

EVIDEN

Digital Forensics and Incident Response (DFIR)

Gain a true partner in your defense when you need one the most. With Eviden DFIR, you will investigate incidents, evict attackers, and return to business - faster.

More attacks, less time to respond

Cyberattacks are growing in volume, speed, and impact. The moment an attacker targets your organization, the clock starts ticking. The longer you take to investigate and stop the attack, the more harm you will suffer from compromised data and assets, operational downtime, lost revenue, and regulatory fines.

Unfortunately, many organizations struggle to respond to attacks. They are overburdened with their day-to-day IT operations and cybersecurity tasks. They lack the bandwidth and internal resources needed to prepare for incidents and to mobilize a rapid and effective internal response when an incident occurs.

Comprehensive DFIR services

Let us accelerate and expand your incident response capabilities. Eviden DFIR services give you a dependable partner for emergency response assistance or cybersecurity incident response on a retainer.

We offer 24/7/365 support and deliver a wide range of incident response capabilities through our 16 global SOCs. Our cybersecurity experts work hand-in-hand with your internal teams to swiftly move you from incident to resolution to business recovery.

With Eviden DFIR services, you get:

Fast and Complete Incident Response

Our certified incident experts are on call 24/7/365 to find, contain, and evict any attackers in your network as soon as they strike.

End-to-End Support

We collaborate with crisis communications, post-incident reporting, and legal and compliance teams.

Reduced Security Costs

Improve the speed and effectiveness of your security without investing in new tools, processes, or internal security staff.

Two options to engage Eviden DFIR services

We offer our DFIR services through two programs designed to fit your organization's unique needs. You can engage our DFIR services through:

Incident Response Retainer

Reserve cyber incident response hours from Eviden. Ensure you have the DFIR services you need — when you need them — and rest easy with predictable costs, shortened SLAs, and deeper alignment between our teams and yours.

Emergency Breach Support

Stop an in-progress incident, even if we've never worked together before. Reach out to Eviden when you are under attack to instantly leverage our complete DFIR services and contain, resolve, and recover from incidents.

What's included in every engagement

Our Incident Response Retainers and Emergency Breach Support include every DFIR service you need to detect, respond to, and recover from an attack. We will:



Investigate Breaches Identify if the attack is external or internal, and define the full scope, timeline, root cause, patient zero, and spread of the breach.



Report to Regulators Help your team notify the relevant regulatory authorities in the applicable jurisdiction about your incident and provide the needed evidence.



Collect and Analyze Evidence Collect artifacts, and analyze evidence from applications, data, networks, and endpoints (both on-premise and in the cloud).



SLA-Driven Response* Provide rapid response every time to contain breaches as quickly as possible and to minimize the harm they can cause.



Analyze Malware Detonate malware in a lab that mimics your environment, reverse-engineer the attack, and identify the threat and its vulnerabilities in its code.



MSS & MDR Collaboration Work hand-in-hand with your existing MSS and MDR vendors (many of whom our DFIR teams routinely work with).



Stop Ransomware and Severe Incidents Provide proven, systematic support that we developed, stopping some of the largest and most complex breaches across the globe.



Why Eviden: a proven, reliable partner in your cyber defense

Eviden is the largest managed security provider in the world and has decades of frontline experience resolving complex, high-impact cybersecurity incidents. We deliver our DFIR services through hundreds of certified, expert, in-house security researchers, ethical hackers, threat hunters, and incident response veterans.

By partnering with Eviden, you gain:



Human Expertise Leverage our hundreds of battle-tested frontline operators and consultants.



Custom Processes Adapt our proven response processes to your specific security needs



Round-the-Clock Support Activate our 24/7/365 security teams as soon as you suffer an incident.



Vertical-Specific Knowledge Deploy solutions designed for the unique needs of each industry and org structure.



Systematic Forensics Follow strict processes when handling evidence to determine root causes.



Cross-Functional Response Connect security with crisis comms, incident reporting, legal teams, and other



Flexible Engagements Augment your internal DFIR program or gain an entire response team out-of-the-box.



Global and Local Coverage Tap into 16 Global SOCs with "boots on the ground" support for most regions

Bring Eviden DFIR services to your organization

With Eviden DFIR services, you will:

- **Protect yourself from major and minor incidents**, and be prepared to resolve any sized attack before it causes significant harm.
- **Support your staff with an external team of experts**, and let your internal experts focus on more strategic security projects.
- **Fill gaps in your current security posture**, and bring in new tools, skill sets, and capabilities without further internal investment.
- **Reduce your risk**, and rest assured that you have a dedicated, proven team on-call to rapidly and thoroughly protect your assets from any attack.

Reach out today to partner with Eviden

Need urgent incident support?

Schedule a consultation to build the DFIR program that works best for you.

Want to learn more?

Schedule a consultation to build the DFIR program that works best for you.

Regional contact numbers:

Global: +48 525 866 415

France: +33 (0)1 70 83 85 84

Germany: +49 30 398 202 777

Austria: +43 1 890 30 43 7777

Switzerland: +41 44 545 10 85

North America: +1-866-246-2848

Stay prepared with Eviden CERT services

- Threat Intelligence
- Threat Hunting
- Digital Risk Protection Services
- External Attack Surface Management
- Tabletop Exercises
- Incident Response Program Development
- Product Security Incident Response
- Compromise Assessment
- Vulnerability Management Services
- Remediation Enabling Service
- Red Teaming
- Bug Bounty

Connect with us



eviden.com

Eviden is a registered trademark © Copyright 2023, Eviden SAS – All rights reserved.

ECT-230626-AR-BR-Eviden-Red-Team-Services-en-v1