mason INFOTECH

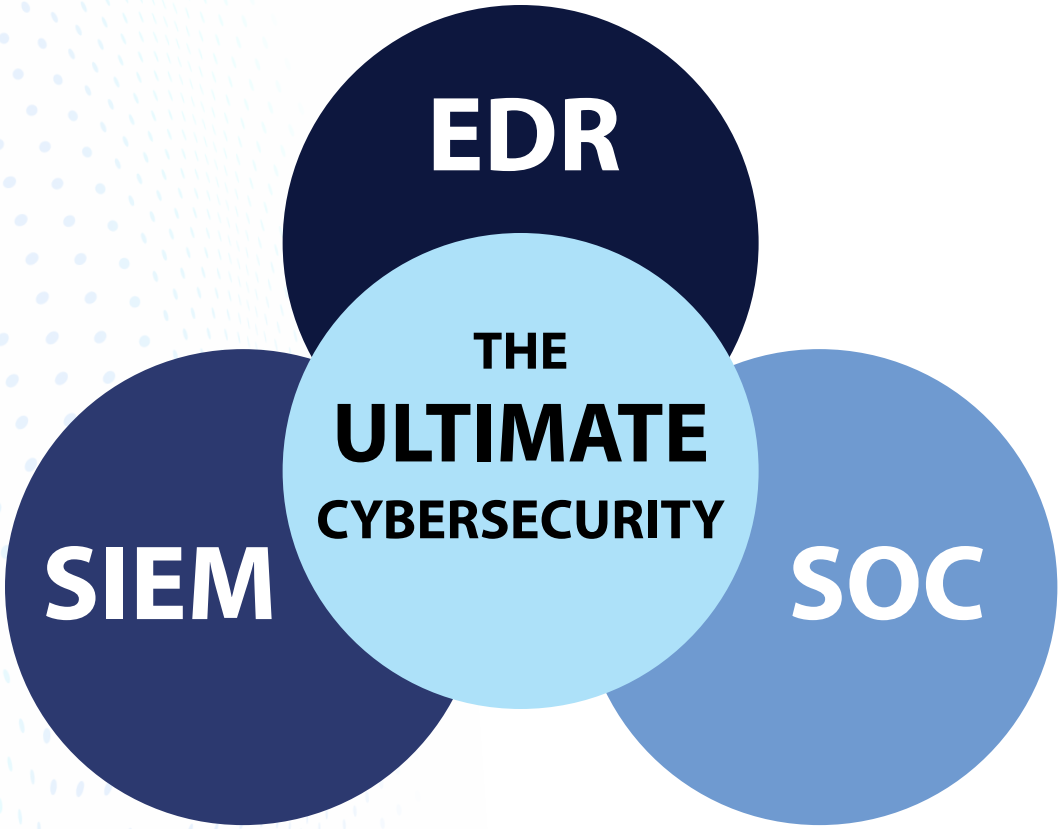
How EDR, SIEM, and SOC Work Together

The Ultimate Security Protection

EDR + SIEM + SOC = The Ultimate Security Protection

Protecting your business from cybersecurity threats is no easy task. It takes a comprehensive solution incorporating people, processes and technology to identify, isolate and remediate threats before they can cause irreversible damage.

Alone, EDR, SIEM and SOC each offer their own unique capabilities instrumental in mitigating your cybersecurity risk. Together, these three tools combine to create one robust solution capable of safeguarding your business in today's complex, ever-evolving threat landscape.



End-to-End Cybersecurity Safeguards

Modern, effective threat protection is multi-layered. Here's how it works:
First, EDR spots a potential threat that triggers an alert. Next, SIEM vets all alerts, escalating the ones requiring immediate attention. Then, SOC analysts review the escalated alert, taking immediate action if necessary. Let's go through each tool in more detail to better understand what makes this combination so successful.

01. Analytics and Restoration

EDR, or endpoint detection and response, provides enhanced behavior analytics across your entire network. This smart software uses artificial intelligence to spot malware and viruses and stop them in their tracks. EDR can even restore your systems to pre-event status if damage is detected. Traditional anti-virus software doesn't hold a candle to EDR.

02. Visibility and Advanced Threat Intelligence

Security information and event management, also known as a SIEM, gathers thousands of security alerts generated from across your network each day and logs the alerts in one central location. A SIEM then cross-correlates the alerts with next-gen technology that can distinguish between the harmless — and the harmful. Threats posing a risk are immediately sent to your security team for remediation.

03. Expert Analysis and Response

What makes a SOC, or security operations center, different is people. Qualified, experienced SOC analysts work 24/7/365 to review incoming security alerts and take immediate action to isolate and remediate potential threats before they can cause significant damage. SOCs with SOC 2 and ISO certifications also play a crucial role in meeting stringent industry compliance standards.

Triple Threat Protection

EDR, SIEM and SOC tools provide invaluable protection from cybersecurity threats. But together, complementing each other, they form a robust cybersecurity defense built to withstand the most sophisticated of threats.

Partner with a managed services provider who can offer the tools — and the talent — to protect your organization. Schedule a demo today!

Mason Infotech Ltd
01159408040
https://masoninfotech.co.uk

Nottingham, Nottinghamshire NG1 2AS