CyberDefenses uses AlienVault's proven tools in our vSOC to deliver best-in-class Threat Hunting.

When it comes to defending your organization against cyber threats, time can be an added enemy. And with millions of potential security events occurring each week, it can be hard to identify the real threats quickly. The longer it takes to detect a breach or malicious activity, the more severe an attack can become. As a result, it's often harder, and takes longer, to recover from the damage.

- 24X7 Virtual Security Operations Center

- Advanced Threat Hunting Capabilities

- Seasoned Cybersecurity Analysts

- 15 Minute Response Time

CyberDefenses' partnership with AlienVault creates a dynamic combination of deep expertise and leading tools to quickly detect potential threats and anomalies that could indicate an attack. By leveraging AlienVault's Unified Security Management® (USM) platform in the CyberDefenses Virtual Security Operations Center (vSOC), our team of Threat Intelligence and cybersecurity analyst staff realize the full potential of advanced detection capabilities.

We're prepared to mobilize quickly to mitigate the risk of a breach or to neutralize a threat. Our SOC team will respond to any indication of an incident within 15 minutes to immediately put our battle-tested defense strategies into play 24 hours a day, seven days a week.

Contact us at info@cyberdefenses.com

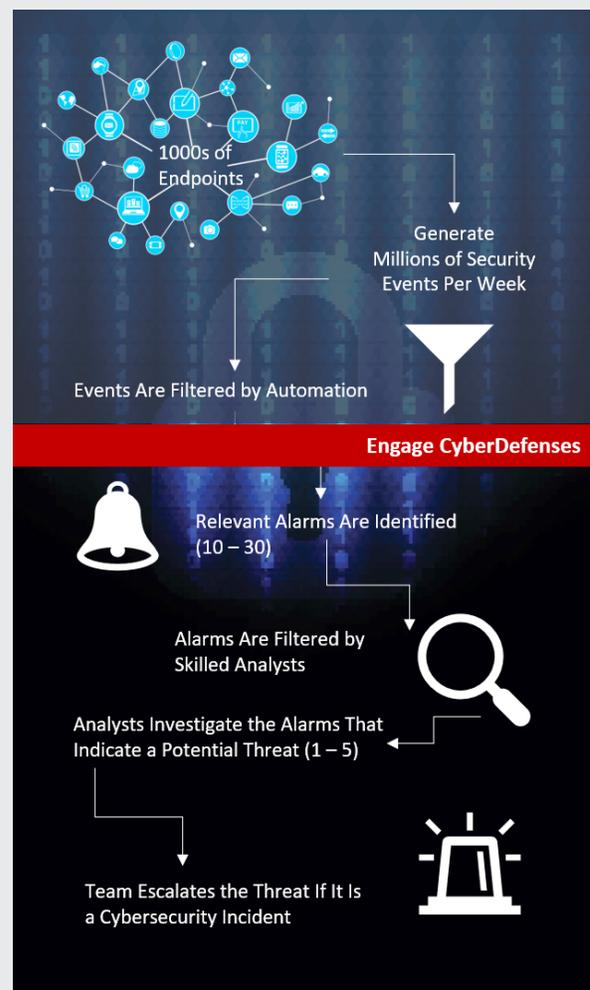## The Security Operations Center Uses AlienVault's Proven Capabilities:

- Security Information and Event Management (SIEM)
- Network Intrusion and Detection (NIDS)
- Host IDS (HIDS)
- Vulnerability Scans

- Critical email address reputation changes
- Social media targeted attacks
- Assets, articles and intellectual property discovered in breached dataset

Identify the Real Threats Hiding in Millions of Security Events

On average, organizations have hundreds or thousands of endpoints that typically generate millions of events per week. It can be difficult, and in some scenarios impossible, to sift through the flood of data to determine if there has been an incident. Enlist the help of CyberDefenses' highly skilled threat hunting specialists to quickly identify the threats so you can take action immediately.

Escalate Incidents to Our Expert Incident Response Team

The CyberDefenses Incident Response and Digital Forensics team is ready to respond when you detect a security incident. With skills in networking, hosts, servers, cybersecurity tools, incident response and digital forensics, our seasoned team is prepared to respond 24X7 remotely or onsite.

1000s of Endpoints

Generate Millions of Security Events Per Week

Events Are Filtered by Automation

Engage CyberDefenses

Relevant Alarms Are Identified (10 – 30)

Alarms Are Filtered by Skilled Analysts

Analysts Investigate the Alarms That Indicate a Potential Threat (1 – 5)

Team Escalates the Threat If It Is a Cybersecurity Incident

Sign up for CyberDefenses' Training
www.cyberdefenses.com/academy

www.cyberdefenses.com   info@cyberdefenses.com