ACTIVEEYE MANAGED DETECTION AND RESPONSE

A TECHNICAL OVERVIEW

MOTOROLA SOLUTIONS

ACTIVEEYE MANAGED DETECTION AND RESPONSE

ActiveEye^{SM} Managed Detection and Response (MDR) leverages our advanced ActiveEye security platform and experienced analysts to detect and respond to cyber threats in your IT environment as well as computer-aided dispatch (CAD), VESTA® 9-1-1 systems and ASTRO® 25 systems. This white paper provides a technical overview of our services and the ActiveEye platform.

ACTIVEEYE MDR COMPONENTS

ActiveEye Security Management Platform

ActiveEye is a Security Orchestration, Automation and Response (SOAR) platform that serves as the heart of security operations. The ActiveEye platform ingests data from connected network elements, analyzes it and sends relevant data and insights to cybersecurity personnel. Analytics and filtering help to differentiate between malicous and routine traffic, making it simpler to focus on actual threats. The following threat detection modules are available in the ActiveEye platform:

- Log Analytics
- Network Detection
- Endpoint Detection and Response (EDR)
- DNS Detection
- Vulnerability Detection

The ActiveEye platform collects and manages security data, optimizing threat detection and increasing focus on the most critical alerts that require quick responses. Built-in analytics capabilities examine multiple real-time threat intelligence feeds, reference past events and follow defined playbooks to automate most analyst actions. Analytics also rank manual investigations, prioritizing those most likely to require remediation.

ActiveEye Remote Security Sensor (AERSS)

AERSS is an optionally deployed component that provides remote collection of logs, network intrusion detection and vulnerability scanning.

Security Operations Center (SOC)

Motorola Solutions' experienced cybersecurity analysts monitor 24/7 for signs of potential threats. Analysts alert key contacts by your organization to mobilize a response and make recommendations based on a predefined plan of action if they detect a threat. Standard SOC services can be enhanced with our optional Advanced Threat Insights service that provides dedicated account personnel and proactive threat hunting.

ACTIVEEYE SECURITY MANAGEMENT PLATFORM

ActiveEye is quick and simple to deploy, removing the burden of installing, maintaining and managing an on-premises security information and event management (SIEM) component. Depending on the log sources that need to be monitored, ActiveEye can replace the need for separate SIEM.

ActiveEye access and content are protected by powerful security functions. Users access the platform via a secure web browser using multi-factor authentication (MFA). Administrative functions allow managing user access as needed.

The platform undergoes regular security audits and has an active SOC 2 Type2 audit certification. We use data security best practices to encrypt data in transit to/from the platform and while at rest. Raw event and alert level data is stored for 13 months by default and can be stored longer if required.

There are several ActiveEye “pods,” self-contained locations deployed around the world, including the U.S., U.S. GovCloud, Canada and Australia.

THREAT INTELLIGENCE AND DATA ENRICHMENT

ActiveEye uses threat intelligence for both threat detection and alert enrichment. Threat intelligence sources are carefully curated by security domain experts who monitor the cybersecurity landscape for emerging threats, new threat actors, command-and-control infrastructure and other relevant entities. This curation ensures that new threats are detected and addressed as soon as possible after the announcement of a vulnerability or threat. Collectively, threat intelligence in ActiveEye is derived from multiple sources, including:

- Expansive open-source intelligence (OSINT) that incorporates numerous smaller sources
- Paid commercial sources that allow both aggregated data and on-demand information about entities such as files or IPs
- Data derived from the ActiveEye SOC experts as they navigate tens of thousands of alerts per day

Additionally, Motorola Solutions develops and maintains broad industry-specific threat intelligence for state and local government, public safety and large enterprise.

THREAT DETECTION

The ActiveEye platform maximizes the value of detections provided by integrated security services such as next-generation endpoint detection and response (EDR) providers. It also offers custom detections against services that only provide logs, like many SaaS and cloud platforms. In both cases, raw event data is ingested into ActiveEye and analyzed by hundreds of policies that sift through the data to discover anomalies, known malware families and other risks.

For vendors that provide detections, the ActiveEye policies enrich the alerts received with alert taxonomy, machine-learning (ML)-derived severities and other metadata. The alerts may also be correlated to other relevant data to expose hidden relationships, enriched with threat intelligence and modified based on historical behavior.

For log integrations without built-in alerting, the same process applies. However, the policies operate on the raw data to discover thresholds being violated, known risky patterns and other conditions requiring investigation. As with vendor-derived alerts, the resulting data is enriched and correlated prior to being triaged.

All policies run both as streaming processes, as soon as data arrives, and also as a historical scan to identify aggregates that may be missed in the stateless streaming process. The full list of applicable policies can be reviewed in the ActiveEye interface.

SECURITY ORCHESTRATION AND AUTOMATION

As a SOAR platform, ActiveEye orchestrates the flow of data and actions, speeding remediation by automatically performing investigation and response tasks. Using predefined or custom playbooks, ActiveEye handles repetitive and precise tasks in place of human SOC analysts. ActiveEye supports two types of automation:

- **Enrichment and Investigation Automation** — ActiveEye can look up threat intelligence, query past data and surface event details to the main investigation screen. This data improves manual investigation quality and speed and provides a basis on which automation can make decisions.

- **Response Automation** — ActiveEye can take response actions defined in playbooks. Actions can include making recommendations to analysts, changing alert priority, closing an alert, blocklisting files, removing files from systems or isolating a host from the network.

ACTIVEEYE CO-MANAGED SECURITY PORTAL

As a co-managed platform, ActiveEye synchronizes security efforts between your security team and our SOC analysts. The web-based portal provides visibility to threat insights, event investigations, security reports, threat advisories and the status of any security cases.

Dashboard

Key information in the ActiveEye portal is summarized on the dashboard. This dashboard includes open alerts, an overview of alert categories, alert processing key performance indicators (KPI), open security cases and recent threat advisories. From here, users can access more in-depth information like security cases, alert details, alert trends, reports and group communications.

Security Cases

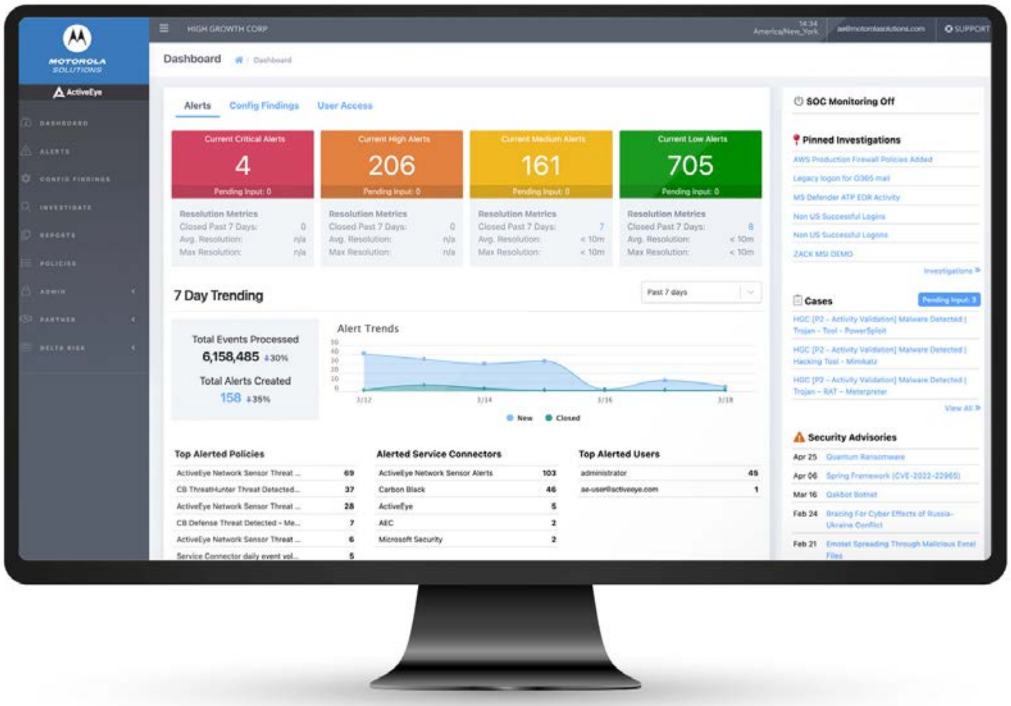
When Motorola Solutions identifies a threat, the SOC creates a security case. Security cases can be viewed in the ActiveEye portal and can be summarized in an optional Daily Security Summary sent via email.

Alert Details and Trends

Alerts are system notifications of unusual activity. These alerts can be evidence of a past, active, or developing threat. If analysts believe alerts are indicative of a threat, they can open security cases based on them.

ActiveEye records relevant data for each alert, enabling users to quickly view its triggers, systems it impacts and any actions taken to address it. Each alert record also includes a summary of key attributes. From that alert summary, users can access related records for more details. These records include threat intelligence, past event data, related events and activity logs.

To put alerts into context, ActiveEye provides tools for reviewing groups of alerts based on key attributes or time periods. Attribute filters enable users to toggle which alert groups ActiveEye shows, helping to spot trends or threat activity. Users can also compare alert logs for time periods to determine if trends associated with a threat or are false positives.



7 Day Trending

Current Critical Alerts	Current High Alerts	Current Medium Alerts	Current Low Alerts
4	206	161	705
Pending Input: 0	Pending Input: 0	Pending Input: 0	Pending Input: 0
Resolution Metrics	Resolution Metrics	Resolution Metrics	Resolution Metrics
Closed Past 7 Days: 0	Closed Past 7 Days: 0	Closed Past 7 Days: 7	Closed Past 7 Days: 8
Avg. Resolution: n/a	Avg. Resolution: n/a	Avg. Resolution: < 10m	Avg. Resolution: < 10m
Max Resolution: n/a	Max Resolution: n/a	Max Resolution: < 10m	Max Resolution: < 10m

Total Events Processed
6,158,485 ▲30%

Total Alerts Created
158 ▲35%

Top Alerted Policies	
ActiveEye Network Sensor Threat ...	69
CB ThreatHunter Threat Detected...	37
ActiveEye Network Sensor Threat ...	28
CB Defense Threat Detected - Me...	7
ActiveEye Network Sensor Threat ...	6
Service Connector daily event vol...	5

Alerted Service Connectors	
ActiveEye Network Sensor Alerts	103
Carbon Black	46
ActiveEye	5
AEC	2
Microsoft Security	2

Top Alerted Users	
administrator	49
ae-user@activeeye.com	1

SOC Monitoring Off

Pinned Investigations
AWS Production Firewall Policies Added
Legacy logon for O365 mail
MS Defender ATP EDR Activity
Non US Successful Logins
Non US Successful Logons
ZACK MSI DEMO

Cases
HGC [P2 – Activity Validation] Malware Detected | Trojan - Tool - PowerSploit
HGC [P2 – Activity Validation] Malware Detected | Hacking Tool - Mimikatz
HGC [P3 – Activity Validation] Malware Detected | Trojan – RAT – Meterpreter

Security Advisories

Apr 25	Quantum Ransomware
Apr 06	Spring Framework (CVE-2022-22965)
Mar 16	Qakbot Botnet
Feb 24	Bracing For Cyber Effects of Russia-Ukraine Conflict
Feb 21	Emotet Spreading Through Malicious Excel Files

Figure 1-1: ActiveEye Interface

Investigations and Reporting

ActiveEye's robust ad hoc reporting capabilities enable users to investigate and hunt active threats, and to view historical data sets. Reports provide a simple, consistent view of collected event data. Pre-defined templates organize the data and display the most important attributes of event types. Users can customize these standard reports to display and summarize different attributes when needed. To share information outside of ActiveEye users can download reports of up to 50,000 rows in .csv or .json format.

In addition to ad hoc reporting and querying, ActiveEye can provide optional monthly reports and daily email summaries. The monthly report summarizes important security items, and is available as a PDF download. The Daily Security Summary provides a customized set of statistics from the previous day to a predetermined user list. This summary can include alert counts, security cases opened/closed, saved queries that have new data and detailed endpoint security statistics. ActiveEye can send one or more summary emails with different content for different groups.

Security Advisories

Security Advisories are messages from the SOC with information on active threats to the general population or your specific industry. These advisories guide security teams on how to best take action against a threat, and tell them where they can find further information.

Information Sharing

To support effective security management, ActiveEye has several functions for sharing information. Automatic security alerts notify key contacts of incidents based on priority. In addition to automatic security alerts, ActiveEye features other information sharing functions you and the Motorola Solutions SOC team can access, including:

- **SOC Bulletins** — Instructions from your security team or the SOC that SOC analysts can reference when creating security cases. These can communicate short term situations where a security case may not be needed, such as during testing or maintenance windows.

- **Customer Notebook** — The SOC can use the Customer Notebook to document details on your specific environment and network implementation information to help our analysts investigate security cases.

- **Contact Procedures** — Escalation procedures and instructions on who to contact if an incident occurs are also readily available. Contact procedures include instructions and procedures for specific security incident levels. The SOC and customer will jointly manage contact procedures.

Together, these functions quickly spread important information to security teams and analysts.

User Access to ActiveEye

User access settings make it simple to add, update, and remove access to ActiveEye. Every ActiveEye user can save queries, customize reports and set up daily email summaries. Users may be given administrative access, allowing them to perform administrative tasks, such as setting up new service connectors, resetting passwords and setting up multi-factor authentication for other users.

ACTIVEEYE THREAT DETECTION MODULES

Log Analytics

The Log Analytics function collects log data from systems, applications, networking components, security systems and even other SIEM solutions. Several analytics components and security policies process log data to identify policy violations and suspicious activity. If ActiveEye detects an event of interest that may represent a threat, it will alert analysts based on your settings.

Over time, past logged events can provide critical context to track the origin of a threat or identify a new threat using previous attack patterns. ActiveEye stores collected events so analysts can search through them and use them for threat hunting. Events remain in storage for a defined period of time based on subscription. While the default term is one year, longer time periods are available by subscription.

"ActiveEye can incorporate a variety of logs from different sources, including authentication and authorization systems, object storage, cloud virtual networks, virtual servers, cloud security services, software applications and physical infrastructure via AERRS.

Network Detection

The Network Detection service module uses an agentless approach to monitor all activity across the network, providing visibility to what devices are connected and what applications are communicating from each device. With ActiveEye integration, security teams can automate investigation of network traffic alerts, then view those alerts in the context of other user activity. In addition to alerting on indicators of reconnaissance or active compromise, ActiveEye investigation screens easily identify unwanted applications in use, unknown devices on the network and communication patterns that create risk.

To support this, Motorola Solutions deploys an Intrusion Detection System (IDS), connected to one or more switch span ports, to monitor traffic signatures and anomalies in real time for signs of malicious activity. The IDS also models network communications using packet level and flow level analysis. This enables analytics to identify anomalous behavior that is not captured by pre-defined traffic signatures, including activity over encrypted connections.

The signature set for the Network Detection module is updated hourly, ensuring that emerging threats are addressed as soon as the cybersecurity community knows about them.

Endpoint Detection and Response

If an attacker attempts to breach security, it is critical to be able to respond faster. Integrating Endpoint Detection and Response (EDR) tools with the ActiveEye platform enables security analysts to respond to attacks and view threat intelligence in one interface. This enables them to react quickly to an emergency, rather than having to swap between separate tools to investigate and counter an attack.

Analysts can access a variety of response actions within ActiveEye, such as isolating hosts, blocking files, allowing files and removing files. Available responses are determined by the EDR tool and security policies. If the customer does not have an EDR solution, Motorola Solutions may recommend or provide one as part of this service for an additional cost.

DNS Detection

Computer networks use the Domain Name System, or DNS, to translate domain names to IP addresses which computers use to communicate with each other. Our DNS Detection feature employs a security-aware DNS resolution service to prevent malware, botnets and phishing attacks from compromising systems and removing data. To prevent data loss, the service can block data removal or transfer over specific network ports or protocols. This can prevent an attacker or unauthorized user from removing data whether they initiate the attack with a DNS request or attempt to bypass the DNS with a direct IP connection. It can also block data transfer initiated on or off your network by preventing DNS resolution to potentially malicious destinations.

Once integrated with the ActiveEye platform, DNS Detection will alert for systems that attempt to access known malicious destinations or destinations blocked by your organization's security policies. The service also lets you view and download usage trend reports by categories or individual systems.

Some DNS settings may need to vary based on where a device is located. DNS Detection can be customized with location-aware policies (which network the system is on) that block or allow traffic based on predefined lists.

DNS Detection is typically integrated at the network perimeter, protecting devices within the network. By installing a software agent on applicable mobile devices, you can extend DNS protection on those devices to outside the network perimeter. DNS Detection can enforce unique protections on these devices, with varying internet access restrictions and logging settings if they are outside your network.

Vulnerability Detection

During system setup or updates, some configurations, software, or updates can inadvertently create an opening in security. The Vulnerability Detection service module connects third-party tools with ActiveEye so it can highlight these vulnerabilities for security teams. Security teams can then address these vulnerabilities to protect against cyber threats like ransomware, breaches and loss of availability.

The vulnerability detection function will regularly scan configured networks and systems for new software component vulnerabilities and insecure system or network settings. A cloud-based scan engine will check for vulnerable internet accessible endpoints, while AERRS will scan on-premises infrastructure. Motorola Solutions works with your team to determine the optimal scan schedule and scope for the system.

Completed scans will summarize any vulnerabilities detected, along with recommended actions to close them. Scans will score detected vulnerabilities using the Common Vulnerability Scoring System, identify if they are on a Common Vulnerabilities and Exposures list and list any impacted hosts.

ACTIVEEYE REMOTE SECURITY SENSOR

The ActiveEye Remote Security Sensor (AERSS) is a rack-mounted server deployed in your environment. It collects and monitors security relevant logs and network traffic and reports back to the ActiveEye platform. For the initial management configuration, AERSS will be configured using command line tooling.

After initial configuration, AERSS is a self-managed box; all upgrades of the components and the operating system are performed automatically in the background. Remote access is needed in some cases for full maintenance of the system. No additional actions by the local staff are typically required.

AERSS NETWORK PLACEMENT

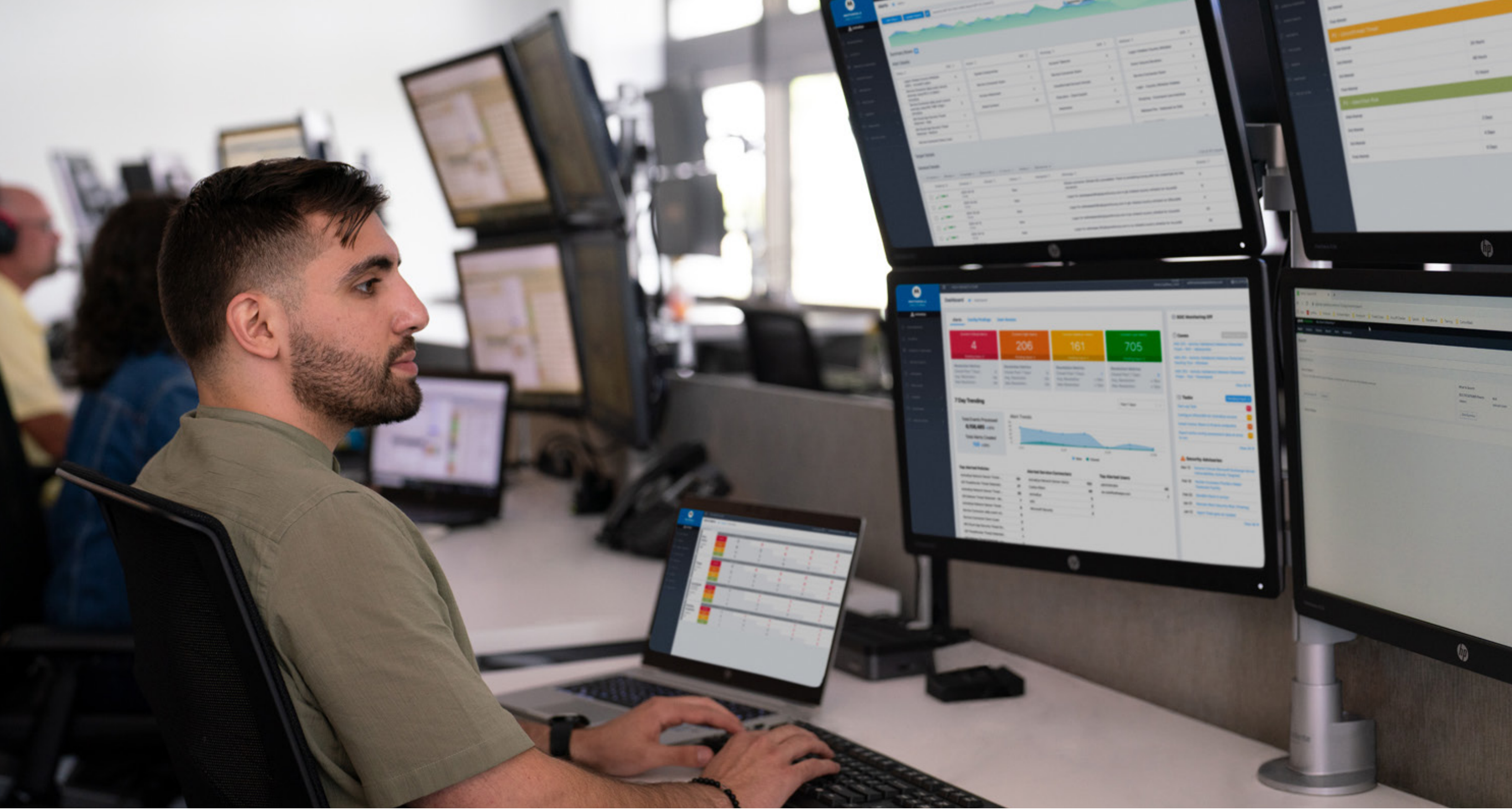
Network monitoring is one of the primary functions of AERRS. An AERSS appliance watches traffic passing through various points in the network to check for malicious activity. Considerations for where to have the monitoring port connected would be:

- Internal interfaces of perimeter firewalls to allow them to block out excessive “noise” from the internet so that only traffic passing through is monitored; or
- Internal networks and servers containing sensitive data to ensure that communications between those systems or other internal choke points in the network, including remote office or partner/vendor connections, are monitored.

Another consideration would be for collecting logs of devices within the network. Systems or network devices would typically forward logs via syslog to the AERSS appliance for collection and forwarding to ActiveEye.

The last consideration would be for network scanning in applicable environments. This requires an AERSS appliance to scan the network for vulnerabilities. Considerations for where to have the management port connected would be:

- A location within the network, for ease of scanning without changing network controls that would be required when scanning through firewalls or other security controls that might affect the scan; or
- For added security, the management port can be more isolated. If so, a precise setup of outbound traffic to scan the desired networks is needed for configuration. This is needed so that the scan discovery and other checks correctly identify live systems on the network rather than false positives.



AERSS BANDWIDTH USAGE

The AERSS appliance uses bandwidth for a variety of purposes. It may affect the network in environments with limited bandwidth. The primary bandwidth consideration is to the internet, which is used for the installation, administration and log collection of the AERSS appliance. At a minimum, the appliance should have a 10Mbps connection to the internet available.

Secondarily, there are bandwidth considerations within the network which may affect the number or placement of AERSS appliances. The following functions can affect bandwidth requirements internal to the environment:

- Log Collection from Devices — Delivery of device logs on the other side of a low bandwidth network connection may be impacted.
- Network Scanning — Scanning a network with a low bandwidth connection may increase scan times or impact other traffic using that connection.
- Network Monitoring — If network traffic being replicated for monitoring is not using a dedicated connection then it could impact other traffic. We recommend always using a dedicated and direct connection from the switch replicating the traffic to the AERSS appliance.

AERSS SECURITY HIGHLIGHTS

The AERSS appliance also has built-in security features, including:

- Updates — All software on the AERSS is cloud managed and updated frequently to ensure it stays up to date and secure. This includes firmware, operating systems, applications, and patches.
- Certificates — The AERSS appliance uses certificates to secure configurations that are applied to the platform.
- API Keys — Log data processed through the platform is authenticated to ActiveEye using dedicated API keys which periodically get rotated for added security.
- Platform Hardening — The base AERSS appliance platform runs a hardened operating system.
- Platform Monitoring — AERSS appliance logs are included in the monitoring of the environment.
- Communication — AERSS utilizes encryption for all data in transit. All communications from the AERSS appliance employs encryption to ensure sensitive data is protected from potential eavesdropping.

SECURITY OPERATIONS CENTER

Motorola Solutions' Security Operations Center (SOC) can monitor networks, applications and devices for security threats 24/7 via ActiveEye. Our SOC analysts possess deep technical skills on both the offensive and defensive side of security. Based on their broad security experience, our SOC analysts recommend security device configurations that optimize threat detection and implement playbooks to cut through the noise and quickly address the most critical threats. This puts our focus on identifying activity that could be a potential security risk or incident.

The SOC uses ActiveEye's ability to prioritize alerts in the queue and focus on alerts that are more likely to result in a security incident or risk. The SOC management team regularly monitors internal SLAs and has established internal KPIs to ensure alerts are investigated in a timely manner.

Our SOC regularly works with new clients who are in the process of mitigating and recovering from a compromise. Using EDR tools, the team actively detects, investigates and stops threat actors and their attacks. When suspicious activity is identified, the team has experience to quickly mitigate and intercept threats before active exploitation.

If a threat investigation requires input from your security team, the SOC will create a security case and follow predefined escalation procedures for each priority level. If the SOC cannot reach the first-level contact, the SOC will escalate according to customer defined procedures. ActiveEye enables you to view security cases and event investigation history any time. The SOC is always available to provide additional consultation on a Security Case, review the Case details in depth, or provide additional assistance with investigation as needed.

In the event of a potential incident, the SOC will use data available in ActiveEye and access your system to determine the extent of malicious activity. If needed, the SOC will add more detection policies to your service modules. With the EDR service module, the SOC can take mitigating actions on remote hosts systems based on a pre-approved response plan, or if they determine it to be necessary for a specific case. When needed, the SOC will recommend mitigating actions you can take to address a threat.

With security investigation and response, time is of the essence. Most initial compromises will result in lateral movement if not detected and mitigated within 60 minutes. The SOC closely monitors resolution time for your security alerts as a joint measure of our ability to interact and respond to activities in your environment. These response time metrics and trends are available on your ActiveEye dashboard and in your monthly reporting.

The SOC team operates from secure, redundant locations in the U.S. The teams can operate securely at remote locations if needed. Analysts complete regular training on customer data management and privacy to protect sensitive customer data.

The SOC team routinely participates in red team and purple team exercises and uses sophisticated training platforms to ensure their skills are up to date. Our senior analysts develop and perform real-world exercises which simulates modern threat actor activity and security breaches for SOC analyst training.

ActiveEye by the Numbers: Detecting and Preventing Malware*

2,078
unique malware samples
TRACKED

RESULTING IN

6,392
RESPONSE ACTIONS
implemented

ALLOWING FOR

658,199
processes
PREVENTED FROM RUNNING

What Will I See in a SOC Alert?

- What We Found
- Analyst Notes
- When We Found It
- Where We Found It
- What We Did
- Recommended Response
- Technical Details

* Data from 2021

Expanded Insights and Strategic Security Planning

Monthly Review and Security Program Recommendations

Trend Analysis and Threat Hunting

Deep and Dark Web Search

Named Security Analyst

ADVANCED THREAT INSIGHTS

ActiveEye Advanced Threat Insights is an optional service that expands the standard SOC monitoring services provided by ActiveEye MDR. This service provides a more proactive, in-depth security research function to enrich awareness of your ongoing cybersecurity posture, optimize the value of existing security controls and ultimately lower cybersecurity risk.

With the Advanced Threat Insights service, Motorola Solutions will assign a dedicated cybersecurity analyst to proactively work with you and your team. The analyst will lead an advanced threat hunting program to identify specific advanced threats and summarize evolving threat patterns of interest. The assigned analyst will use ActiveEye MDR and connected tools to search endpoint, network and cloud security log data for evidence of undetected compromises to the network. Based on the relevant external threat intelligence or high-risk entities (user accounts or systems) identified in ActiveEye or by your team, the assigned analyst will search externally across the surface, deep, and dark web for cybersecurity threats to the your network. Potential threats include compromised corporate user accounts, corporate IP addresses connected to botnets and data for sale.

Each month, the assigned analyst will meet with your security team to provide an overview of any threats detected in the previous month and discuss security strategy going forward. They will also share a summary report of completed threat hunting results and suggested mitigation of and threats discovered.

Although the Advanced Threat Insights service offers in-depth intelligence from the surface, deep and dark web, there are new underground forums being created every day where threat actors trade information and data. As such, we cannot guarantee that we can uncover each and every threat in real time, as some underground forums and communities can take months to surface or for security researchers to gain access. In addition, the scope of these services do not include employee-related investigative services, such as those that may target any specific employees (or other individuals) or implicate privacy rights, alleged or suspected internal conduct, or rights that may be protected or regulated by law.

ONE PARTNER FOR YOUR CYBERSECURITY NEEDS

GLOBAL SCALE AND EXPERIENCE

With more than 90 years of experience managing mission-critical technologies and more than 20 years of developing cybersecurity solutions, Motorola Solutions is well-positioned to be the ‘one service provider’ for your cybersecurity needs.

With best-in-class people, processes and technology we bring scalable operations that can help organizations manage cyber risk awareness, detection, response and recovery. Our cutting-edge security automation and orchestration platform, ActiveEye, delivers 24/7 insights on potential threats to your environment, and a co-managed approach to security management. We provide a purpose-built and integrated approach to end-to-end cyber resilience.

Learn more at: motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com