mnemonic

SERVICE DESCRIPTION

ARGUS MANAGED DEFENCE

Managed Detection and Response service

Place	Oslo, Norway
Date	13.10.2019
Version	4.0
Author	AF/KMA

Table of Contents

1 Argus Managed Defence – Service Description

1.1 Executive summary

Argus Managed Defence provides 24x7 managed protection against cyberattacks and security threats targeting your business. With complete enterprise coverage, including cloud, data centre, network and endpoint, our expert team of security analysts, incident responders and threat researchers will act as an extension of your security team to help you defend against today's complex, targeted cyberattacks and keep your business safe.

The service provides advanced correlation across six key areas – **networks, e-mail, log data, endpoints, vulnerability & asset data and cloud services** – to gain complete visibility and detect cyber threats that may have otherwise gone unnoticed. When a threat is detected, our security analysts will give you the actionable information and recommended actions you need to immediately respond to the threat. By filtering out the noise, Argus Managed Defence allows your security team to concentrate on responding to confirmed threats and stop wasting time chasing false positives.

Powered by our Argus security platform, driven by our Threat Intelligence and acknowledged by Gartner as one of the top managed security services in the world, Argus Managed Defence allows our customers to strengthen security, reduce operational costs and focus on their daily business.

Highlighted elements within the service include:

- **24x7 security monitoring, event analysis and incident alerting,** powered by:
  - Argus Network Analyser monitors network traffic for threats
  - Logs from internal systems (including firewalls, proxies, Active Directory, servers, etc.) are collected and analysed for suspicious behaviour and indicators of compromise
  - Anything and everything mnemonic monitors is correlated against our constantly updated Threat Intelligence ecosystem
  - Any and all incidents are analysed by an experienced Security Analyst – you are only notified once a security incident is verified by an analyst
- **24x7 global threat intelligence,** monitoring threats and attack vectors and providing advisories as new vulnerabilities or attack campaigns occur
- **Dedicated Technical Account Manager** that knows you, both technically and your business priorities, along with the threat landscape and incidents you're facing
- **Regular service meetings** for incident review, service improvement and recommendations
- **Reporting** of your security status, including management-level information to quickly assess the situation, in-depth analysis of events and incidents, as well as recommended initiatives for improving the security posture

1.2 Service Details

Argus Managed Defence is a flexible, customizable and extensible service that is designed to grow with our customers. This means that the service can be expanded with additional services in the future.

Example of additional services available to be integrated to the service

- ✓ Endpoint incident response tools and services
- ✓ Incident handling and/or incident response
- ✓ Advanced malware detection
- ✓ Managed firewall, web proxy, email proxy, web application firewall, +more
- ✓ DDoS mitigation
- ✓ Continuous vulnerability scanning & management
- ✓ Security testing, risk assessments, product support and other consulting services
- ✓ Managed PCI DSS testing & scanning

…and more

All of mnemonic's managed security service offerings are customized in some manner to provide the best security coverage for our customers. We have however been able to divide our most common service implementations into four phases that frame common deployments, and a vision to future capabilities. This phased approach is based on our experience delivering managed security services over the past 17+ years, current services delivered to our customers, and our knowledge of the threat landscape.

Phase 1	**24x7 security monitoring** -Argus Network Analyser monitoring user traffic -Basic log analysis (Active Directory, firewall & web proxy) -Establish incident response procedures
Phase 2	**Advanced log analysis** (application servers, other network & security appliances) **Expanded coverage for network monitoring** (remote sites, services/servers, encrypted netbank traffic, etc.) **Continuous Vulnerability Scanning**
Phase 3	**Threat specific technologies & expanded services** -Advanced client detection & incident response tools -Advanced malware detection -DDoS mitigation services
Phase 4	**Expanded services** -Threat Intelligence services -Integrated security testing

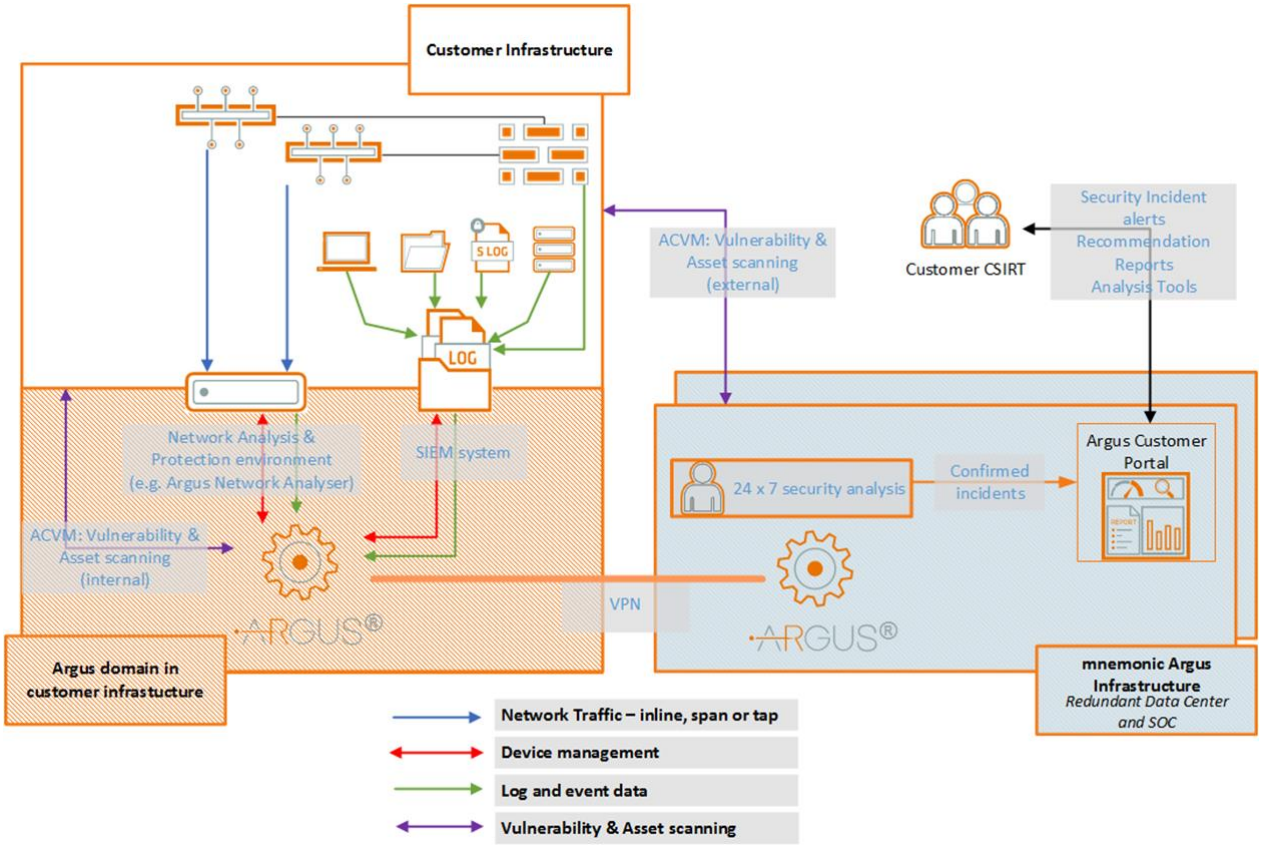
Argus Managed Defence is often implemented in a phased approach to systematically raise the security level at our customers.

This service will immediately raise your security awareness, the ability to detect, prevent and respond to modern cyberthreats, and reduce the strain on internal security resources currently responsible for detecting security threats. The service continues to develop over time and will protect your business for years to come.

1.2.1 High level architecture overview

Below is a high-level conceptual design of a single site service implementation.

Argus Managed Defence high-level architecture concept



1.2.2 The Argus Platform

At the core of our offered solution is our proprietary MDR platform known as Argus - our purpose-built ecosystem exclusively designed to rapidly detect, analyse and respond to security threats on a colossal scale. Taking advantage of **big data analytics, machine learning**, and a **complex event processing framework**, Argus provides the advanced threat prevention ecosystem needed to see the big threat picture in real-time and protect our customers against **advanced persistent threats, zero days** and **targeted attacks**.

Under development for over a decade, Argus is a scalable, flexible platform that is continually adapted to keep pace with the evolving threat landscape. Argus is now a mature threat management ecosystem that integrates threat intelligence through the entire platform and integrates into diverse, multi-vendor IT environments.

Argus has been designed to tightly incorporate with our customer's processes, frameworks and workflows, and will serve as an integral component in the detection and response workflows mnemonic will establish together with the customer CSIRT.

Argus incorporates a combination of proprietary technologies developed by mnemonic, internal and external threat intelligence and integrations with leading 3rd party security solutions from our product portfolio.

Argus utilizes the Esper Complex Event Processing framework. Often used in algorithmic stock trading, Esper is designed specifically to simultaneously process large volumes of event data at high-velocities from numerous sources, combining historical and real-time data on the fly. For Argus, this translates to a big data processing engine that is scalable, capable of tracking and correlating data from many sources over long periods of time and tuned to detect unwanted, anomalous and malicious activity.

1.2.3 Argus Network Analyser

The Argus Network Analyser is a mnemonic appliance custom built specifically for detecting security incidents. The sensor will inspect traffic in real-time to identify patterns that may indicate undesirable or malicious activity.

The sensor also contains an extensive range of functionality to identify threats targeting our customers and provides mnemonic Security Analysts with the necessary information to make an accurate and quick assessment of a potential threat.

Argus Network Analyser feature	**Key benefit**
Intrusion Detection System (IDS)	✓ Inspects traffic in real-time to identify patterns that may indicate undesirable or malicious activity ✓ Provides up-to-date protection against modern threats through our constantly updated *custom* signature set powered by *mnemonic Threat Intelligence*
Advanced malware detection	✓ Provides advanced malware detection by analysing files seen on the network in the Argus Intelligence Cloud
Web reputation correlation	✓ All traffic is correlated against our IP and domain reputation database. Built from our sensor network and over 200 intelligence partners, if your users are communicating with a suspicious website, we'll know it.
Botnet pattern recognition	✓ Attackers often follow a recipe when communicating with infected clients – their botnet. Using custom identifiers discovered by our Malware Research Team, we spot the infected clients and get the attackers out of your network.
Incident packet capture	✓ When an alarm is triggered, the network traffic surrounding the incident is captured and made available for later analysis. Having as much evidence as possible increases our ability to assess the threat, understand how it happened and to prevent it in the future.

1.2.4 Argus Log Analyser

Logs from selected servers and network components will be collected, analysed and correlated against network activity detected by the Argus Network Analyser. In addition, logs and other events will be analysed for signs of malicious behaviour, anomalous activity, misconfigurations and hardware/software failures.

The Argus platform can accept logs from various standardized log platforms and formats, such as syslog and Windows Event Collector, without the requirement for a 3rd party log management solution, such as Splunk.

Different log sources offer varying value for diverse use cases and scenarios. Some logs are used in the **detection of security threats**, others are used to **add context** to a detected event and some are used to **investigate a potential threat**. Depending on the scenario, the role of a particular log source may change as well. We support a very wide range of log sources, and virtually any log source that can be produced in a readable format can be integrated.

mnemonic will also use data collected from various log sources, such as Active Directory, to contextualize and enhance our incident notifications. With this enhancement, security incident alerts will not only contain the IP address of the clients involved in a security incident, but also the **username** and **machine name** at the time an incident occurred. This saves time when responding to the incident by not having to search through DHCP or Active Directory logs to identify which user and device the IP address belonged to at the time of the incident.

In addition, if the Active Directory catalogue is exported to Argus, our incident alerts can also contain extended user details, such as department, phone number, location and more.

mnemonic has **thousands** of signatures to identify unwanted activity through various log types. Unwanted activity will vary depending on the log source. Below is an example of the type of activity we monitor for using different types of log sources.

Log source	Signature use case examples
Active Directory	✓ Brute force logon attempt ✓ New user in admin group(s) ✓ Admin logon to specific servers ✓ Correlate active logged on users with Security Events
Firewalls	✓ Compared against our reputation database
Web and email proxy	✓ URL, IP and Domain reputation ✓ Pattern matching for known exploit kits and botnet communication
DHCP	✓ Identify hijacking of IP-addresses ✓ Identify rogue devices ✓ Correlate machine names with Security Events

DNS	✓ Domain and IP reputation ✓ DNS tunneling ✓ DGA (Domain Generation Algorithms) domain names used by malicious attackers
Database	✓ Brute-force attempts ✓ Privilege escalation attempts ✓ Attempts to connect to “default” databases
Web servers	✓ Brute force attempts ✓ Reconnaissance attempts ✓ IP reputation ✓ Correlate user activity with security events from other sources

1.2.5 Argus Endpoint Responder

The Argus Endpoint Responder extends the Argus Managed Defence service directly to the endpoint, anywhere in the world. Endpoints will be actively monitored for signs of compromise and the enterprise can be sweeped to actively hunt for threats. Compromised endpoints can be quarantined and are ready for forensic investigation by the mnemonic Incident Response Team.

Argus Endpoint Responder includes one or more managed agent-based endpoint detection and response (EDR) tools. Dependent on the selected tool, the agent facilitates host isolation and custom detection, and support for remote forensics. The EDR tools are both used for detecting security incidents, investigating alerts from other parts of the Argus service and to perform incident investigations and incident handling.

Some of the key highlights of the platform include:

- **Rapid interrogation of all endpoints**
  Investigate tens or hundreds of thousands of endpoints in a matter of minutes.
- **Agent Anywhere**
  Investigate any endpoint even when they are not on your network.
- **Easy to understand interface**
  Transform front-line analysts into investigators by making it simple and straightforward to quickly interpret data and follow up appropriately.
- **Containment**
  Contain endpoints and immediately deny attackers further access through those endpoints.

The Argus Endpoint Responder service offering can be divided into three main parts:

- Operation and maintenance
- 24/7 analysis, monitoring, and correlation
- Threat hunting, investigations and content development

Operations and maintenance

The Argus Endpoint Responder service consist of two main components; a central management system and agents deployed at the endpoint. As part of the service offering, mnemonic will set up, operate and maintain the central management components of the EDR technology in use. This include Device Management of the central management components, such as license management, health monitoring, device configuration backup, management of the application, platform and hardware and patching.

The endpoint component – agent – is the responsibility of the customer's operations resources (or any third party engaged by customer) to deploy, update, and otherwise maintain. mnemonic will provide the installation packages of the agent and notify of any new versions and assist the customer with other relevant information to operate the endpoint component.

24/7 analysis, monitoring and correlation

Monitoring, analysis, correlation of the events and alerts originating from the EDR technology will be conducted by mnemonic's Security Operation Centre (SOC). This will include:

- Incident handling by executing analysis of event from the EDR product based on IOCs
    - This will include first line of analysis and triage of the event and determine if the event need further analysis by Tier 2 or Tier 3 SOC analysts
- Correlate and analyse event from other security solutions (if available) to verify possible breach on the endpoint
- Containment of clients in the event of attack
    - Require the incident being escalated to and analysed by Tier 2 and/or Tier 3 SOC analyst and the actions being executed in line with customers incident response policies and routines

The alerts will be integrated into the Argus platform and presented in the same view in the Argus Customer Portal as all other alerts reported to the customer.

In the event of a high severity security incident requiring more in-depth analysis, the investigation will be escalated to a senior and more specialized analysts. This capability will be used in the service for verification purposes where necessary. More thorough forensics investigations are available as time and material or deducted from a Service Retainer.

Threat hunting, investigations, and content development

Threat hunting, investigations, and content development is performed by specialized security personnel and can be initiated by an externally alerted incident (e.g. from authorities), ad-hoc

requests from the customer, external threat intelligence reports or as part of mnemonic internal malware and threat intelligence research and incident handled by mnemonic. Indicator sweeping is performed on the basis of indicators we collect and receive from partners and collaborating organizations.

Threat Hunting is hypothesis and scenario-driven hunting for threat actor activity or presence, but without preliminary knowledge about relevant atomic indicators and artefacts. In scenario and hypotheses driven hunting, we hunt based on preliminary knowledge about tactics, techniques, and procedures, or based on theories about expected or possible tactics, techniques and procedures.

Both indicator sweeping and threat hunting are prototyped in runbooks. Reliable detection is then migrated to continuous detection. Runbooks prone to producing false positives, but which still deliver value, will remain runbooks, while less valuable runbooks are deprecated.

Runbooks are developed by mnemonic, with or without input from the customer organization. Depended on customer's ambition- and maturity level, we can assist in develop customers own hunting capabilities, and/or develop scenarios in collaboration with mnemonic, and possibly other third parties.

Threat hunting, investigations, and content development is a standard component of the Argus Endpoint Responder service. These activities are not part of the standard fixed monthly service cost and is delivered either as time and material or deducted from a Service Retainer.

1.2.6 Argus E-mail Security

This service will add more functionality and configurability for detecting and preventing threats sent via e-mail. It will provide additional sandboxing and analysis options of content received and sent by e-mail. The service is delivered as a SaaS using FireEye Email Threat Prevention technology and service.

The FireEye Email Threat Prevention service module will add advanced analysis of email, including sandboxing of attachments to detect malicious emails. The FireEye solution will use their proprietary Multi-Vector Virtual Execution (MVX) engine to analyse e-mail attachments and links with emails. E-mail headers, network traffic from executed binaries and URLs are also matched against FireEye's indicator sets to detect and block threats. FireEye also supports downloading and analysing links to attachments in e-mails, and blocking of malicious content.

FireEye is known to have the most precise prevention mechanisms for malicious code, and is often seen to detect targeted malware used only one time.

1.2.7 Argus Continuous Vulnerability Monitoring

Vulnerabilities are a natural by-product of software development. Software is only as secure as its weakest link, and with the constant wildcard that is the human element, combined with increasing complexity and rapid development, software will inherently have vulnerabilities.

It is these vulnerabilities however that attackers exploit when attempting to compromise your network. When business environments are measuring their hosts in the thousands, tens of thousands or even hundreds of thousands, maintaining control and visibility into the vulnerabilities on these systems is a daunting task that requires continuous, structured attention.

mnemonic addresses this challenge through a combination of technology, processes and experience performing security assessments, penetration testing and web application assessments. This service is packaged together as Argus Continuous Vulnerability Monitoring.

Argus Continuous Vulnerability Monitoring will allow the customer to maintain a constantly updated, holistic view into the vulnerability status of assets across the entire environment. The customer will also receive continuous visibility into assets across the network, discovering new assets that come online and identifying those that have gone missing.

Argus Continuous Vulnerability Monitoring is a fully managed service that establishes a framework for vulnerability management. Systems, services and applications are continuously monitored to establish and maintain an up-to-date status of vulnerabilities in an environment.

Argus Continuous Vulnerability Monitoring also enhances and adds additional context to the entire Argus Managed Defence service delivery. The result is an integrated service that will be more accurate and precise in identifying legitimate security incidents, and enhance the alerts customers receives with additional context to further assist customer's response efforts and ultimately reduce the time from detection to remediation.

Argus Continuous Vulnerability Monitoring (ACVM) provides:

- **Constantly updated, holistic view into the vulnerability status of assets across the environment**
    - Through frequent vulnerability scanning integrated with vulnerability feeds, asset and patch management products, and management reporting systems, ACVM retrieves information about which systems, misconfigurations and vulnerabilities exist on a continuous basis. The service provides comprehensive and up-to-date intelligence of your assets and vulnerabilities in the IT environment. Furthermore, ACVM monitors and reports on configuration and security hardening, as well as the validity and security of TLS/SSL certificates.
- **Portal for asset and risk management**
    - Asset and vulnerability information is uploaded to Argus; a feature-rich security and intelligence platform. Accessed through a secure web-GUI, asset and vulnerability data is structured and made available to intuitively support vulnerability management workflows. Dashboards and reporting provide insight into an organisation's vulnerability status, and data can be freely exported to other tools through the REST API and common file formats. mnemonic calculates a common ground for risk based on the CVSS's assigned CVSS value.
- **Detection and response to new vulnerabilities and misconfigurations**
    - Receive automatic notifications for all high or critical severity vulnerabilities that are discovered, and create custom notifications, such as for the detection of vulnerabilities with a specified criticality on identified systems or business processes, or if new assets are discovered. Alarms and alerts can be further defined, and the organisation has a tool to structure their vulnerability management activities, as well as create statistics and reports for benchmarking and follow-up. With the time saved, resources can concentrate on ensuring critical patches are applied in a timely manner and ultimately improving the overall security posture.
- **Assets correlated with business services and processes**
    - Assets can be further associated with the services and business processes they support. This allows vulnerabilities to be prioritised based on the business processes the affected assets support. When combined with Argus MDR, security

incidents can also be assessed in the context of the business, with the incident severity level influenced by the affected business processes. Thus, identification of legitimate security incidents and alerts are enhanced and appropriately prioritised based on how it may affect the business.

- **Integrating ACVM with Argus MDR**
  - ACVM can provide valuable context to the core Argus MDR service delivery. By knowing the vulnerability status and configuration of the assets within the network, we are able to provide additional context of incidents and allow for more effective prioritization and escalation of incidents. Furthermore, reporting becomes more flexible, as information can be sorted and grouped. Additionally, the service can customize alerts by adjusting who receives an alert depending on the assets, services and business functions affected by the incident.

Compliance control with ACVM

The consequence of a serious security incident can impact the entire business, and continues to become more strictly regulated with data privacy laws, such as GDPR, and cybersecurity laws, such as the NIS Directive.

- CIS Controls: The service corresponds to best practices for discovery and vulnerability scanning as defined in CIS Controls (CIS Basic Controls 1-5 (ref: https://www.cisecurity.org/controls))
- NIS Directive: ACVM achieves several obligations related to the NIS Directive, such as managing security risks by identifying, documenting and actively managing assets, enabling log data by flagging alerts that relate to essential services, and providing knowledge to monitoring staff in the identification, prioritisation and investigation of related assets.
- Compliance reporting: ACVM provides simplified compliance reporting for COBIT, GLBA, HIPAA, HITRUST, ISO-27002, ITIL, MASS 201, NERC-FERC, NIST, PCI, SOX, and many more government and industry mandates with pre-built templates.

1.3 Service inclusions

This section describes a selected subset of the Argus Managed Defence service inclusions.

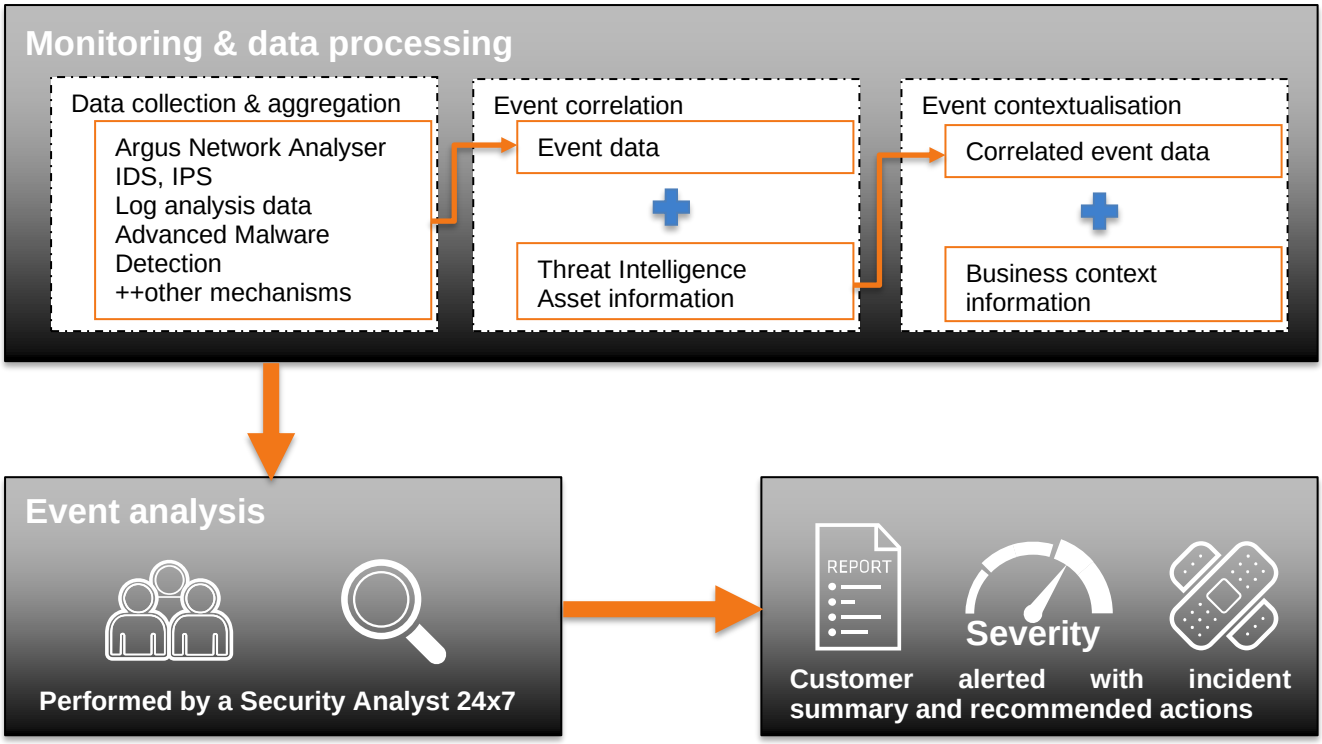
Argus Managed Defence inclusions	
✓ 24x7 security monitoring ✓ Argus Customer Portal ✓ Access to the mnemonic Incident Response Team ✓ Customised, contextual service delivery	✓ Threat intelligence ✓ Manual, automated and customized reporting ✓ Service meetings ✓ Full service infrastructure management

1.3.1 24x7 Security Monitoring & Alerting

Advanced Threat Defence requires a combination of the right technology, people and processes. Staffed with more than 110 highly skilled security analysts, and supported by an additional 90 subject matter experts, the mnemonic SOC will act as an extension of customer's operations and part of the team. With specialists in network analysis, SIEM, log analysis, digital forensics, malware reverse engineering, incident response, and many more disciplines, the customer will be backed by a team with expertise across the entire information security spectrum.

The service customers will receive is one that, through 18 years' of continual improvements, has been fine-tuned to support workflows that reflect how security incidents are evaluated as part of an Incident & Continuous Response Framework. Supported by our Argus platform, customers will receive a custom service that will tightly integrate with customer's response functions – before, during and after the incident.

Incident monitoring, data processing and event evaluation is a complex process that is driven by mnemonic's Argus Processing Engine. The conceptual process is described below:



The details surrounding the alert are analyzed in context with the involved asset(s), affected services and overall business impact. This investigation is performed by a qualified and experienced Security Analyst to help eliminate false positives and ensure that the customer is only notified of legitimate security events.

Should undesirable or suspicious traffic be detected, an alert is automatically sent to mnemonic's SOC for investigation by a Security Analyst. If the Security Analyst validates the alert as a legitimate security incident, only then will the customer be notified via email, SMS or phone, based upon the agreed escalation and prioritization procedures.

Alert options	1st line analysis	Response time
✓email ✓SMS ✓phone	Performed by a trained Security Analyst - always	< 1-hour, 24x7

The customer will not only be notified of an incident, but will also receive **actionable intelligence** to respond to the security event. mnemonic Security Analysts will create an incident ticket for each validated security event in the Argus Customer Portal.

Argus Managed Defence incident tickets

Every Argus Managed Defence incident ticket includes:

- ✓ Short, easy to understand summary with background details on the incident
- ✓ User(s), assets and/or service(s) involved or affected by the incident
- ✓ Case severity assessment based on agreed incident severity ranking
- ✓ Technical details used to analyse the threat (e.g. packet capture extracts)
- ✓ Consequence of the incident as it relates to the customer's business context
- ✓ Recommended actions on how to respond to the incident

See the Argus Customer Portal section for an example screenshot of an incident alert.

1.3.2 Argus Customer Portal

Customers will also receive access to the Argus Customer Portal. The web-based customer portal is a component of Argus to meet the demands of our customers for analysis, reporting and case management.

Argus is designed to fully support incident handling workflows, from notification through analysis and resolving the incident. Our analysts share the same case management view as our customers, and use Argus as their primary incident tracking, analysis, communication and workflow tool.

Argus Customer Portal highlights

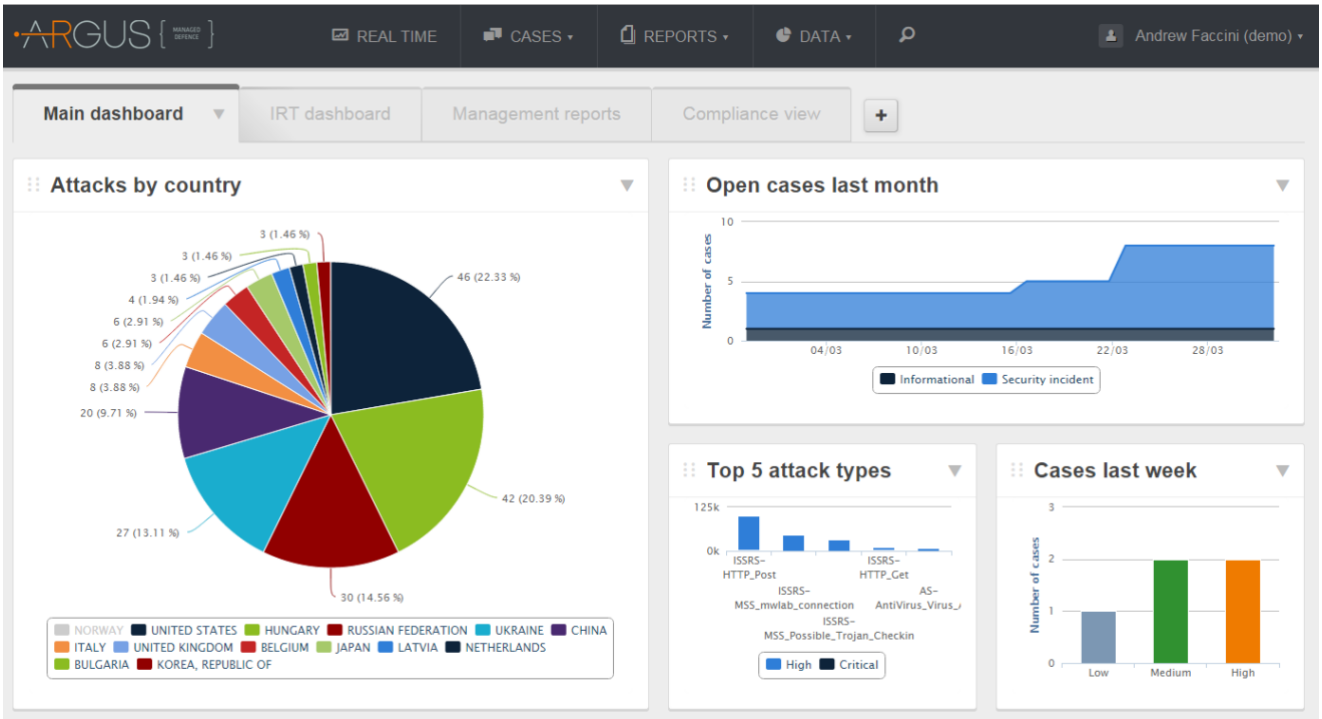
- ✓ Single point of contact for all mnemonic services
- ✓ Case management system
- ✓ Comprehensive reporting – manual, automated and customized reports
- ✓ Notification via SMS, email and telephone
- ✓ Detailed incident reports
- ✓ Powerful analysis tools for incident analysis, investigation and response
- ✓ Two-factor authentication
- ✓ Secure communication and exchange of data and documentation
- ✓ Interactive widgets provide high-level overviews

Incident Management and Workflow

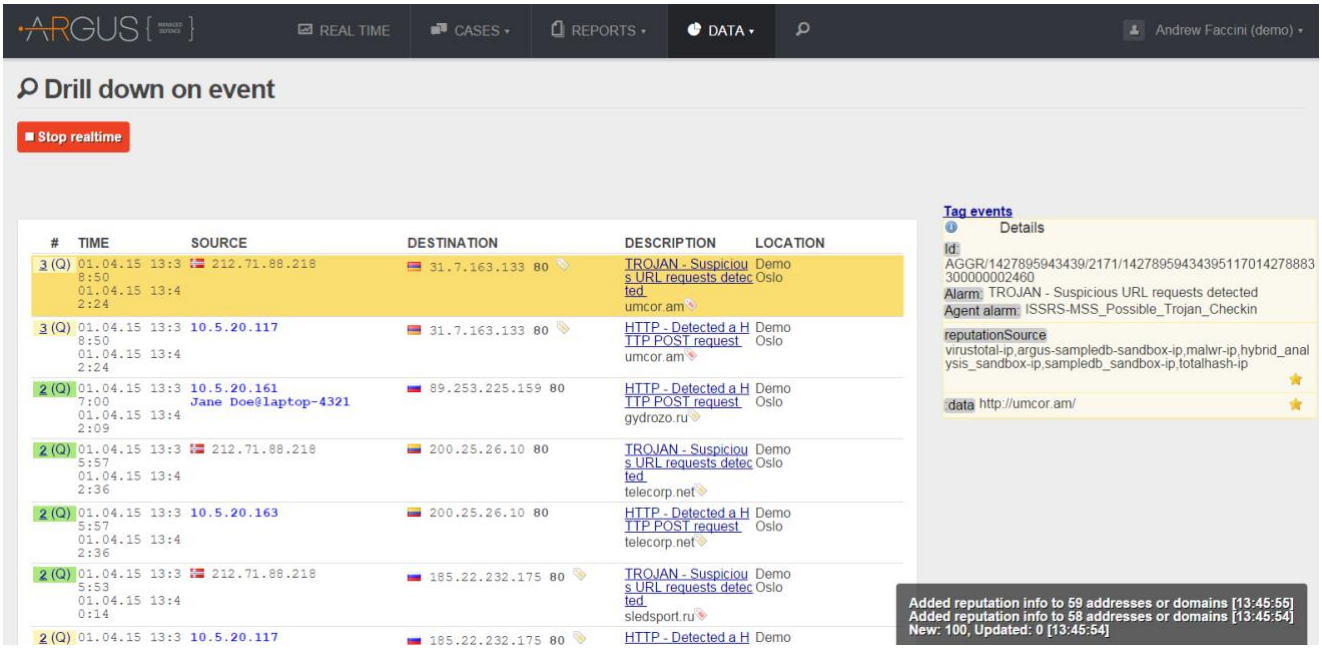
One of the main functionalities within the Argus portal is the case management system, developed with the aim to support our MDR services and support customer workflows. The functionality far exceeds a basic ticketing system's functionality.

Functionality in the case management module includes:

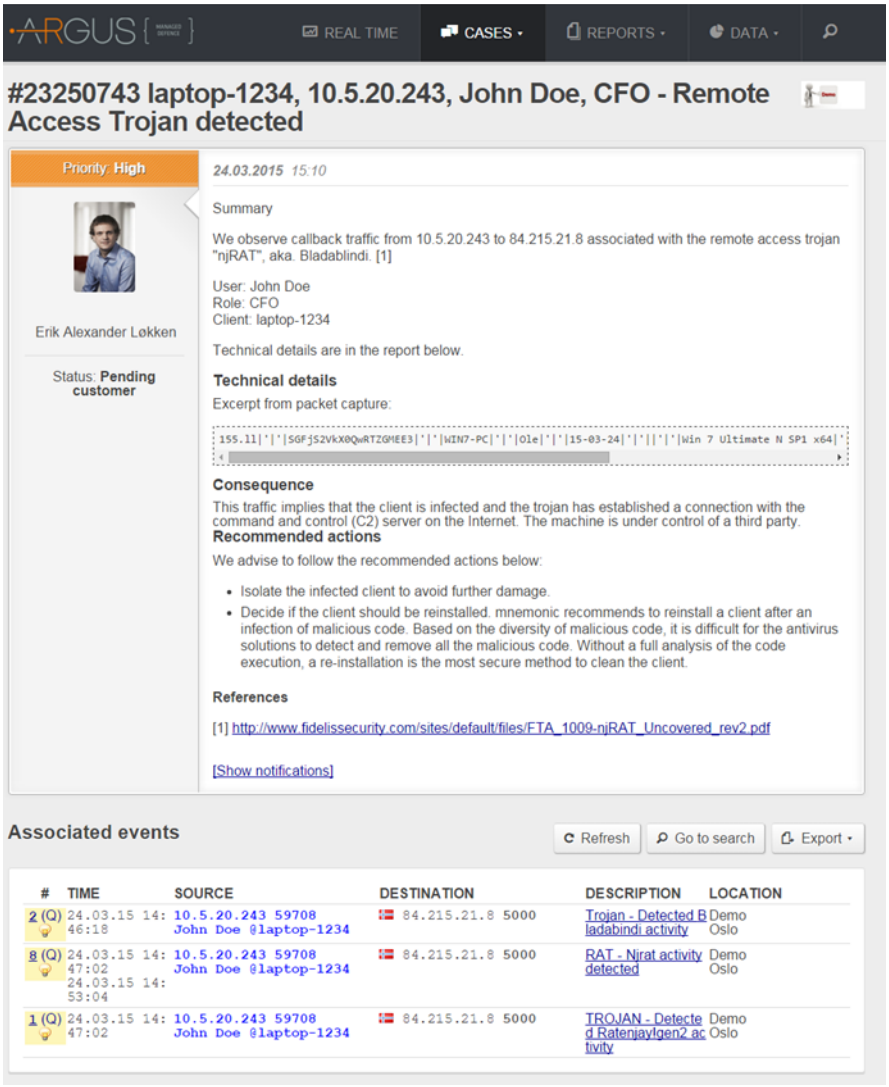
- Thread based ticketing
- Status (closed, pending customer, in progress customer, pending mnemonic, in progress mnemonic)
- Default access for all defined service personnel, but possible to limit access for specific users from case to case
- Severity (low, medium, high, critical) and support for escalation
- Custom notifications using email and SMS based on incident type and severity
- Functionality to add attachments and links to similar cases
- Add tags to incidents
- Search old incidents based on subject and body



Argus Customer Portal – main dashboard with customizable widgets to provide a visual overview of the service and organizational security



Argus Customer Portal – customer real-time view of events as they are detected. mnemonic Security Analysts use the same view to triage and initially assess security incidents as they are detected by Argus.



Argus Customer Portal – example of a security incident notification, including a summary of the incident, involved user(s), technical details, consequence and recommended actions. The priority is based on our recommendations and as agreed with each customer. All technical information surrounding the incident (e.g. packet captures) is appended to the case and available for customers.

1.3.3 mnemonic Incident Response Team (IRT)

Argus Managed Defence customers receive access to mnemonic's Incident Response Team. This team consists of 17 core incident handlers who specialize in responding to any and all types of security incidents - including the regions' most serious and targeted attacks.

Incident handling is a specialist skill. It requires knowledge of attacks and attackers, how to contain and recover, familiarity with recovery plans and processes, and extensive practice. Whether it is a DDoS attack, efraud, worm outbreak, ransomware, an insider threat, or any other type of security threat, the mnemonic Incident Response Team has the tools, experience and skillset to assist organisations in responding to the incident.

Our security analysts experience attacks every day. They live in this world, and when incidents happen, it is not something out of the ordinary – they are expected. They can be trusted to know how to handle the incident to minimize the consequence to your business.

mnemonic IRT has been a member of FIRST (Forum of Incident Response and Security Teams) since 2010 and is listed as an incident response team by Trusted Introducer.

Common security incidents mnemonic IRT responds to include:

- ✓ Distributed Denial of Service (DDoS) attacks
- ✓ Malware infections
- ✓ Advanced Persistent Threats
- ✓ Persistent and targeted attacks
- ✓ Worm outbreaks
- ✓ Insider threats
- ✓ Electronic fraud
- ✓ Forensic investigations

…more

1.3.4 Customised, contextual service delivery

A key component, differentiator and distinct value proposition for an Argus Managed Defence service is that our *service delivery will be mapped to our customer's business processes*.

Beginning with the implementation project, this process includes:

- Mapping of monitored assets to the service(s) they support (e.g. SQL server supports customer support system & service)
- Business impact of service interruption
- Establish incident severity ranking (based on our recommended template)
- Setting standard alerting procedures based on incident severity and involved assets/networks/services
- Escalation procedures

The end result is a set of contextual escalation and prioritization procedures that allow mnemonic's Security Analysts to become integrated members of the customer's security strategy. Should a security incident be detected, our Security Analysts will have valuable knowledge of the customer's business and technical environment and will follow a documented and predetermined escalation path to ensure incidents are prioritized and handled appropriately and effectively.

1.3.5 Threat Intelligence

Technology alone is not enough to secure assets against today's threat agents and modern attack methods. Security vigilance requires constantly updated, relevant and localized threat intelligence that is both accessible and actionable. This is why our Argus Managed Defence service is supplemented by the mnemonic Threat Intelligence group – a team of experts solely dedicated to researching modern threats and turning collected security information into actionable intelligence.

We are among the leaders in producing all subtypes of threat intelligence within Europe and globally, and are relied upon by law enforcement agencies (including Europol EC3), CERTs and enterprises as a source for regional intelligence.

The data and information obtained from our own sensor network is one of our key differentiators. While our sensor network has global coverage, we have an unprecedented view of threats facing Europe. Customers with operations based in Europe, will be facing threats from regional websites that serve malicious code in the form of drive-by downloads or waterhole-style attacks.

Over 80% of all events detected and reported to our customers are enhanced by mnemonic Threat Intelligence

By collating and analysing the information collected from various security sources - including mnemonic's Global Sensor Network - attack patterns and threat signatures are discovered and translated into protection filters that will immediately combat threats against the customer.

Sources of information used by mnemonic Threat Intelligence include:

- mnemonic's Global Sensor Network
- security forums (open and closed industry forums)
- security organisations (e.g. SANS, NSM, NorCERT, etc.)
- reputation services (commercial and open-source)
- malware analysis (performed in-house in mnemonic's dedicated malware lab)
- trojan monitoring

By correlating and analysing these sources, mnemonic has a unique insight into the threat landscape, both nationally and globally. This information and knowledge is unique to mnemonic and is applied to all Argus Managed Defence customers.

Another important source of information is intelligence derived from incident response work, where the mnemonic Incident Response Team is responsible for responding to some of the region's most serious security breaches and targeted attacks from nation-states. This real world, in the trenches experience, along with IOCs (Indicators of Compromise) and TTPs (Tactics, Techniques and Procedures) are translated back into the Argus ecosystem to benefit all of our customers.

Applied Threat Intelligence

Threat Intelligence plays a vital part of our security monitoring services. Our threat intelligence process is integrated into the Argus platform, and we have an eco-system within Argus for applying threat data and information to all security analysis activities in near real-time.

An example of applying Threat Intelligence within the Argus Platform is how threat information is shared across our customer base. For example, if we alert Customer X about a drive-by download from a given website, an e-mail with a malicious attachment, or similar, relevant details of the attack information (e.g. Indicators of Compromise) are reused for improving detection for other customers. This shortens the time to detection significantly. Furthermore, it ensures that an attack that affects Customer X will enable us to detect similar attacks targeting other customers. Note that we do not share information that can be used to identify other customers, unless we have explicit consent from the affected party to do so.

1.3.6 Reporting

Various reports intended for both management and technicians are available and included as part of the service. The Argus portal provides flexible reporting capabilities to support users' individual needs and as a communication channel to deliver security reports from mnemonic. Reports are available both on-demand and delivered periodically, and may be available in several file formats (PDF, CSV, etc.).

The periodic reports delivered as part of the service are:

- **Weekly reports** to summarise alarms and notifications from the previous week. The weekly report is a technical report intended to provide details on incidents and trends to help further identify unexpected or undesirable traffic patterns.
- **Monthly/quarterly** reports describe incidents in even greater detail, discuss current threats and vulnerabilities and provide advice on how information security can be improved. The report is intended for both technicians and management, and includes:
    - Management summary
    - Service on-boarding (status on project)
    - Service improvement (planned activities)
    - Local and global analysis of the threat landscape
- **Annual reports** that summarize the previous year's activity within the service as well as general security information based on mnemonic's experiences over the past twelve months.

In addition, the Argus Customer Portal supports flexible report features such as:

- On-demand generated reports for all users
- Predefined report templates that customers can use to create their own reports
- Ability to edit and customize reports with editor
- Export reports to PDF and HTML formats
- Archive containing all reports

Sample from a monthly/quarterly report:

Contents

Summary

This report provides an overview of the managed security monitoring solution as delivered by mnemonic to Demo for the previous month. The report is focused on security incidents as reported through the mnemonic customer portal. It also includes observations and assessments concerning the local and global threat landscape, as well as ongoing and recommended activities as relating to the service.

Security incidents for January 2015:

Case ID	Priority	Subject
23028985	3	Toolbar download from 198.168.1.2 to a client behind 10.0.0.1
23011139	4	Advisory - CTBLocker campaign hits Nordics
22948269	3	Suspicious traffic from 172.27.1.2 to 10.0.0.2.
22936413	3	Download of unwanted software from 10.0.0.3 to 192.168.2.1

The incident in **bold** are pending action from Demo at the time of writing.

The chapter on *Projects and Activities* list a number of activities that need follow-up. Mnemonic recommends that we have a service meeting subsequent to the publishing of this report.

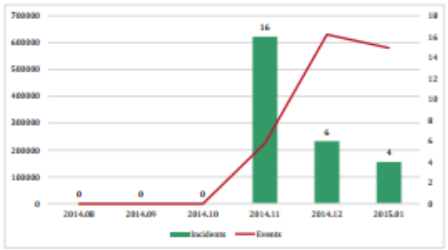
The common chapters at the end of the report is a summary of current observations from Scandinavia and globally, as well as information on new vulnerabilities and threats.

Service overview

Security Monitoring

mnemonic monitors traffic between the Demo office network and the Internet. The listening interface of the Intrusion Detection System sensor is receiving traffic from the external interface of Demo's outside firewall.

The graph below shows alarms that have been considered for the past six months:



The lack of incidents between August and October was due to a relocation of Demo infrastructure which led to the IDS not receiving traffic. The sensor was reconnected to the SPAN port on November 11.

Projects and activities

This chapter is a summary of activities that concern the service

A#1: Information about Demo's internal infrastructure	
Description	In order to deliver a better service, mnemonic has requested information about Demo internal IP addressing and network diagrams.
Status	Mnemonic is waiting on Demo to provide this. However, until we move the monitor location to look at internal traffic, this will not provide any useful information.

A#2: Improve current monitoring solution	
Description	The current view that mnemonic has of Demo traffic is limited. We are seeing traffic on the external interface of the firewall, and not the internal IP addresses. mnemonic has suggested two alternative solutions: 1) Move the network "tap" location to the inside of the firewall 2) Add security monitoring of the external firewall logs for correlation
Status	We will dicuss internal IDS monitoring on the status meeting January 27.

A#3: SIEM system integration	
Description	Demo wishes to integrate the security monitoring solution with their internal SIEM system.
Status	Mnemonic has provided information to Demo for integration.

1.3.7 Other common reports

Statistical reports are reports that represent statistical data relevant to a service element. These are automatically generated by the Argus platform, and can be customized to view any data source that is available to the service. This contains a number of different statistical tools and diagrams. These reports are used to measure specific service elements, and are useful for detecting trends and watching utilization levels.

SLA reports are reports that report specifically on key metrics agreed in the service contract. The service level agreement will typically dictate metrics such as response times, uptime, system availability and false positive ratios. These reports are manually created. These reports are used to measure the service delivery and for identifying issues that need to be addressed.

Security Management reports are reports containing high level information about the service delivery, such as what service is being delivered, what incidents have been detected, information about incident handling and any trends in security event data. The reports also contain threat intelligence information that is relevant to the customer. The reports are manually created by the Technical Account Manager. These reports are used to assess the security status, and to gain control of incident statuses.

Business Management reports are aimed at higher level executives with responsibility for IT and IT security. These reports connect any security incidents and security data to the business value chain to highlight any changes in risk status. The reports are manually created by a security risk professional. These reports are used to demonstrate value of IT security investments and to identify significant changes in risk posture as the result of incidents or the current threat climate.

Regulatory reports provide insight into how the service delivery answers or corresponds to specific regulatory requirements. These include legal requirements, as well as industry standards such as ISO or PCI, or internal security policies. These reports are designed together with the customer to ensure that they cover the necessary topics at the level of detail that is required. We can extract and report on any regulatory relevant information that has been included in the service data collection.

1.3.8 Quarterly status meetings

Quarterly status meetings will be arranged to discuss various aspects of the service delivery. Status meetings are conducted either on-site or via conference call between the Technical Account Manager at mnemonic and representatives from the customer. Additional mnemonic staff may also participate as necessary.

The status meeting agenda is agreed upon in advance and typically covers:

- Review of open cases and noteworthy closed cases
- Recommendations on general security and service improvements based on incident observations and analysis
- Relevant, customer-specific security and incident trends
- Customer’s business context – changes in the customer’s business that may affect the service delivery
- Service roadmap
- Overview and discussion about security trends and active threats

1.3.9 Full service infrastructure management

Argus Managed Defence is a fully managed security service. This means that for all hardware and software deployed as part of the service, mnemonic will manage:

- ✓ all minor and major upgrades
- ✓ hardware & software health monitoring
- ✓ other ongoing maintenance tasks
- ✓ patching
- ✓ any applicable vendor maintenance contracts

Support for the underlying infrastructure (e.g. Argus Network Analyser) are monitored and follow similar analysis, response and notification procedures as detected security events on the customer network.

Upgrades, patching, and configuration changes to the infrastructure or service are expected during the normal operation of the Argus Managed Defence service. mnemonic follows best practices for auditing, evaluating change impact, and general change management procedures to minimize the impact on the service delivery.

1.4 Service implementation project

Argus Managed Defence is implemented using mnemonic's project management framework. Our framework 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 are delivered on-time.

The service implementation project encompasses technical components, such as physical 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 Managed Defence service 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:

- Service design: high and low-level designs
- Planning technical and procedural integration of service
- Classification and documentation of assets and services
- Physical installation of hardware
- Configuration, testing and tuning
- Data collection to observe traffic patterns and establish normal traffic baselines
- 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.

1.5 Complementary services

Argus Managed Defence can be expanded with additional integrated services, and supplemented with complementary security services from mnemonic. Below are a few examples.

Managed Security Solution	**Incident handling and/or incident response**	**Advanced malware detection technology**
24x7 management of network and security appliances and solutions, including: firewalls, mail proxy, web proxy, web application firewall and more	The mnemonic Incident Response Team helps organisations respond, handle, and recover from incidents every day. The team can also help improve your internal response capabilities.	Malware is evolving, becoming more elusive and bypassing traditional defences. Integrate the leading advanced malware detection solutions to Argus Managed Defence.
DDoS mitigation	**mnemonic Premium Support**	**Managed PCI DSS testing & scanning**
DDoS attacks can target any Internet service at any time without any warning. Having the right protection in place can mitigate the attack and keep your services running uninterrupted.	Working with the industry's leading security vendors, mnemonic provides 24x7 support to help your systems stay up and running and keep business running as usual.	Ensure payment card information is secured by testing your systems for vulnerabilities, meet PCI DSS requirements and stay compliant.
Risk & Security consultancy services	**Argus Endpoint Responder**	**Argus Continuous Vulnerability Monitoring**
Need to conduct a risk assessment? Test the security of a new application? Design a secure infrastructure? If it's related to security, our 180+ security consultants can help.	Expand detection and response capabilities to your endpoints and gain the capability to quickly isolate and contain infected or targeted machines from the rest of your network.	Vulnerabilities in software are a significant risk to your business. Know which of your systems are vulnerable, how to patch them and how to protect them before a patch is available.

2 About mnemonic

mnemonic helps businesses manage their security risks, protect their data and defend against cyber threats. Our expert team of security consultants, product specialists, threat researchers, incident responders and ethical hackers, combined with our Argus security platform ensures we stay ahead of advanced cyberattacks and protect our customers from evolving threats.

Acknowledged by Gartner as a notable vendor in delivering Managed Detection and Response (MDR) services, threat intelligence and advanced targeted attack detection, we are among the largest IT security service providers in Europe, the preferred security partner of the region's top companies and a trusted source of threat intelligence to Europol and other law enforcement agencies globally (www.mnemonic.no/Gartner).

With intelligence-driven managed security services, 200+ security experts and partnerships with leading security vendors, mnemonic enables businesses to stay secure and compliant while reducing costs.

mnemonic facts

Founded: 2000

Offices: Norway – Oslo (HQ), Stavanger
Sweden - Stockholm
UK – London
USA - Palo Alto, CA
The Hague, Netherland.

Employees: ~250

Consultants: ~200

Certifications: ISO 9001, ISO/IEC 27001:2013, PCI DSS ASV