cybereason® | PRODUCT BRIEF

Digital Forensics and Incident Response Solution

DIVE DEEP AND DISCOVER THE TRUTH

KEY BENEFITS

Conduct full post-mortem attack analysis

Remediate and address all aspects of a threat

Enrich detections with forensic artifacts and telemetry

Search for and collect suspicious files based on wide-ranging criteria

Reduce MTTR (mean-time-to-remediate)

Streamline deployment of adjacent DFIR tools

Complete Visibility

Forensic Data Ingestion enables IR teams to incorporate nuanced forensic artifacts into threat hunting and investigative queries. The MalOp™ Detection Engine automatically correlates and contextualizes the detected operation using this forensic data for an enriched view of the attacker journey while in the environment.

Contain Ongoing Attacks

Use the Cybereason DFIR Solution to contain an ongoing attack in minutes by executing commands directly on the host in question with remote shell and real-time response actions. Address all aspects of a threat to avoid partial remediation and return impacted systems to a safe state.

Uncover Advanced Adversaries

Fully discover sophisticated adversaries and analyze complex TTP's by tracing the attacker path back to root cause. Understand the full scope and timeline of an incident using enriched forensics and identify all impacted systems and users. Search for relevant files and forensic artifacts of interest through wide-ranging criteria to collect files as needed.

Fully Supported Technology

With a lack of Tier III experts available in the market, many teams are understaffed and lack in-house IR expertise. Cybereason automates many aspects of a DFIR investigation and up-levels the capabilities of an L1 analyst to perform more forensic tasks. In addition, our Services Teams fully support investigations, breach recovery, forensic audits, and deep-dive analysis.

Investigate Deeper

With the Cybereason DFIR Solution, security analysts gain immediate insights from a wide array of forensic artifacts, including:

- File events
- OS artifacts
- Memory dumps
- MFT's
- NTFS transaction information
- Threads
- Registry files
- Event logs
- RDP Cache
- + much more

Your security team can leverage these forensic artifacts to ensure there are no backdoors or other malicious elements left behind by an attacker, ensuring comprehensive remediation.

Tools Your Analysts Need

Deploy adjacent IR tools using the Cybereason sensor path and centralize investigation results in the intuitive Cybereason UI. Advanced teams can also deploy a pre-provisioned IR environment with all of the necessary tools for investigation pre-configured for the specific IR workflows that are required. Experts need expert tools, and analysts can dive deep where needed and avoid cumbersome deployments to reduce the overall mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).

Expand Your Security Team with a Trusted Partner

During an incident, there is often a struggle where teams have to extend their resources to fully engage in remediation. During these high-risk times, it's especially critical to have the right resources to address incident remediation. With Cybereason, your team can rely on our world-class experts to deliver comprehensive protection on-demand when you need it. Our analysts are a powerful extension of your security team that help resolve incidents using advanced, cross-industry playbooks developed from years of experience defending millions of endpoints.

UNIQUE FEATURES

- FORENSIC DATA INGESTION FROM ADJACENT DFIR TOOLS
- LIVE FILE SEARCH OF ANY FILE ON ANY SYSTEM IN THE ENVIRONMENT
- IR TOOLS DEPLOYMENT OF SIMILAR DFIR TOOLS NEEDED IN THE INVESTIGATION
- EXPRESS IR TO AUTOMATICALLY DEPLOY A PRE-PROVISIONED IR ENVIRONMENT
- ANALYZE AT SCALE WITH SUPPORT FROM CYBEREASON EXPERTS
- FORENSICS FOR MAC, WINDOWS, AND LINUX
- TAILORED REMEDIATION ACTIONS
- EXECUTE COMMANDS DIRECTLY ON THE HOST

ABOUT CYBEREASON

Cybereason partners with Defenders to end attacks at the endpoint, in the cloud and across the entire enterprise ecosystem. Only the Cybereason Defense Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in Boston with customers in more than 40 countries.