Active Threat Hunting

Powered by HUNTRESS

Who's Hiding in Your Network?

Traditional IT security tools like antivirus and firewall focus on prevention -- in other words, trying to stop cybercriminals from breaking down your front door. And while these still play an important role today, hackers are finding new and innovative ways to bypass these systems and infiltrate small and medium business networks.

So what happens when a hacker slips through the cracks undetected? How long will they spend dwelling in your environment? What sensitive information will they capture? And at what point will they deploy ransomware and fully encrypt your systems?

To protect our clients from these evolving threats, we offer a managed detection and response (MDR) solution as part of our security service. This added layer of protection is designed specifically to look for these hidden threats and "quiet" indicators of compromise that other tools miss.

Key Features

Communication
Your organization is kept up-to-date on any issues and your organization will be given simple instructions on threat removal, if necessary.

Threat Detection
Manual data review will eliminate false positives flagged in your systems and highlight any existing threats.

Quick
Avoid downtime and reduce the likelihood of disaster by staying ahead of the bad actors threatening your systems.

Managed Detection and Response

Think of it as a safety net or the backup cord on a parachute; if your primary defenses fail, MDR provides active threat hunting that can be the difference between a quick recovery or a major incident.

Collect: Our software collects data from your desktops, laptops, and servers, and sends it up to a cloud-based engine for automated review; this process is invisible to users.

Analyze: Once captured, our threats team manually review suspicious and potentially malicious activity to eliminate false positives and identify real threats to your network.

Remediate: If an active threat is present, our team will isolate and remediate any infected machines; we'll also provide you with easy-to-follow instructions if additional work is required or if we need to coordinate with you directly.

Hackers have upgraded their systems. It's time to upgrade yours.