelis partnerships, and machine-learning algorithms that are applied to data sent to the Fidelis Content Analysis Platform.
- Fidelis Insight provides a feed of Behavior Rules to Fidelis Endpoint providing behavior-based detection of malicious and suspect activity. Behavior Rules are compared against the activity on endpoints in near-real time driving detections and alerts. Insight provided Behavior Rules are mapped to Mitre ATT&CK techniques when possible, providing additional context when rules are triggered.



Endpoint Intelligence Feeds

Fidelis Insight delivers continuously updated intelligence to Fidelis Endpoint in both atomic and behavioral indicator feeds to drive detection. This data is used by Fidelis Endpoint to compare against all endpoint activity in near-real time to identify bad behavior or dangerous actions. Because intelligence data is bundled and sent to each individual endpoint, you don't have to worry if the endpoint doesn't have an internet connection when something malicious occurs.

Threat Cache

The Global Threat Cache stores information about executable files, including the number of antivirus engines that know about the file and the number of those engines that determine the file to be malicious. This information is available for all network transactions that include an executable file.

Content Analysis

Fidelis Insight includes the Content Analysis Platform, which includes a sandbox execution environment with active networking that allows samples to call out as they would in normal operations. Analysis is performed and the results associated with the alert created are displayed in the sandbox report that carries the malware score. Scores range from 0 to 100, where 100 indicates high confidence that the file or site is malicious.

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.

