ADVANTIO
an Integrity360 company
your security in mind

Managed Security Services by Advantio

We defend your business. You grow it.

With every day passing there is news of yet more cyber threats and as a result, organizations remain on alert seeking to stay abreast of the latest developments. In many ways, the challenge is now greater than ever before due to the evolution of the threat landscape, the reliance on cloud infrastructure, the prevalence of malware, and more specifically ransomware. This makes it impossible for organizations of any size to avoid being targeted by malicious threat actors.

Adding to this is the skills shortage that organizations are faced with in the cybersecurity specialty. According to The Global Risks Report 2022 (World Economic Forum) there is a 3 million gap in cyber professionals needed worldwide. To counter this, companies are turning to outsourcing models to bolster their capabilities without the added burden of recruitment, upskilling, and retention in-house. This method also means organizations don't carry the additional cost of hardware and software costs or those associated with building a robust security operations center.

For many organizations, the necessity to remain compliant with industry regulations and standards adds additional pressure. Many of these businesses, regardless of their size, lack internal resources to support data security and compliance requirements without the help of an external third-party specialist. This leads most organizations towards a Managed Security Services option.

Did you know?

277 days

In 2022 it took an average of 207 days to identify a breach and 70 days to contain it

$4.3 million

In 2022 the cost of a data breach averaged 4.35 million USD

Statistics according to the Cost of a Data Breach Report 2022 (Ponemon Institute)

Learn more

ADVANTIO.COM/MSS

MDR for Endpoint

Cloud SIEM

Managed SIEM

MDR

Threat Intelligence

Managed Security Services by Advantio

Advantio's suite of Managed Security Services are fully hosted and managed, ISO 27001 compliant offerings with a range of immediate benefits:

Significant Cost Reductions

Outsourcing your cybersecurity needs to Advantio will generate significant cost savings. You can scale up your security operations without adding headcount or investing in the related costs of a 24/7 in-house team. With Advantio's suite of Managed Security Services, you gain access to best-in-class cyber experts without the CapEx associated costs.

Extended Capability

Our threat detection, mitigation, and containment services are managed 24/7 by an expert team of SOC analysts dedicated to maximizing your cyber resilience and reducing your risk. Building an equivalent Security Operations Center (SOC) with similar expertise in-house requires a substantial budget.

Improved Security Posture

By continuously monitoring and analyzing your network and systems for potential threats, you can improve your overall security posture and reduce the likelihood of a cyberattack or data breach.

Turnkey Tech Stack

Our turnkey solution and next-generation tech stack is continually sharpened and seamlessly deliver the latest in endpoint, network, and cloud services that can be easily customized.

Active Threat Containment

Advantio proactively contains threats in real-time, alleviating organizations from any burdensome coordination, and allowing us to act fast, with confidence.

Enhanced Visibility & Reduced Detection Time

With integrated monitoring to correlate patterns and highlight suspicious activities overall visibility is enhanced and detection time can be reduced.

Compliance

If your organization operates in a regulated industry or handles sensitive data, MSS can help you meet certain security standards and compliance requirements.

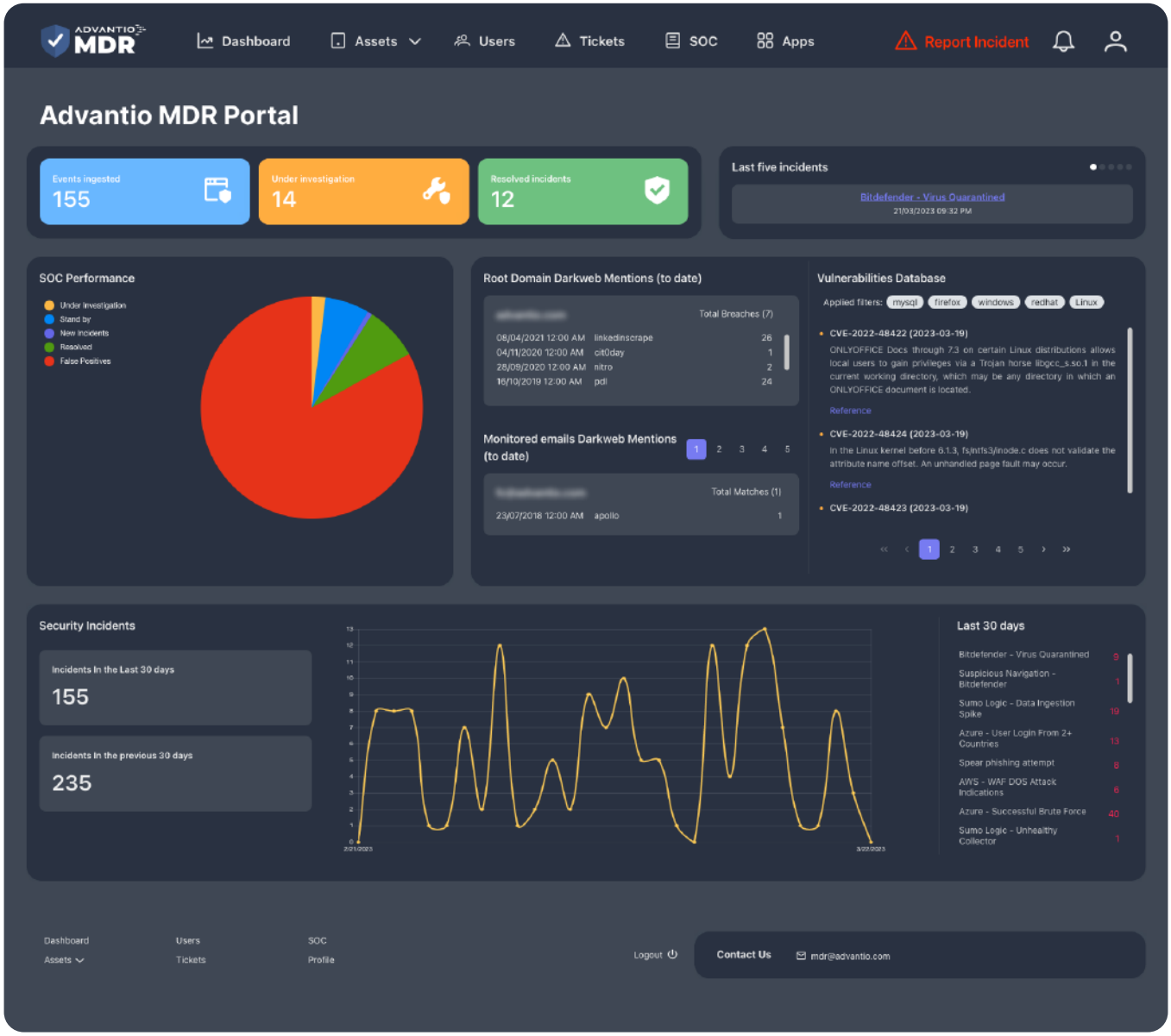
Security Operations Center

A modern enterprise can't rely on preventive defenses alone and for this reason, Security Operations are considered a crucial component of an effective security program. Determining the cause of a compromise is difficult, if not impossible without system activity logs, proper log review, correlation, analysis, and timely response, including Incident Response Plan invocation. Through our ISO 27001-certified Modern Security Operation Center (MSOC), Advantio provides monitoring and Managed Detection and Response (MDR) services including:

- Daily security log reviews
- Detection and Response to identify attacks beyond preventive security controls
- Continuous monitoring to detect the failure of security controls, services, and security components
- 24x7 proactive threat monitoring, analysis, investigation, diagnosis, threat hunting, notification, containment, and remediation support to provide continuous event monitoring and incident management.
- Vulnerability management to prevent attacks
- Threat remediation support on high-priority alerts to identify and understand the issue, and subsequently produce a remediation plan.
- Support of clients' relevant compliance requirements, e.g., PCI DSS, ISO 27001
- Timely restoration of security services and controls in accordance with the agreed SLA
- Real-time dashboard and ticketing updates via our dedicated MSS Customer Portal
- Phone, email, and portal support to back incident management

Enhanced Visibility with an Interactive & Dynamic Customer Portal

As part of our MSS suite, Advantio offers complete visibility and reporting of your security information through our Customer portal which includes realtime dashboards and a snapshot of your service including SOC activity, security logs, threat intelligence, incidents and compliance management.



Real-time dashboards	Incident management
On-demand reporting	Compliance reporting
Ticket creation	Phone support

ADVANTIO
an Integrity360 company
your security in mind

Service Offerings

MDR for Endpoint

Managed endpoint protection and endpoint detection and response (EDR) services support malware protection and remediation backed by 24x7 SOC Team monitoring.

Learn More

Cloud SIEM

Remote management of a cloud-native SIEM solution including the creation of a wide range of SIEM use cases, log parsers and reporting content, detection content writing and tuning, and automatic alerting.

Learn More

Managed SIEM

Also referred to as SIEM-as-a-service includes Level 1 SOC, automatic alerting, manual alerting with co-managed Incident Handling and a first-line triage.

Learn More

Managed Detection & Response

Full threat containment 24/7 from a fully monitored Modern SOC (MSOC) giving you actionable intelligence and protection against sophisticated and persistent attacks.

Learn More

Threat Intelligence

Improves your security capability by identifying threats & leaked data outside of your network. By identifying digital risks sooner, you can act faster to mitigate and avoid cyberattacks.

Learn More

MDR for Endpoint

MDR for Endpoint combines the telemetry that comes from EDR technology with the monitoring of a 24/7 SOC team to provide extensive coverage of your network perimeter.

This proactive service searches for advanced threats on both endpoint and server targets offering best-in-class managed endpoint protection (EPP) and endpoint detection and response (EDR) services for malware protection and remediation.

Organizations benefit from improved detection of known and unknown application reliability issues, alerting security teams in real-time and highlighting the most significant threats to your organization to improve response.

Cloud SIEM

Cloud SIEM provides remote management of a cloud native SIEM solution and includes the creation of a wide range of SIEM use cases, log parsers and reporting content, detection content writing and tuning, and automatic alerting.

The service includes:

- 100 GB (per month) log ingestion
- Up to 30 data sources
- 5 custom dashboards
- 30 custom scheduled searches
- 700 predefined use cases
- 30 custom use cases

Why organizations choose a SIEM

- Enhanced visibility delivers context and speeds up prioritization & response time
- Removes the burden of monitoring individual technology platforms and improves internal security teams productivity
- Focused workflows and automation allow teams to focus on higher-value activities

Managed SIEM

Managed SIEM includes all the features of a Cloud SIEM with the addition of SOC capability for co-managed Incident Handling with first-line triage, giving you greater visibility and actionable intelligence powered by machine learning.

A managed SIEM can help your organization to speed up incident investigation by automatically triaging alerts and correlating threats to maximize security analyst efficiency and focus.

Advantio offers an industry leading SIEM technology to your organization using over 700 use cases to cover your on-premise, cloud, and hybrid environments. Custom use cases can also help you to cover a wide range of unique data sources to ensure that threats are more efficiently discovered and resolved. All alerts are tagged with the related MITRE ATT&CK framework tactics and techniques.

Service features:

- All Cloud SIEM features
- Level 1 SOC services, 24x7 continuous monitoring
- Co-managed Incident Handling with a first-line triage to add a 24/7 service capability and a low-grade investigation of customers' security events
- Unlimited remote support for confirmed incidents
- Dedicated Customer Portal (SIEM data)

Gartner

Advantio Recognized by Gartner® as a Representative Vendor in the 2022 Market Guide for Managed SIEM Services

(Al Price, John Collins, Andrew Davies, Mitchell Schneider, Angel Berrios, August 17, 2022)

Gartner's advice to organizations when selecting the correct partner for a managed SIEM journey is that the decision should "be planned with the goals of the business and the security strategy at the forefront." It recommends that "an organization's SOC should be operating in line with the cybersecurity strategy, which aligns with the organization's business strategy in understanding and addressing cyber risk." (Market Guide for Managed SIEM Services 2022)

Managed Detection & Response

MDR by Advantio detects, responds, and stops threats in minutes from our 24x7 modern Security Operations Centre (SOC), giving you actionable intelligence and protection against sophisticated and persistent attacks. With our complete MDR package, we offer a combination of MDR and IT operation services in the cloud. This combination can be easily customized to individual organizational needs thanks to our breadth of complimentary Professional Services & extensive industry experience.

As a turnkey solution, our MDR has the following features out of the box:

- ✓ 24/7 MSOC Services: real-time event monitoring, intrusion detection, threat hunting, analytics, incident analysis, and incident response
- ✓ Remote incident investigation and remediation including guided containment, eradication & recovery, and guided post-incident activities
- ✓ A dedicated & interactive Customer Portal including dashboards, tickets, incident management, threat intelligence, compliance portal, etc.
- ✓ SIEM-as-a-service for log management and correlation, powered by machine learning
- ✓ Endpoint protection and EDR technology
- ✓ Real-time global Threat Intelligence
- ✓ Vulnerability Scanning

Why choose MDR by Advantio?

- Rapid time to value with quick deployment
- Unlimited multilingual remote support for incidents
- Dedicated & interactive customer portal
- Compliance features are included as standard
- Leverage comprehensive cybersecurity experience across specialist industries

Gartner estimates that by 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers (up from 30% today).

Services Comparision

Advantio offers a multiservice model which provides flexibility so you can select what elements of our services best fit the needs of your unique organization.

What's included?	Cloud SIEM	Managed SIEM	MDR for Endpoint	Most Popular MDR
Full hosted remotely delivered cloud SIEM	✓	✓	N/A	✓
Cloud SIEM tuning and maintenance	✓	✓	N/A	✓
24/7 Level 1 Modern SOC (MSOC) services	N/A	✓	✓	✓
24/7 Level 2/3 MSOC Cyber Analysts Support	N/A	N/A	✓	✓
24/7 Threat Containment	N/A	N/A	✓	✓
24/7 Threat Hunting	N/A	N/A	✓	✓
24/7 Incident Response	N/A	✓	✓	✓
Unlimited remote incident support	N/A	✓	✓	✓
Dedicated Customer Portal	✓	✓	✓	✓
EDR Licenses	N/A	N/A	✓	✓
Vulnerability Scanning Services	N/A	N/A	N/A	✓
Threat Intelligence	N/A	N/A	N/A	✓
Cybersecurity Maturity Assessment	N/A	N/A	N/A	✓
Management for 3rd party security vendors	✓	✓	✓	✓

Additional Managed Security Service:

Threat Intelligence

Learn More

Threat Intelligence

Advantio helps organizations to improve their traditional security capability by safely identifying threats and leaked data that may exist outside the network perimeter. By identifying this digital risk sooner, businesses can act faster to mitigate and avoid cyberattacks.

Our service combines the power of surface, deep, and Dark Web monitoring, data breach detection, and focused threat intelligence with our expert security, intelligence, and SOC services. Advantio enriches the information gathered including knowledge about adversaries (threats actors), their motivations, intentions, and methods (tactics, techniques, and procedures), or TTPs and creates customer data sources, alerts, and periodic threat reports in order to ensure continuous brand protection.

- ✓ TI callout (Reduced risks of common threats)
- ✓ Account Takeover (ATO)
- ✓ Supply Chain Attacks
- ✓ Phishing & Business email compromise
- ✓ Brand impersonation
- ✓ Unauthorized access
- ✓ Attack planning
- ✓ VIP targeting
- ✓ Fraud
- ✓ Intellectual property (IP) leak
- ✓ Typosquatting
- ✓ PII leaks
- ✓ Payment card leaks

Threat Intelligence is also included as part of Advantio full MDR solution

Why clients choose Advantio

Advantio has become the trusted security partner of choice for hundreds of top tier companies and tens of thousands of small businesses globally. Advantio enjoys a 93% average retention rate of its clients who continue to place their trust in Advantio and value the company's expertise. Clients are based globally and typically have a specific focus in the Payment Card Industry but range across industry verticals including Financial & Payment Services, Hospitality & Leisure, Retail, Telecommunications, Government & Defence, Healthcare, Education, Travel, Technology, Infrastructure and Entertainment.