Fidelis Cybersecurity

DATASHEET

Incident Response Retainer

Accelerate your response, resolve the threat, and return to business as usual.

When a Security Incident Occurs, Every Moment Counts

Advanced attackers are well-hidden and once a threat is identified, it is often unclear at the time of detection 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 disruption to business, and return to business as usual.

Fidelis' incident response professionals know what works and what fails based on our firsthand experience responding to high-profile security incidents over the past decade. We move quickly to identify and remove attackers from the environment, re-secure the enterprise and help organizations successfully recover from any incident.

Our Approach

Every minute matters during a security incident. Our service focuses on timely detection, the discovery of attacker activity, identification of compromised systems and data accessed or removed, and a plan of action to improve the organization's security posture to deter similar incidents from occurring again.

Initial Response: During the first phase, we review any existing information and evidence, assess current security controls in place, and conduct an initial assessment to develop an appropriate response strategy.

Investigation: We establish enterprise-wide visibility across your network and endpoints where we will investigate suspicious behavior, hunt for malicious activity, isolate compromised accounts, and identify data, system and network assets accessed. We set up monitoring capabilities and leverage our endpoint technology to quickly search complex and diverse environments.

Containment and Expulsion: After identifying a timeline of activity, systems and networks affected and attacker activity, we work closely with your team to contain the attack. During this stage we continue to monitor the enterprise for malicious activity, as we covertly cut off the attacker's ability to access or exfiltrate data by disconnecting or isolating the attacker from the network. Containment activities culminate in an expulsion event where we remove traces of attackers malware and tools, reset credentials, and mitigate exploited vulnerabilities.

Remediation and Recovery: A successful remediation involves eradicating the malicious attacker from the enterprise and returning to business as usual. Once the attacker is out of your environment we work with you to enhance the security of your network to reduce the likelihood of another security incident. Our recommendations are based on our defense-in-depth strategy and includes people, processes, and technologies to reduce your risk while keeping costs at a minimum.

Our Experience

- Members of our security consulting team have over 18 years of incident response experience on average.
- We have responded to more than 4,000 security cases in both the commercial and government sectors.
- Our security professionals were instrumental in building one of the first security operations centers.
- We have provided expert testimony in over 100 court proceedings.
- Our team successfully guided one of the largest forensic laboratories (DCFL) to achieve international digital forensic accreditation.
- We have a dedicated malware team focused on reverse engineering malicious files and researching the latest exploits.

Expertise at Every Stage of the Response

Key areas we support during an incident response investigation include:

Investigation Management: We work closely with the executive, legal and public relations teams and other key stakeholders to minimize the disruption to business, align the business units, and keep everyone informed using a clear and synchronized communication plan.

Forensics: Our forensic examiners perform a thorough examination of system artifacts and images, including an initial forensic triage that looks at system information, user activity, registry, file listing, file metadata, log analysis, network communication, and timeline analysis.

Malware Analysis: Our dedicated malware analysis team can reverse engineer malware code samples found in the environment. By understanding the malware's behavior we are able to gain visibility into where the attacker had been, what they are doing and where they intend to go.

Containment: Our security architects develop a concise action plan that leverages information gained during the investigation and moves the incident towards completion. Containment culminates in an expulsion event that is carefully choreographed to minimize risk of the attacker regaining network access.

Network Monitoring: Sensors are deployed to provide full visibility into all communication moving in and out of the network, including traffic traversing laterally inside of the enterprise where the malicious actor may be staging data for exfiltration.

Endpoint Scanning: Leveraging our Fidelis Endpoint™ product we apply our intelligence and any known Indicators of Compromise to sweep all endpoints in an enterprise to rapidly detect all compromised systems.

Deception Environment: Quickly detect post-breach attacks which discovers and classifies all network assets, and automatically creates breadcrumbs and decoys to lure and trap attackers.

Recovery: Recommendations are provided around the measures to reduce the likelihood of an attacker reestablishing access to the environment. We also establish a short and long-term roadmap to enhance your overall security posture.

Legal, Regulatory, and Law Enforcement Support: We provide expert support in communications and interactions with counsel, regulators, auditors, law enforcement, and other third-parties. Examples of this support can include testimony, exhibit preparation, compliance reports, and other required documentation.

CUSTOMER STORY

Large Manufacturer

A large manufacturer discovered an advanced threat actor had circumvented their security measures and was active in their environment looking for intellectual property. They engaged Fidelis to lead the incident response. Within three hours, our security professionals were on-site and moved quickly to form a collaborative, cross-functional incident response team comprised of internal and external stakeholders.

After performing a focused and thorough forensic analysis and developing an aggressive remediation plan, our team removed the attacker from the network within 36 hours. The expulsion event eradicated the attacker's tools, cut off their ability to reenter the network and minimized the risk of retaliation.

Fidelis offers flexible IR retainer services to help customers quickly recover from a security event. From a no-cost retainer that establishes terms and conditions between your organization, to pre-paid retainers that enable the swiftest and most cost-effective response, Fidelis experts are at the ready.

SERVICE	TIER 1	TIER 2	TIER 3
24x7 Hotline	Included	Included	Included
Initial Telephone Consult	Within 12 Hours	Within 8 Hours	Within 3 Hours
Initial Triage Fee	Inquire for Cost	Included	Included
Remote IR Team Support	48 Hours	24 Hours	Immediate
IR Team On-site	Availability	48 Hours	24 Hours
Discount to IR Rate	0%	0%	10%
Review of IR Readiness	Inquire for Cost	Included	Included
Network Threat Evaluation	Included	Included	Included

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.

