

DIGITAL FORENSICS & INCIDENT RESPONSE

Cybercriminals have more resources and time to focus on finding a way in than you have in stopping them. **Falling prey to an incident can happen to anyone, so having the right response team in place is crucial.**

Provided as an on-demand crisis response service as well as retainer-based program, Avertium's Digital Forensics and Incident Response (DFIR) helps you to rapidly assess, contain, eradicate and recover from a security incident to minimize impact and return you to normal operations. Because superior DFIR extends beyond technical expertise, Avertium's skilled incident handlers help you and your executive team to navigate potential legal and reputational liabilities while driving to identify and resolve the root cause that led to the incident in the first place.

**THE CYBER WAR IS WAGED ON MANY FRONTS.
AVERTIUM HELPS YOU FIGHT IT, BRINGING TOGETHER...**

A BUSINESS-FIRST MINDSET

Avertium tackles each unique incident with the right tools, methodologies, and people to meld to the distinct challenges presented and ensure we react quickly and appropriately to your situation. Our team responds to an emergency within two hours to gather details while creating an action and communications plan for our customers.

Types of incidents we encounter:

- » Ransomware
- » Data Exfiltration
- » Business Email Compromises
- » Advanced Persistent threats
- » Social Engineering
- » Unauthorized Access
- » Banking Trojan Outbreaks
- » Spear Phishing Attacks
- » Insider Threat
- » Malware and Worm Outbreaks
- » Drive-by-Downloads

A CYBER FUSION PHILOSOPHY

As the leading provider of accessible managed security and security consulting services to the midmarket and enterprise, we offer a comprehensive array of solutions that support the **full incident response lifecycle**...

- » Plan Development: Incident Reponse, Business Continuity, Disaster Recovery
- » Digital & Mobile Forensics
- » Table Top Exercises
- » Managed Security
- » Penetration Testing

where we monitor threat activity, collect forensic artifacts, and analyze actions to determine incident timeline, root cause, and scope.

A HUMAN ELEMENT

Avertium's collaborative strategy with your team **increases the speed to return to normal operations on top of building long-term defenses**. Our team stays in contact in the near term with **regular touchpoints**, to then provide a full understanding of the incident to avoid reoccurrence once all information is gathered:

- » Daily or Weekly Update
- » Post-Incident Report and Briefing

ABOUT AVERTIUM

Avertium is the security partner that companies turn to for **end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context**. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity - one that drives action on the ground and influence in the boardroom. That's why over 1,200 mid-market and enterprise-level organizations across 15 industries turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **AVERTIUM | SHOW NO WEAKNESS.®**

THE AVERTIUM ADVANTAGE

Attacking the chaos of the cybersecurity landscape takes **context of your business, of your existing technology + cybersecurity infrastructure, and of the threat landscape**. Avertium's approach offers **more flexibility, more control, and more resilience**.

» KNOW THY SELF

Using proven frameworks like NIST CSF alongside our in-depth onboarding diagnostic, we get to know your business, your attack surface, your protocols, and your areas of greatest weakness + strength.

» KNOW THY ENEMY

Leveraging our cyber threat intelligence (CTI) alongside the MITRE ATT&CK framework, we then understand current and most likely future attack scenarios.