

ASIP MDR-SOC for Microsoft powered by AI

ASIP MDR-SOC for Microsoft 365 protects your cloud environment and users from advanced threats. Our technology platform provides you with fully managed MDR SOC services in a matter of minutes, supported by artificial intelligence and a specialist team of security analysts.

Artificial intelligence and detection-as-code (DaC) technology enable us to identify advanced threats and unknown threats with a greater degree of accuracy. The ASIP MDR-SOC platform incorporates infrastructure-as-code (IaC) technology, cloud native computing and horizontal scaling to meet the most demanding security standards. Services based in the ASIP platform and certified to ISO 27000, ENS and LEET, will help you reduce risk and ensure efficient regulatory compliance.

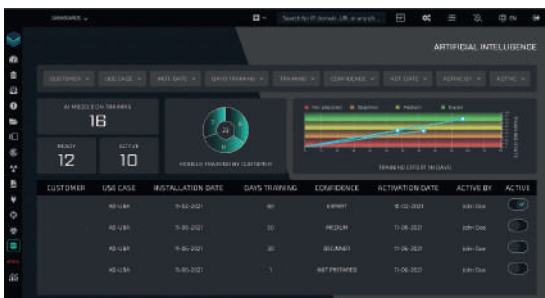
ASIP MDR-SOC

ASIP MDR-SOC revolutionises the concept of a next-generation SOC platform, with enhanced capacity to process security telemetry and more accurate detection. Our technology enables you to:

- Detect unknown threats quickly.
- Reduce mitigation time for your organisation.

Artificial intelligence and machine learning

ASIP MDR-SOC detects new threats and anomalies, by combining predictive artificial intelligence models with automated and assisted learning provided by our specialists. The platform continuously incorporates new models and trains them to adapt to the needs of each environment. See how it is behaving in your organisation, before deciding when to enter production mode and start detecting threats with high accuracy.

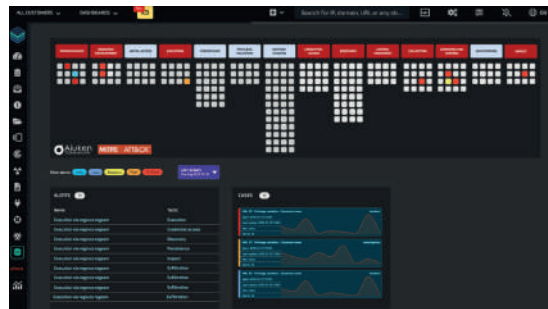


Integrated Threat Intelligence

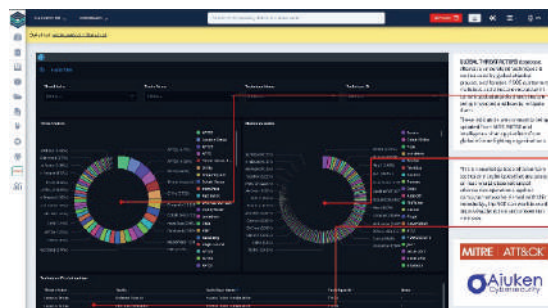
Step up the security telemetry of your Microsoft 365 environment, using data gathered from malicious activity, via our intelligence network with over 40 different sources. Detect malware activity and cyber attacks in real time.

Threat detection using MITRE ATT&CK

Alerts are standardised and prioritised based on each attack's ability to impact your organisation's business. Our incident response team will provide you with the appropriate actions to mitigate each incident.



All events related to Attack Techniques, Global Threats and Actors are researched in order to understand and contextualise their threats.



Global Threat Actions
Malicious codes used
MITRE Techniques relationship

KEY FEATURES



Leading SOC / MDR Platform

This service is provided via ASIP, a SIEM/SOC MSSP and MDR security event correlation platform in the Cloud, located in Europe and distributed across multiple data centres. GARTNER has rated Aiuken's MDR service, based on its ASIP MDR-SOC Cloud platform, as one of the most innovative solutions on the market.



Multi-level security dashboard

Advanced reporting can be adapted to the needs of your organisation. The platform provides real-time reporting through operational, tactical and executive dashboards, for complete service tracking and alignment with the company's business objectives.



Incident and alert management

Receive security incident notifications, based on use cases and intelligence from built-in security frameworks. Risk and alert priority management enabled, along with incident generation and notification.



Deployment and configuration of managed use cases

Our service provides each client with a collection of managed use cases, based on the main market best practices and current regulations, as well as the main threats detected by our intelligence teams.



API Integration

ASIP features native API integration for Cloud platforms such as AWS, Google Cloud and Azure. It can also be integrated with any ticketing platform on the market.



Multi-Cloud Native

Multi-Cloud Native integration capability and support for transparent on-premise environment. ASIP MDR-SOC for Microsoft 365 services adapt to any Cloud, hybrid or On-premise environment, guaranteeing your investment via an integrated SOC platform.

Key advantages

Make SIEM use cases a thing of the past

Our solution provides threat detection capabilities based on MITRE ATT&CK and CAPEC frameworks, as well as NIST controls. The platform provides continuous updates of new use cases and monitoring from our analysts, to deliver a complete standalone SOC tailored to your needs.

Make the most of Microsoft 365 security solutions

ASIP MDR-SOC for Microsoft 365 integrates with Microsoft security solutions to provide one overarching management system, identifying areas for improvement in your setup and consolidating threats. Integrate your Sentinel, Exchange Online Protection, Microsoft Defender and Azure Information Protection services to minimise risk to your users.

Real-time event analysis

Artificial Intelligence technology enables us to process real-time infrastructure security telemetry, to search for threats and detect both known and unknown attacks in real time.

Regulatory Compliance

Ensure alignment with ISO 27000, GDPR, HIPAA SOX and NESA, and simplify the process of complying with key industry regulations. Deploy detection capabilities based on NIST, MITRE and CAPEC automatically.

Highly scalable, next-generation distributed Cloud Native platform

The ASIP MDR-SOC platform implements the latest technological advances, based on infrastructure as code (IaC) for end-to-end, automated management. Our technology guarantees the highest levels of availability and disaster recovery with non-stop upgrades. It also guarantees horizontal scaling to adapt to the needs of our clients at all times.

