

Threat Hunting and Response Service

Organizations struggle to detect and respond to cyber threats that have evaded traditional security defenses.

CyberDefenses has the expertise, experience, and technology to find and respond to threats and attacks before it's too late.



Today's attackers are clever and motivated. Once inside your organization, attacker dwell time (from malicious attack entry to discovery) remains over six months. Even worse, the average total cost of a data breach is \$4M.

Every organization is a target. A serious breach is not a question of if, but when. And yet, the vast majority of businesses, government agencies, and educational institutions are ill-equipped to hunt for, and respond to, targeted or insider attacks.

CyberDefenses' Threat Hunting and Response Service provides 24/7 monitoring of leading edge threat indicator technologies, actively hunts for post breach activity, and provides incident investigation and response - all as an end-to-end service. Threat hunting expertise is both expensive and difficult to obtain for many organizations, especially midsize concerns.

With CyberDefenses, organizations can focus on their core business, having assurance that a skilled set of military-grade security experts are on the watch, and at the ready to address breach activity.

- Expertise in managing your existing security solutions
- Experienced and credentialed threat hunters with top level security clearances
- 24/7 advanced threat indicator monitoring
- User and device behavioral analysis
- Proprietary advanced security analytics
- Integration with cutting edge security monitoring and threat intelligence products
- Proactive incident response



Our services integrate cutting edge products, innovative proprietary technologies and leading cyber security experts to:

- Constantly monitor and protect your organization's network, endpoints, servers and users
- Manage and maintain the key security infrastructure within your environment
- Find and analyze previously undetected threats that have bypassed traditional security defenses
- Contain the attack at the endpoint, server or network - preventing further attack spread
- Determine whether an attack included exfiltration and represents a larger threat to the business
- Restore normal operations to the business as quickly as possible



CYBERDEFENSES

Threat Hunting and Response Service Platform

ziften

*Endpoint Detection
& Response*

 **SpyCloud**

*Early warning
breach detection*

 **SOPHOS**

Firewall / Anti-X

 **Infocyte**

Threat hunting

STEALTHbits
TECHNOLOGIES

*Data access
governance*

 **elastic**

*Data Collection &
analytics*

Best of breed technologies integrated into a seamless service provides maximum threat discovery, insight, analysis, and mitigation

Contact CyberDefenses to learn more about threat hunting and incident response, and our comprehensive suite of managed security services.

 **CYBERDEFENSES**

1 Chisholm Trail, Suite 327, Round Rock, TX 78681
(512) 255-3700 / info@cyberdefenses.com / www.cyberdefenses.com