DATASHEET

The Platform Relied on By Incident Responders

Ensure faster, more effective incident response for your clients.

When a Security Incident Occurs, Every Moment Counts

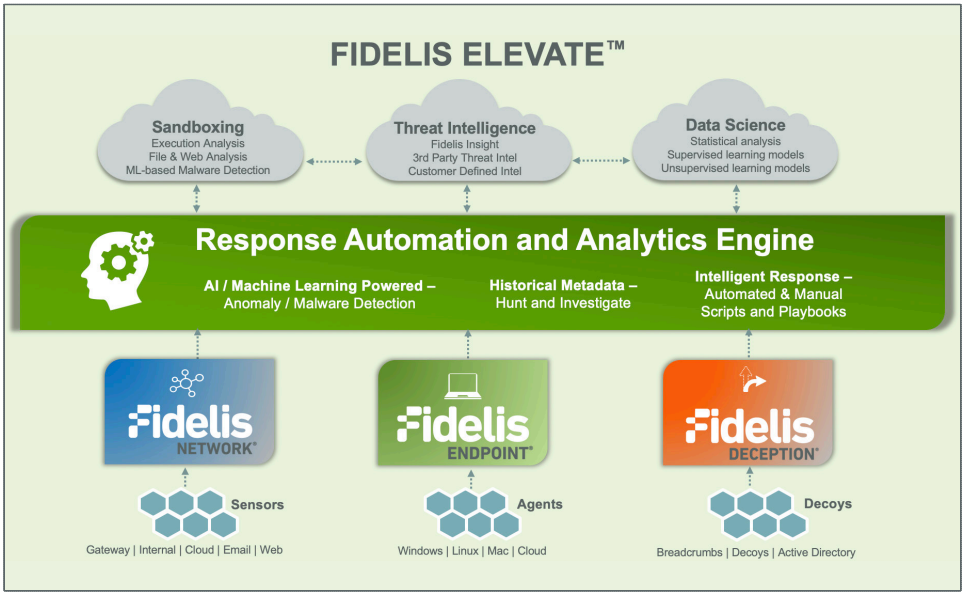
Advanced attackers are well-hidden and once a threat is identified, the initial detailscan be limited. Important factors include how long the attacker has been active in the environment, how many systems are compromised and what, if any, information has been exfiltrated. A rapid response is required to contain and eradicate the threat, reduce the loss of IP and minimize any disruption so you can quickly return to business as usual.

When an incident response event occurs, quickly getting a lay of the land is critical. Having visibility from the network and cloud traffic to endpoint activity is a must to understand the who, what, when, where, and how — and having the tools and automation to resolve issues is of utmost importance.

Incident Response Platform Used by the Pros

The Fidelis Elevate platform has been relied on in thousands of incident response cases, including many of the largest breaches on record, to identify threats, minimize the damage and remediate the threat. Incident responders use the platform for timely detection, the discovery of attacker activity, identification of compromised systems and data accessed or removed, and to prevent similar reoccurrences through automated response playbooks.

Fidelis Elevate provides a streamlined security stack that integrates network, endpoint and deception defenses, automates and orchestrates workflows, and correlates rich metadata across these security layers so you have continuous visibility across your environment. Now you can quickly detect, hunt and respond to threats, while keeping your sensitive data safe.



Key Benefits

- **Visibility Across the Environment:** Fidelis Elevate provides visibility across all ports and protocols, including network, email, web and cloud traffic, endpoint activity, and visibility of enterprise IoT devices.
- **Fast Initial Response:** Fidelis provides IR teams with the ability to quickly understand the environment, conduct an initial assessment and develop an appropriate response strategy.
- **Deep Investigation and Forensics:** With Fidelis Elevate, in even the most complex environments, incident responders have the tools and data to properly investigate suspicious behavior, hunt for malicious activity, isolate compromised accounts, and identify data, system and network assets accessed.
- **Contain and Expel the Threat:** Using Fidelis to identify a timeline of activity, systems and networks affected and attacker activity, incident responders can contain the attack (i.e. Remove traces of attackers' malware and tools, reset credentials, and mitigate exploited vulnerabilities) and continue to monitor the enterprise for malicious activity.
- **Remediate and Recover:** A successful remediation involves eradicating the malicious attacker from the enterprise and returning to business as usual. Once the threat has been removed, automated responses can be deployed to eliminate similar threats from impacting the environment in the future.

Improving Incident Response with Fidelis Elevate

Here are just a few recent examples where incident responders used the Elevate platform to resolve high priority security events. The flexibility and power of the platform enables incident responders to efficiently address unique scenarios, minimize attacker dwell time, and more quickly resolve critical issues.

Using Automation to Remediate Attacker Actions

Upon investigation of a recent attack, incident responders found that malware was trying to mask its activity by disabling and clearing the Event Viewer on some Windows machines.

Responders used the Fidelis platform to remediate this action by initiating a task to re-enable the Event Viewer service every time it was turned off. The powerful scripting capability of Fidelis allowed this to be created on the fly within 5 minutes. Once responders saw that the script was resolving the malicious actions manually, it was then set to an automated response, enabling them to move on to other issues.

Seeing Endpoint Activity Prior to Agent Installation and Tracking Attacker Movement Throughout the Network

Incident responders needed to understand what endpoint activity occurred before the response team arrived and began installing Fidelis agents. Specifically, they needed to scan the machines to look for Indicators of Compromise (IOCs) and to identify the tools being used in the attack. Using the Fidelis platform, a YARA script was run to look for the attacker's tools in memory and on disk.

Endpoints were scanned and the IR team on this case identified infected machines and added them to the scope of the incident. Via the Fidelis platform, responders were also able to search for malicious artifacts by leveraging the file hashes identified to search through metadata and see not only where the files were coming from, but also how they were moving throughout

the network. Armed with this information, the team now had the ability to identify staging areas for tools and security holes, while also creating new rules to identify the movement of the tools and track the attacker.

Minimizing the Impact of Installed Malware

With the Fidelis platform, responders can enable local AV and Advanced Malware Detection, which in a recent case was used to quarantine email attachments that were attempting to run, sitting on disk, and embedded in Outlook OST files on disk, while also identifying the malware being used by the attacker. The malware had bypassed the original AV software that was installed on the endpoints prior to the incident. The quarantined files were sent to the Fidelis sandbox to understand how the tools worked, where the files were being moved throughout the environment and what they were doing. With the integration of network and endpoint information, Fidelis Elevate enabled the IR team to correlate information between endpoint malware alerts and network traffic alerts to identify incident timelines. Additionally, since the original AV agent was found to be compromised and did not identify the offending malware, the security team wanted it removed from the machines. Using Fidelis, they were able to quickly modify the Registry and allow for agent removal.

Remote Agent Installation

In an incident where the security team onsite needed help deploying more agents, a script was created to remotely install the agent using PowerShell on remote hosts from the endpoint with the agent currently installed. This allowed the agent to populate to surrounding endpoints without having to use the IT channels and slow down the investigation.

Hunt Down Advanced Threats

The IR team used Fidelis Endpoint behavior rules to identify attacker scripts, beacons, and other malicious files being run on infected endpoints. The Fidelis agent also enabled the team to collect and sandbox the files for better insight of what they were doing. With the Fidelis script and executable collection feature turned on, all first-time seen files were ready to be downloaded in a secure zip file and submitted to the Fidelis Network Sandbox for analysis. Tying in with the network metadata, the team was able to identify the movement of malicious files through the

environment leading to additional machines that had not launched the tools, but to which the tools had been transferred and staged. By hunting through the metadata, the IR team was able to identify a machine where a new scheduled task had been created to launch ransomware. This task was found by the team 15 minutes before it was set to trigger and encrypt all accessible drives in the environment.

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.

