CyberProof®
A UST Company

Better Security,
Together.

CyberProof Digital Forensics and Incident Response (DFIR)

Many organizations lack the in-depth skills and knowledge necessary to act quickly and effectively in the case of a cyber-attack or a data breach. CyberProof's Digital Forensics and Incident Response (DFIR) is a specialized cybersecurity discipline that combines two skill sets for attack identification, remediation, and investigation. By using data analysis and computer forensics with the predefined incident response plan, CyberProof's DFIR experts can find the root cause of any incident and help to limit the scope of the attack.

What's included in CyberProof's Digital Forensics and Incident Response?

24/7 Incident Response

Both remote and onsite incident response and support in the event of a security breach

Threat Reduction

Protection of critical infrastructure without an impact on business continuity, detecting, containing, and preventing threats.

Deep Expertise

We analyze, prioritize, and categorize security incidents, investigating root cause and cross-incident correlation.

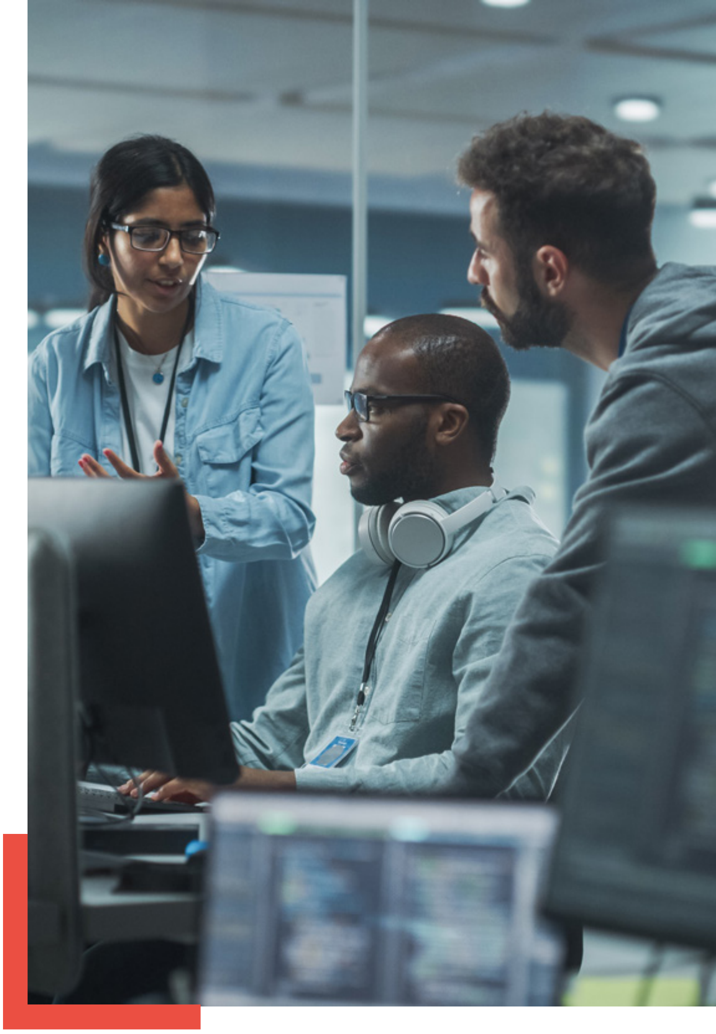
Advanced Threat Intelligence

Benefit from advanced threat intelligence, runtime and dynamic malware analysis, and attacker profiling against known Advanced Persistent Threats.

Digital Forensics

In-depth digital forensic capabilities, across Workstations and Servers - Windows, macOS and Linux.

Highlights



In-depth forensics lab
Conducting static and dynamic malware analysis, memory analysis, image forensics, registry window forensics, and more.

Leading technologies
Leveraging industry-leading tools such as Caine, Redline, and Autopsy, as well as open-source and in-house developed scripts.

Dedicated incident manager
One person who takes the lead in the event of a major breach and takes point on incident response activities.

Reduced time to incident response:
Team is available to start remote investigation within 2 hours, and SLA-based onsite support is also available.

What Makes CyberProof Unique?

Nation-state-level security expertise

Cyber experts around the world with years of hands-on industry experience, including offensive and defensive nation-state expertise.

Service modularity and flexibility

Completely tool and tech-agnostic, CyberProof services can also be provided on the client's tech stack.

Cross-vertical expertise

Robust understanding of industry-specific needs such as specific compliance regulations and targeted incident investigation.

Clear onboarding process

Includes an incident breach readiness assessment, table-top exercises, red teaming and blue teaming, and more.