mnemonic

SERVICE DESCRIPTION

ARGUS SECURITY OPERATIONS

Managed Security & Support Services

Place	Oslo, Norway
Date	05.10.2021
Version	2.1
Author	KMA/AG/JFM

Summary

mnemonic has 20 years of experience working with different security technologies. We provide 24x7 operations and support for security devices and services for numerous organisations. The Argus Security Operations service is tailored to ensure our customers security solutions and cloud security services are optimized, maintained and kept up-to date by our team of product and operations experts. Argus Security Operation can either be used as a standalone service or an add-on to our Managed Detection and Response service offering.

Argus Security Operations is available 24x7, providing round-the-clock qualified support and managed services via the web, email and phone. The mnemonic Network Operations Center is at all times staffed highly qualified IT security experts who are ready to assist you.

Optimized & Secure operation of security solutions

For a great deal of organisations the complexity and scale of managing security technologies and services is a comprehensive task, especially when taking into account todays limited availability of security expert resources.

With the Argus Security Operations service from mnemonic, you are guaranteed access to one of the strongest teams of product expertise in the market. mnemonic has more than 200 security specialists, and our services are delivered by skilled experts with long experience and up-to-date knowledge and certifications.

The Argus Security Operations service provides you with the expertise and processes to optimize your investment made in security solutions, ensuring proper configuration aligned with the customers' business operation and best practise.

Accurate & Reliable event management

Whether it is an operational incident or a request for change, customers will always receive the attention of mnemonics team of expert operators. Just as with the Argus Managed Defence service, Case management is available through mnemonics Customer Portal.

The Argus Security Operations service includes an SLA that ensures all requests and events are managed in a timely manner, escalated appropriately and professionally handled by mnemonics operators. Customers are always kept informed of the progress, and through mnemonics comprehensive Customer Portal, you will be able to track events and generate reports as desired. Customer can rest assured that mnemonic will handle their tickets in an accurate and reliable way, never closing a case before it is solved.

Combining Argus Security Operations with Argus Managed Defence provides a service package that correlates security and operational events with day-to-day operations, strengthening the overall efficiency and security posture as well as reducing workload for the customer.

Continuous improvements

With a threat landscape that is constantly changing and rapid development in technology you need to stay up-to-date and know how to address these continuous challenges. The Argus

Security Operations service is brought together by a range of deliverables that ensures customers security solutions are up to date at all times. mnemonic will keep track of any available updates, security patches and upgrades, evaluate their relevance for the customer and ensure they are appropriately tested and installed. The customer will also receive advice and recommendation through regular service meetings, where new developments and trends relevant for their security solutions is part of the agenda.

The Argus Security Operations service takes advantage of mnemonic Threat Intelligence service, whereas relevant intelligence is leveraged to improve customer's security solutions and their ability to protect their business.

Partners

mnemonic has partnered up with the leading security vendors globally. We typically achieve the highest partner status with these vendors, which requires significant investments in product certifications and a commitment to support these products.

Through close ties with our technology partners, we can offer our customers a thorough understanding of security products and features.

Argus Security Operations supports products from these top IT-security vendors:

- ✓ Check Point
- ✓ Broadcom
- ✓ Arbor
- ✓ Forcepoint
- ✓ Palo Alto Networks
- ✓ FireEye
- ✓ CyberArk
- ✓ Cisco
- ✓ Trend Micro
- ✓ Proofpoint
- ✓ Algosec
- ✓ Fortinet
- ✓ Splunk
- ✓ Microsoft
- ✓ McAfee

Service components

The Argus Security Operations model comprises several components that can be combined to form a service package adapted to accommodate customers' demands.

This way you can select the options that makes the most sense for your organization, and based on your requirements mnemonic will provide a flexible and cost efficient solutions for managing you IT-security solutions.

Remote Access

To enable management of security devices located at customers' datacentre(s) or in the cloud, a secure channel for remote access is established.

Remote Access can be either be a traditional VPN solution, a cloud based solution such as software-defined perimeter or secured direct access to SaaS solutions.

Whether a private network (VPN) solution or cloud service connection is best suited for your environment, mnemonic will establish a fast, secure and stable direct link to your managed devices, hence eliminating the need for on-site presence.

System Monitoring

System Monitoring is an automated alerting and notification service for health monitoring of managed security devices, supervised 24x7 by our Network Operations Center.

mnemonic can monitor a wide range of parameters depending on system type, enabling us to respond and notify customers of detected operational incidents within minutes.

Supported monitoring parameters include, but are not limited to:

- *CPU load*
- *Memory usage*
- *Disk utilization*
- *Interface status*
- *Throughput*
- *Connections*
- *User count*
- *Queue size*
- *Process status*
- *VPN status*
- *Certificate expiration time*
- *License status*
- *SNMP traps*

mnemonic can monitor most on-premise, hybrid and cloud based solutions, using direct service access, logs and/or API's. Our developers can even create custom monitoring for the services and parameters of your choice.

Operational Incident Handling

Incident handling for operational events is a supplementary service to System Monitoring. In addition to detecting operational events with System Monitoring, the Operational Incident Handling module enables mnemonic to handle operational incidents, with the option to troubleshoot and remediate issues 24/7.

Our event management system immediately informs the operators on duty when an operational incident occurs, and the incident is handled according to your customer specific pre-defined policy.

Change Management

With Change Management mnemonic gives you change handling with class leading implementation times and verification by experienced security and network experts.

Through the Argus Customer Portal customers can easily request policy and configuration changes for their managed security devices.

Change requests are qualified and verified by mnemonic in accordance with Customer policy and industry best practice before they are implemented.

Updates & Patches

mnemonic ensures that minor updates, bug fixes and security patches are installed on-demand to ensure system stability and security.

All patching is performed in agreement with Customer and in accordance with Customers' processes for system updates.

As part of this service mnemonic will notify the Customer of system vulnerabilities or other security related issues known to mnemonic and give recommendations on how such issues should be handled.

Upgrades

For larger upgrade operations, such as lifting your hardware and/or software platform to a more recent version. This usually implies more planning and precautionary measures than installing a small patch or hotfix.

mnemonic uses vendor recommendations combined with our own expertise and experience to determine frequency and time for upgrades.

Backup

Automatic backup of system configuration and/or logs performed periodically and transferred to mnemonic through encrypted channels where it is safely stored at mnemonics' facilities.

Retention time for online backups is 3 months, while offline backups are normally stored for 3 years or as long as desired by the customer.

Support

Support services from mnemonic guarantees you access to some of our most experienced consultants for high quality support.

With our Support service mnemonic offers several levels of support, whereas the level you choose will depend on the supported system's importance to your business, up-time requirements and general business practices.

Central components in your network, such as firewalls, are business critical, and any downtime may severely impact business. Such cases will require immediate action, and mnemonics support services is there to remediate the situation skilfully and effectively.

Reporting

Periodic reports published monthly, quarterly or yearly through the Argus customer portal.

While report content is highly customizable, a report typically includes:

- *Overview of changes*
- *Projects/assignments*
- *Recommendations for improvement*
- *Policy review*
- *Health status / graphing*
- *Overview of incidents*
- *SLA-reporting*

There is also an option for customers to create or request reports on-demand through the Argus customer portal.

License Maintenance

As a reseller of product maintenance and licenses, mnemonic takes the responsibility to keep track of the assets covered under the agreement and their maintenance status.

We notify our customers well in time before maintenance contracts and licenses expire and request renewal or discontinuation of relevant subscriptions.

Sytem Check-up

A System Check-up performed by mnemonics product experts provides an insight to the state of a customer's security solution.

mnemonic will review the systems of your choice, including performance, patch levels, rule base(optional), logs, amongst others.

The customer can choose if mnemonic should implement suggested changes directly, or deliver a report with recommendations after the review.

Other Services

In addition to the core service components of Argus, new services are constantly being developed and added to mnemonics extensive portfolio.

With mnemonics dedicated development team we can tailor solution for our customers, such as:

- *SSL-certificate validity monitoring – Argus Certificate Service (ACS)*
- *Service availability monitoring*
- *Dashboards for reporting or automated policy actions*
- *Argus Email Authentication Service (EAS)*
- *Threat Intelligence Feeds for importing into NGFW/web proxy – Argus Threat Feed (ATF)*
- *Integrations with CRM systems*
- *Local spare parts storage (Norway only)*
- *Secure remote access solutions for third parties – Argus Gatekeeper (AGK)*
- *Emergency firewall shutdown panel for off-shore environments*
- *Policy revisions for firewall, email/web proxy rulebase*
- *And much more!*

1.1 Argus Security Operations packages

Although the Argus Security Operations (ASO) service can be tailored to fit your needs, there are some compositions our customers often choose. Included in all of our ASO offerings is access to the mnemonic Argus customer portal.

1.1.1 ASO Support

If you manage your own IT security solution and you need a trusted partner to provide support and technical assistance, the *Argus Security Operations Support* package is the perfect choice.

The following modules are included in the ASO Support service package:

- *Support*
- *License Management*

1.1.2 ASO Lite

Argus Security Operations Lite comes with a base package that includes the necessary components to enable the core ASO service in your environment. This is the service model for customers who want to manage their own solution on a daily basis, but need 24/7 monitoring and remote assistance for advanced operations or support enquiries. ASO Lite can easily be upgraded to the ASO Advanced or Premium service packages.

The following modules are included in the ASO Lite service package:

- *Remote Access*
- *System Monitoring*
- *Backup*
- *Support*
- *License Management*

1.1.3 ASO Advanced

With the *Argus Security Operations* Advanced service package you give mnemonic complete responsibility for the platform, meaning we make sure you solution is always up-to-date and running optimally.

The following modules are included in the ASO Advanced package:

- *Remote Access*
- *System Monitoring*
- *Operational Incident Handling*
- *Change Management*

- *Updates & Patches*
- *Backup*
- *Support*
- *License Management*

1.1.4 ASO Premium

Similar to the Argus Security Operations Advanced service package, with *Argus Security Operations Premium* you give mnemonic complete responsibility for the platform. In addition, periodic reports, major upgrades and regular system check-ups are included.

The following modules are included in the ASO Complete package:

- *Remote Access*
- *System Monitoring*
- *Operational Incident Handling*
- *Change Management*
- *Updates & Patches*
- *Upgrades*
- *Backup*
- *Support*
- *Reporting*
- *License Management*
- *System Check-up*

1.1.5 ASO service package comparison

Service Component	ASO Support	ASO Lite	ASO Advanced	ASO Premium
Remote Access	✗	✓	✓	✓
System Monitoring	✗	✓	✓	✓
Operational Incident Handling	✗	✗	✓	✓
Change Management	✗	✗	✓	✓
Updates & Patches	✗	✗	✓	✓

Upgrades	✗	✗	✗	✓
Backup	✗	✓	✓	✓
Support	✓	✓	✓	✓
Reporting	✗	✗	✗	✓
License Maintenance	✓	✓	✓	✓
System Check-up	✗	✗	✗	✓

1.2 Support Coverage

No matter which service level you choose, Support and License Maintenance are always included with the ASO services.

mnemonic offers three levels of support coverage to accommodate most support needs for IT-security products:

Level	Case Handling	Remote support	On-site support	Emergency call-out
Basic	Included	Invoiced per hour	Invoiced per hour	Call-out fee
Standard	Included	Included (unlimited)	Invoiced per hour	Call-out fee
Priority	Included	Included (unlimited)	Included (unlimited)	Included

All service levels delivered 24/7 or 8x5 (08:00-16:00) on Norwegian working days.

Standard guaranteed response time can be 1 or 4 hour(s). (Other response times are available upon request)

1.2.1 Basic

The Basic support level is for customers who want guarantee that our product experts will provide support within a given time. With this support level, qualified mnemonic personnel will begin to work on a reported issue within the agreed response time. All work related to the ticket will be invoiced.

This service level is best suited for products with a low degree of change or historically low amount of problems. It is suitable if your organisation has strong knowledge about the specific product(s), but you would like assurance that support assistance is available should a problem arise.

1.2.2 Standard

With this support level the customer will receive unlimited support assistance through the web, email, phone and/or remote access tools. Email channels and the Argus Customer Portal are manned from 08:00-16:00 on Norwegian working days, while phones are manned 24x7. Emergency call-outs for on-site assistance are available and invoiced separately.

Standard Support is the most common service level chosen amongst our customers and is suitable for most types of products and product categories.

1.2.3 Priority

Priority is mnemonic's highest support level. With this level, mnemonic guarantees that a qualified consultant will be on-site within the agreed response time. The consultant will also make use of mnemonic's complete consultant resource pool to resolve the issue as quickly as possible. No additional charges apply.

This service level is best suited for critical systems where downtime can result in significant consequences for business. Customers also benefit from a predictable, all-inclusive cost, regardless of the size of the support case or resources required.

2 Secure Cloud Management

In later years a great deal of companies has embraced the benefits of cloud computing and moved parts or most of their workloads into the cloud. mnemonic and our service offerings are no exception and our customers has put their trust in us assisting them on their journey to the cloud, with everything from risk assessments to deployment of cloud centric security controls and cloud security monitoring.

No need to hire a team of cloud experts to capitalize on your cloud investment, the Argus Security Operations service ensures that your cloud or hybrid solutions are managed securely and professionally.

2.1 Microsoft Azure

Microsofts cloud platform Azure holds a variety of native security features which mnemonic can manage for you.

2.1.1 Service Delivery Model

Mnemonic utilizes Azure Lighthouse to access customers Azure environments in order to deliver managed services for the Azure platform. This is a secure and efficient service delivery model that ensures that the customer remains in control of who has access to their tenant and resources, and what actions mnemonic personnel are allow to perform.

With Lighthouse we create a logical projection of resources from mnemonics tenant to your tenant, enabling authorized operators to perform management operations on behalf of the customer, eliminating the need to sign directly into any of our customers tenants.

Customers can be onboarded by simply choosing the Argus Security Operations in the Azure Marketplace or through Azures delegated resource management feature.

2.1.2 Supported Azure security services and technologies

2.1.2.1 Firewall

The Azure firewall is a firewall as a service with common firewall features like policy enforcement, web filtering, logging, forced tunnelling, high availability (HA) and more.

2.1.2.2 Azure Web Application Firewall

The Azure Web Application Firewall provides centralized protection for common web-based attacks for your web facing workloads. The Azure Web Application Firewall can be deployed in multiple ways such as on an Application Gateway, Azure Front Door service or on the Azure CDN.

2.1.2.3 Application Gateway

Azure Application Gateway is a load balancer featuring policy based routing, web application firewall, SSL/TLS termination, auto scaling and more.

2.1.2.4 Virtual Hub

An Azure virtual hub connects VNets, VPNs, SD WAN together within the Azure infrastructure, making it an essential part of virtually any Azure environment. Acting as the central security feature with all network traffic traversing the hub, having assistance with management is essential to your cloud posture.

Mnemonic can manage your secure hub consisting of either only native Azure services or third party security products.

2.1.2.4.1 DDoS Protection

Microsoft offers advanced and highly scalable DDoS-protection for Azure. For public facing services mnemonic can help with configuration, event management and monitoring of DDoS Protection.

2.1.2.4.2 Microsoft Cloud App Security

MCAS is a Cloud Access Security Broker (CASB) tightly integrated with Azure, Microsoft 365 and third party cloud solution providers. It can help you identify shadow-IT, protect your data and provide granular access control when set up in reverse proxy mode.

2.1.2.4.3 Cloud native infrastructure

Microsoft Azure also provides several integrated infrastructure services like Load Balancers, Network Security Groups, Routing tables etc.

Mnemonic can manage these essential cloud network components for you.

Appendix A: SLA - Response times & Severity Levels

Severity	SSA-V Level	Initial response	Description
CRITICAL (1)	A	30 minutes (phone)	Issue that causes major consequences for traffic and/or business-critical services. Risk of privacy breach and/or data loss.
HIGH (2)	A/B	1 hour (phone)	Significant impact to business-critical services and/or core functionality heavily impacted.
MEDIUM (3)	B	4 hours	Degradation of service that could further impact traffic and/or business-critical services.
LOW (4)	C	24 hours	Typically request for information, a minor inconvenience or issue that is not related to an immediate need.

Appendix B: Onboarding

The Argus Security Operations service is implemented using mnemonic's project management framework, which is based on core principles from PMI and Prince2, and has been customised over the years based on our experience in successfully implementing our services. The framework ensures that our implementation projects meet the agreed expectations, are of a high quality and delivered on time.

The service implementation project encompasses technical components, such as installation and device configuration, along with information gathering activities focused on customer business operations, service deliverables and escalation procedures.

The implementation service is a mandatory component of the Argus Security Operations initialization. The implementation project has various components that may be delivered on-site, while other deliverables can be performed remotely.

An example of project tasks and deliverables includes:

- Arrange start up meeting for the service with relevant Customer personnel and mnemonic personnel, as an introduction to the service
- Service design: high and low-level designs
- Planning technical and procedural integration of service, including establish customer- and solution-specific management routines and documentation for the operations center
- Classification and documentation of assets and services
- Establish secure communication lines between the mnemonic operations center and the solution
- Establish Customer users at mnemonic customer portal
- Establish administrative users for mnemonic in the solution
- Physical installation of hardware (if applicable)
- Data collection to observe traffic patterns and establish normal traffic baselines
- Configuration, testing and tuning
- Configure scheduled backup
- Establish service handbook with key information about the solution, service, contact information and escalation paths etc.
- Review of policies, procedures, escalation path and service handbook

The time required for implementation will vary, dependent on factors such as the required network changes, existing documentation available regarding the customer's services and network, and the availability of physical access to facilities.