EDR + MANAGED SOC IS A GAME-CHANGER

Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR), also known as Managed SOC (security operations center), are powerhouse security technologies. While each is an excellent solution on its own, the real magic lies in using them in concert to gain a big security advantage. It's a game-changer that gives companies an array of benefits including 360 visibility into their threat picture, valuable threat intelligence and critical tools to speed incident response.

Aren't EDR and MDR the same thing?

EDR and MDR may have similar abbreviations, but they're not the same technology. Instead, each provides IT teams with part of a company's threat picture.

EDR focuses on detecting and responding to threats at the endpoint level, such as laptops, servers, and other computing devices. It uses advanced techniques such as behavioral analysis, machine learning, and threat intelligence to detect and respond to threats that traditional antivirus solutions may miss.

Managed SOC or MDR is a comprehensive security solution that involves a combination of people, processes, and technology to detect, investigate, and respond to security incidents across the entire organization. Managed SOC services are typically provided by a third-party vendor who monitors their customer's network and endpoints for suspicious activity.

EDR and Managed SOC – Better Together

The combination of EDR and Managed SOC together offers an array of unbeatable benefits including:

1. **Comprehensive Threat Detection:** By combining EDR and Managed SOC, an organization can achieve comprehensive threat detection capabilities. EDR can detect threats at the endpoint level, while Managed SOC can detect threats across an entire organization's IT infrastructure, including cloud, networks, and various endpoints, including servers, as well as other devices.
2. **Faster Incident Response:** EDR can quickly detect and respond to threats at the endpoint level, but adding Managed SOC can provide even faster incident response by quickly correlating threat data from multiple sources and providing a holistic view of the incident. This allows organizations to respond to threats more quickly and effectively.
3. **Improved Threat Intelligence:** EDR can provide valuable threat intelligence to Managed SOC services, which can help them improve their detection capabilities. For example, if EDR detects a new type of malware, it can immediately send that information to Managed SOC analysts, allowing them to update their detection capabilities.
4. **Reduced False Positives:** EDR can help reduce the number of false positives generated by Managed SOC services by providing more context around alerts. For example, if EDR detects a suspicious file on an endpoint, it can provide additional information about that file to the Managed SOC analysts, allowing them to better determine whether it's a true threat or a false positive.
5. **Reduced Tool and Vendor Fatigue:** By leveraging a joint EDR and Managed SOC solution, IT professionals simplify their cybersecurity tool stack and reduce the number of disparate security vendors that they must use in order to stay secure. Not only does this save time and money but makes the day-to-day workload more efficient for the IT professional.

EDR + MANAGED SOC IS A GAME-CHANGER

EDR and Managed SOC: The Perfect Match

EDR and Managed SOC are powerhouse technologies that complement each other perfectly. This winning combination can affordably provide organizations with a better defense-in-depth posture. By combining the two, MSPs can achieve faster incident response, improved threat intelligence and reduce false positives while minimizing tool and vendor fatigue, giving you and your clients the security edge you need in today's dangerous world.

Datto EDR – Endpoint Detection Made Easy

Datto EDR empowers IT teams to detect and respond to advanced threats quickly and efficiently. An easy-to-use cloud based EDR solution that's purpose built for Managed Service Providers (MSPs), Datto EDR defends all endpoints: desktops, notebooks and servers, across Windows, MacOS and Linux operating systems and integrates seamlessly with Managed SOC and Datto RMM.

- Patented deep memory analysis ensures that you're informed of even the most elusive threat actors.
- Take action against advanced threats right from your alert dashboard to isolate hosts, terminate processes, delete files, and more without wasting precious seconds.
- Alerts are mapped to the MITRE ATT&CK framework to provide context and helpful clarity to your team.

Managed SOC powered by RocketCyber

Managed SOC is a white labeled managed service that leverages our Threat Monitoring Platform to detect malicious and suspicious activity across three critical attack vectors: endpoint, network and cloud. Our elite team of security veterans hunt, triage and work with your team when actionable threats are discovered including:

Continuous Monitoring – Around the clock protection with real-time threat detection.

World Class Security Stack – 100% purpose-built platform backed by over 50 years of security experience.

Breach Detection – The most advanced detection with to catch attacks that evade traditional defenses.

Threat Hunting – Elite security team proactively hunt for malicious activity.

No Hardware Required – Patent pending cloud-based technology eliminates the need for on-prem hardware.

SCHEDULE A DEMO TODAY!