ECS MANAGED DETECTION AND RESPONSE

WHAT IS IT?

ECS offers 24x7x365 Endpoint Detection and Response services utilizing the McAfee MVISION EDR Platform. MVISION EDR is a cloud-hosted solution that enables users to detect advanced endpoint threats, automate investigations, and quickly respond. ECS combines this integrated technology with experienced analysts and refined security operations processes to deliver a comprehensive threat analysis program, further protecting your organization from advanced endpoint attacks.

KEY FEATURES

- 24x7x365 Alert Monitoring
- Content Buildout
- Data Source Integration and Management
- Management of Threat Exclusions
- Alert Triage and Management of Investigations
- Threat Prioritization and Escalation
- Proactive Threat Hunting
- Security Incident Reporting
- Comprehensive Deliverables

HOW DOES IT WORK?

Daily Operations

ECS works with your organization to ensure proper configuration and management of the deployed technology. Our engineers assume the day-to-day management, troubleshooting, and operation of tools included within the scope. We integrate with your help desk, ticketing system, and change control process to become an extension of your team, minimizing the use of your internal security resources until an escalation point is reached.

Our analysts regularly review and update content to drive continual improvement, ensuring that your organization has fully operationalized your security investment with all tools configured to the latest best practices.

Managed Detection and Response

ECS leverages the advanced capabilities within MVISION EDR and ThreatQuotient to review alerts, investigate threats, prioritize incidents, and initiate a response.

Monitoring: ECS provides 24x7x365 eyes-on-glass monitoring to actively triage MVISION EDR alerts. MVISION EDR provides continuous, real-time monitoring of connected devices, enabling threat identification and immediate and historical search. ECS analysts use this information to open cases and compile actionable intelligence to fuel investigations.

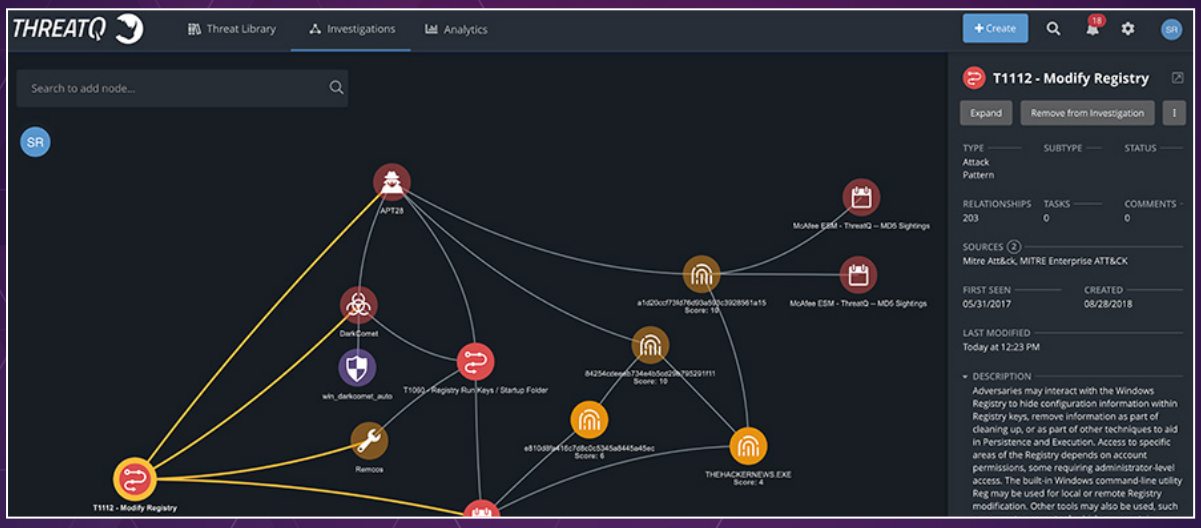
Investigating: Automated playbooks help drive investigations with MVISION EDR. Our ability to collect data from McAfee ePO and potential additional data sources (with our Tier 1 offering) allows correlation with additional threat intelligence (such as McAfee GTI and Virus Total) to help reduce false positives and streamline investigations. Behavior alerts are mapped to the MITRE ATT&CK framework. ECS analysts take these prioritized alerts and leverage the real-time and historical search, as well as on-demand data collection functionality, to aid investigations and provide the actionable intelligence required to mitigate threats.

Threat Hunting: ECS analysts use external threat intelligence sources, that are prioritized by relevance to our specific customer's industry and location to provide proactive, manual threat hunting, leveraging the latest IOCs to identify malicious threats impacting your organization.

Incident Response: Real-time action through MVISION EDR allows ECS to quickly quarantine machines or kill processes when needed. As an optional service, ECS offers on-site forensics and incident response to help investigate and mitigate sophisticated attacks.

INVESTIGATIONS

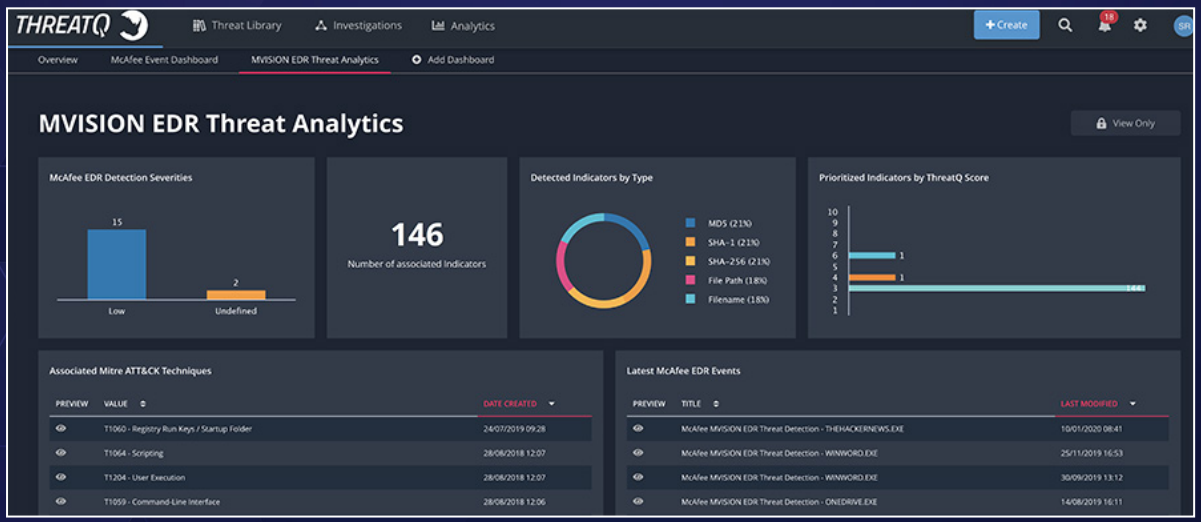
Our expansive threat intelligence program enables seamless prioritization, automation, and collaboration to reduce remediation time in your environment. Our automated hunting capability drives down mean time to detect (MTTD) and mean time to respond (MTTR).



MITRE ATT&CK – CASE MANAGEMENT

ECS provides regular reporting, alerting, and alignment against MITRE ATT&CK, as well as case management for each unique event investigated by our analysts. The MITRE ATT&CK functionality offers the opportunity to perform deeper analysis from a threat perspective. When associated with an EDR event, we can use this data to provide insights into questions such as 'Who is potentially attacking?", "What attack techniques are being leveraged?", "Is there any related data (such as other types of malware or even legitimate tools) that we can use to inform IR or threat hunt team actions?".

The ATT&CK data automatically relates to other data in the Threat Library so as to offer suggestions for both pro-active and reactive responses. When combined with an EDR event, this data can be used to identify specific mitigations and signatures that may be deployed to defend against a potential threat.



TIERED OFFERINGS

Tier 1: Delivered 100% through the MVISION EDR platform and consists of all services outlined on previous pages. Alerts and correlation are limited to endpoint data and external threat intelligence sources.

Tier 2: Delivered via the MVISION EDR platform in conjunction with an integrated back-end security analytics platform. Endpoint events from MVISION EDR are correlated against targeted data sources from your environment, in addition to external threat intelligence sources, to deliver a comprehensive Managed Detection and Response Program.

Deliverables	Tier 1	Tier 2
Provide threat reports	Monthly	Weekly
Provide analyst calls	Bi-weekly	Weekly
Provide threat trends	✗	Quaterly
Case creation and management	✓	✓
Playbook integrated into MVISION EDR Platform	✓	✓
Security incident & remediation reports as needed	✓	✓

Andy Woods
VP, Enterprise Managed Services

andy.woods@ecstech.com
703-795-0636

Matt Fuller
Exec. Director, Enterprise Managed Services Sales

matthew.fuller@ecstech.com
862-432-3931

ECS is a seasoned McAfee Platinum Partner and Tier 1 Service Provider, bringing years of experience and expertise gained across a broad range of end-user environments to help deliver successful cybersecurity programs. ECS operates McAfee's largest single customer of 1.4 million endpoints deployed globally. Our engineers and analysts are certified by McAfee to provide dedicated support across their entire portfolio of products. ECS leverages McAfee's tool set to help our partners deliver industry leading outcomes that meet your needs today and prepare your organization for the future.