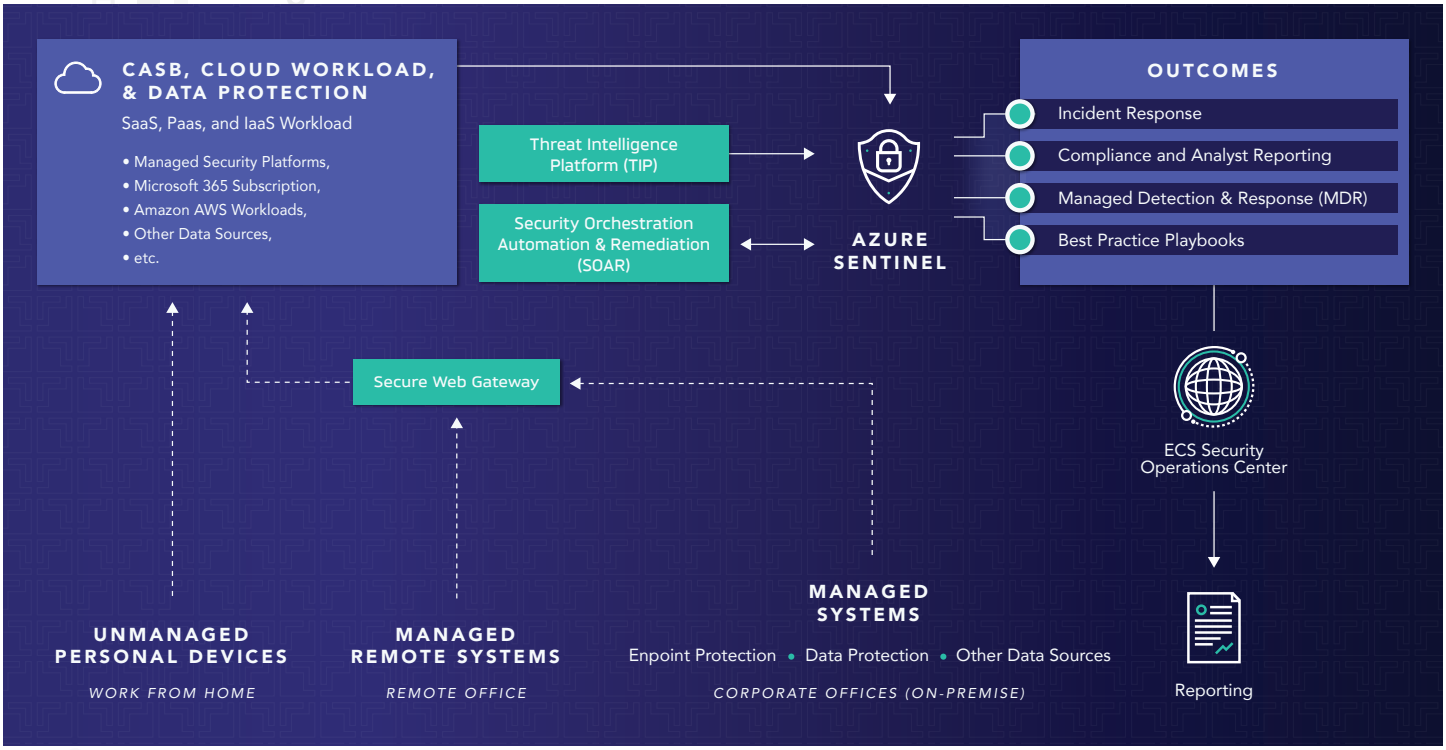
ECS

AZURE SENTINEL
USE CASES

As security operations teams manage increasingly distributed and complex IT environments, detecting and responding to cyber threats is more difficult than ever. With trillions of transactions occurring across a network each day, organizations must be able to effectively collect, correlate, and analyze incidents into actionable intelligence. Many security incident and event management (SIEM) solutions, however, cannot integrate with the cloud apps and services on which many organizations now rely, leaving security teams unable to distinguish signal noise from imminent threats.

To help organizations meet this challenge, ECS has partnered with Microsoft to incorporate the cloud-native Azure Sentinel SIEM solution into ECS's managed security services (MSS). ECS' security team uses Azure Sentinel's advanced threat hunting, automated playbooks, and high-fidelity data correlation to reduce the complexity of your organization's SIEM process, empowering your internal teams to monitor more data with less time, cost, and effort.



ECS delivers Security Analytics and Security Operations Center as a Service (SOCaaS) as part of our Threat Analytics Platform (E-TAP). This offering includes:

Azure Sentinel SIEM – Gather, process, and remediate events with alert detection, threat visibility, proactive hunting, and threat response.

Threat Intelligence Platforms – Streamline threat feeds into one integrated vertical for greater threat visibility, contextualization, and accuracy.

Security Orchestration Automation and Response (SOAR) – Achieve faster alert validation and threat mitigation through automated runbooks, alert triage, and response actions.

Client Platforms – Gain insight into your organization's security posture with project reports, ticket status, and executive dashboard functions.

This program is delivered via 24x7 intelligence-driven security monitoring, which combines industry leading threat intelligence and experienced security analysts to enrich your Sentinel environment. Whatever your specified outcome, ECS custom tailors their established back-end processes and procedures based on your specific needs. With our state-of-the-art **security operations center** (SOC), our team of experts will continually keep your data safe and secure in a world of evolving threats.

DATA CORRELATION

CHALLENGE: With the sheer volume of alerts occurring each day, your security team struggles to filter out actionable items from the noise.

SOLUTION: Whether your data resides on-premises, in Azure, or in any other cloud, ECS' experts use Azure Sentinel to collect and correlate low-fidelity anomalies into high-fidelity security alerts for analysts to easily digest and remediate. By using scalable machine learning (ML) algorithms, analysts no longer have to manually correlate alerts across different products or rely on traditional correlation engines. Organizations that incorporate Azure Sentinel into their SIEM report a 90 percent decrease in alert fatigue, reducing the likelihood that an incident is overlooked.

INVESTIGATION

CHALLENGE: Your current SIEM solution lacks the necessary visibility to investigate incidents.

SOLUTION: When incidents occur, ECS experts use real-time and historical data to quickly investigate and analyze the entire attack sequence. Azure Sentinel has customizable workbooks that allow users to combine data from disparate sources into a single report. Using Azure Sentinel's data visualization capabilities, users can graphically depict rich insights that would be impossible to uncover on traditional SIEMs.

AUTOMATED PLAYBOOKS

CHALLENGE: Your security analysts tediously fight the same incidents over and over again.

SOLUTION: Microsoft Azure Sentinel includes built-in SOAR tools that enable your IT team to automate and quickly respond to repetitive incidents. These playbooks can be set to run automatically when specific alerts are triggered, shortening response time and reducing complexity for the user.

HUNTING

CHALLENGE: Silent, hard-to-detect attacks routinely make it past your network's security perimeter.

SOLUTION: Using Azure Sentinel's visibility and recording capabilities, ECS' cyber experts actively hunt across all data being generated. Azure Sentinel provides built-in templates to create threat detection rules that automatically search across your environment for suspicious activity including known threats, common attack vectors, and suspicious activity escalation chains. Many of these templates can be customized to search, filter, and monitor activities based on your company's needs.

Interested in learning more about ECS' cybersecurity solutions?
Reach out and speak to an expert today at **cyber@ECStech.com**

ECS is a leading information technology provider delivering solutions in cloud, cybersecurity, software development, IT modernization, and science and engineering. The organization'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.