ECS EXTENDED DETECTION AND RESPONSE

A Managed Service Powered by Elastic

With hybrid work environments and cloud services the norm for today's organizations, threat actors have more access points to exploit than ever before. To mitigate risk, you need complete visibility of your attack surface and the ability to detect and disrupt threats in seconds, not days.

Complete Visibility and 24/7/365 Detection and Response

ECS Extended Detection and Response (XDR) provides you with 24/7/365 detection and response to threats targeting your environment. It gives you comprehensive visibility into your entire attack surface and holistic protection for multiple devices and data sources.

ECS XDR uses artificial intelligence and machine learning to detect and investigate modern threats and anomalous behavior and can reduce threat-actor dwell time from months to minutes. With ECS XDR, you can:

- Reduce staffing, operational, and resource constraints.
- Allow your security analysts and engineers to focus on other important work while ECS defends your environment.
- Satisfy regulatory requirements.

Powered by Elastic's SIEM Solution

The ECS XDR service uses Elastic's cloud hosted SIEM solution to ingest network, cloud, and endpoint telemetry. Our SecOps and threat analytics platform (E-TAP) enriches incoming signals from your environments with third-party intelligence feeds and research performed by our ARC Intelligence team.

Finally, this enriched information is fed to our US-based security operations center (SOC), where our SOC analysts take action to stop threats targeting your environment.

ECS is a global Elastic partner and a 2022 Elastic Excellence Award winner.

Quick Time to Value

ECS SIEM engineers have the expertise and skill to onboard you quickly and provide you with immediate monitoring and response capabilities.

Tailored to Your Unique Use Case

Have a unique use case requiring a data source with no existing parsers? ECS will create custom parsers to enable compliance and provide absolute visibility into your attack surface.

Co-Managed Flexibility with Custom Reporting

Get the benefits of a mature XDR program – including full access to run your own reporting – without the complexity.

Out-of-the-box and Custom Detection

ECS customizes detections to your environment, providing you with insights to continue moving your cyber program forward while also detecting and mitigating security threats.

ECS is a leading information technology provider delivering solutions in cloud, cybersecurity, software development, IT modernization, and science and engineering. The company's highly skilled teams approach and solve critical, complex challenges for customers across the U.S. public sector, defense, and commercial industries. ECS maintains partnerships with leading cloud and cybersecurity technology providers and holds specialized certifications in their technologies.