cybereason® | SERVICE BRIEF

Cybereason Incident Response & Professional Services

PROTECTING ORGANIZATIONS EVERY STEP OF THE WAY

BENEFITS

Packages designed to suit the needs of any size organization

Security experts designated to help you before, during and after an attack

Unlimited IR included in the Premium bundle

Cybereason IR and Professional Services

Cybereason's IR and Professional Services offer organizations a customizable approach to improve security posture, uncover vulnerabilities and fortify their infrastructure against modern threats. Cybereason leverages it's Forensics-as-Code (FaC) engine to uncover a threat actor's tradecraft and intent by enriching the data associated with a MalOp, and looking at historical artifacts. This tool delivers complete visibility into an attack and reduces the complexity and manual methods of data stacking that are often seen with other IR solutions. The FaC engine reduces the average investigation time by up to 60% saving time and money.

A direct result of these tools and features, is the ability to offer unlimited IR as part of our Premium bundle. This subscription based service is delivered to customers and partners through a single self-service portal with services access to Cybereason's premier IR team, continuous threat intelligence and proactive assessments.

SERVICE	MODULES	PRO	PREMIUM	CUSTOM
Global Threat Intelligence	Threat Spotlight	✓	✓	Build your own package
	Threat Intelligence Feeds	+	✓	
	Detection Package	+	✓	
Proactive Services	Security 101	✓	✓	
	Compromise Assessment	✓	✓	
	Security Validation	+	✓	
Incident Response	IR and Forensics Experts	-	✓	
	Threat Hunting	-	✓	

Cybereason's IR and Professional Services Portal

Cybereason's IR and Professional Services customers will have access to the single self-service portal that provides Professional Services, Incident Response and Threat Intelligence reports.

Based on IBM 2021 data breach report, the duration of breach containment was 75 days during 2021, based on IDC research, the time to triage and contain an incident based on a survey was 23 days, taking an average of 48 days between the two researches, Cybereason average response time during 2021 was 18.5 (148 hours \ 8 hours per day) days, which is 60% more efficient then mentioned in the reports.
IDC Research can be found here. IBM Research can be found here.

Incident Response (IR)

Best-in-class experts rapidly deploy remote and scalable IR to investigate the incident in minutes and stop the attacker in its tracks to reduce any future damage and loss. Leveraging DFIR and Forensics-as-Code (FaC) technologies, Cybereason's IR team will work with an organization to uncover all instances of malicious activity quickly and efficiently, saving time and money.

Professional Services

Threat Intelligence: Global Insights	Cybereason Threat Intelligence provides attacker insights, trends and adversary information that will help you improve your security posture and identify potential targets within your environment.
Compromise Assessment	The Compromise Assessment provides a complete and rapid review of an organization's systems to identify evidence of past or current compromise. In the event that traces of intrusion are identified, Cybereason performs initial forensic verification and provides an option to pivot from Compromise Assessment to Incident Response service.
Security 101	Security 101 collects data across the customer environment on managed and unmanaged systems, performs security hygiene checks to uncover weakness, and provides recommendations to bolster the security and IT hygiene.
Security Validation	Security Validation is a proactive measure to assess an organization's cyber-resilience by reviewing a customer's infrastructure to identify weaknesses that are known to be frequently abused by attackers. In a single package, it combines Attack Surface Discovery and an Active Directory security health check, designed specifically to provide immediate value and uncover security vulnerabilities.

ABOUT CYBEREASON

Cybereason is the XDR company, partnering with Defenders to end attacks at the endpoint, in the cloud and across the entire enterprise ecosystem. Only the Cybereason AI-Driven XDR 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.