MANAGED DETECTION AND RESPONSE (MDR)

MDR detects, analyzes and contains attacks faster for you.

Outcomes, not alerts

MDR natively built for the cloud era

MDR is specifically designed to detect advanced threats that bypass existing security controls. These threats are complex in nature, where correct identification often requires the correlation of suspicious behaviors from many different angles.

The foundation of Open Systems MDR is a cloud-based SIEM – Azure Sentinel by Microsoft – in unison with MDR Sensors for threat detection, as well as automation and a two-tier operations model. MDR provides advanced threat detection for activities across the cyber kill chain.

Modules

Open Systems MDR model.

Type	Component	
MDR Sensors	Endpoint Detection and Response (EDR) Network Detection and Response (NDR)	Either EDR or NDR is necessary
Security Logs	Open Systems logs	Firewall and Secure Web Gateway (proxy) necessary
	Third-party logs	
Context Logs	Active Directory logs DNS logs DHCP logs	Necessary
	Client logs, cloud logs, other logs	Optional

The following Microsoft components are necessary for the MDR service:

- Azure Sentinel
- Azure Monitor Log Analytics Workspace

MDR Sensors

The following sensor scenarios are possible:

- Use both EDR and NDR
- Only use EDR
- Only use NDR

Note: A mix is also possible e.g. EDR and NDR for offices, but only NDR for data centers.

Security Logs

Open Systems and third-party Security Logs:

- Firewall logs (necessary)
- Secure Web Gateway logs (necessary)
- Secure Email Gateway logs
- Azure ATP
- IDS
- Other Security Logs

Context Logs

Different types of Context Logs are supported:

- DNS Server (necessary)
- DHCP Server (necessary)
- Active Directory (necessary)
- Client logs
- Cloud logs
- Other logs

Integrated Service Management

For MDR and EDR services, engineers work with you as part of the Security Operations Center (SOC) of Open Systems in one of two roles:

- **DevOps Security Engineers:**
  - Perform initial triage of alerts
  - Investigate each incident for certitude of whether the incident is real or a false positive
  - Escalate true positives and suspicious behaviors
- **Designated Security Analysts:**
  - Are responsible for each account and supported by the entire Open Systems SOC team
  - Investigate the harm done by the incident and respond to it, e.g. isolate host, contain the threat, clean the computer
  - Do proactive threat hunting

24x7 Operations by Mission Control – our integrated NOC and SOC

Installation

- Definition of technical configuration
- Definition of the administrative contacts and escalation procedures
- Customized detection tuning based on your potential attack surfaces

Alert handling

- Triage of incoming alerts (plausibly separate true positives from false positives)
- Suspicious events are reported to you together with a proposal for next steps
- Feed tuning: reduction of false positives and new rules to increase sensitivity to detecting further attacks
- Creation of watchlist from your provided indicators of compromise (IOCs)
- Escalation of alerts (true positives) to you or host isolation according to agreed-upon procedures

24x7 monitoring

- 24x7 proactive monitoring
- Event notifications (by email or SMS), automatic log file analysis and reporting
- Prompt response to detected critical events
- Unlimited number of escalations, tickets, support calls
- Direct support by Open Systems engineers
- Support for other third-party log sources via raw text and syslog
- Log search for all collected logs over the period defined by your selected data option
- Open Systems curated threat intelligence used for threat detection
- Log retention:
  - Logs will be stored for 90 days (standard)
  - Additional options: you can choose to store logs from 1 to 7 years

Troubleshooting, investigation and maintenance

- Collaborative investigation board
- Threat response including recommended response actions to true positive incidents
- Threat containment (using Open Systems Security Stack)
- Real-time auditability with integrated ticketing system
- Debugging of incidents within the periods defined in the SLA
- Analysis, testing and installation of software patches and upgrades
- Predefined disaster recovery processes

Change management

- Enforced change management processes by comprehensive ticketing system and built-in sign-off procedures
- Review of change requests by Open Systems engineers, clarifications and feedback in case of hidden risks
- Strong user authentication with audit trail

Reporting

- Monthly SOC reporting and status meetings with Open Systems Security Analysts
- Real-time reporting of configuration settings and logs
- Compliance report: Service Organization Controls 1 Type 2 (SOC 1)

Coverage of technology risk

- Hardware and software are replaced free of charge if defective, outdated or if the quality or availability of the implemented systems are no longer guaranteed by the manufacturer

Mission Control Portal

- Delegated administration
- Ticketing

VANREIN COMPLIANCE
HIPAA Compliance Verified by VanRein Compliance 2020

swiss safety center ISO/IEC 27001 certified system

Open Systems services are ISO 27001 certified.

Approved for public use.

ENDPOINT DETECTION AND RESPONSE (EDR)

To defend against current threats, the endpoints need to be part of the plan.

EDR
Critical monitoring and analysis of endpoints

Endpoint Detection and Response (EDR) provides critical monitoring and fast analysis of your endpoint devices – for example laptops and servers – even if they're not connected to your network.

The EDR service monitors your endpoints, alerts you if there are suspicious activities, and isolates the compromised systems to prevent further spread of the attack in your environment. EDR is available standalone or as a core component of the Managed Detection and Response (MDR) service by Open Systems.

The EDR service is based on sensor agents that are deployed to endpoint devices, such as user machines or servers, in your environment. The endpoint sensors provide:

- A source of truth in the environment, which is used both for tickets in Mission Control as well as context for threat hunting and correlation
- Access to the endpoint for Open Systems SOC analysts to query the running state in order to confirm true positive attacks
- SOC analysts with the possibility to use Microsoft Defender for isolating a compromised host

The following two (mutually exclusive) endpoint agent options are available:

- Microsoft Defender for Endpoint (bring your own license model)
- Carbon Black Cb Response (license reselling model)

Microsoft Defender for Endpoint

Microsoft Defender is supported in the BYOL (bring your own license) model. Customers acquire licenses through Microsoft directly.

- Open Systems engineers use the EDR features for the purpose of advanced threat detection and containment
- Out-of-scope features include vulnerability management, next-gen protection (anti-virus), attack surface reduction (network and URL filtering) and Microsoft threat experts

- Deployment and configuration of Microsoft Defender for Endpoint on the endpoints is the responsibility of the customer.
- Customers need to provide access to the Microsoft Defender for Endpoint Portal to the Open Systems SOC (requires Azure AD Premium P2 license).

Carbon Black Cb Response

With Cb Response as endpoint technology, the service includes the reselling of the license as well as full management of the monitoring and alerting infrastructure.

EDR server infrastructure

Setup and maintenance of the server components to deploy EDR in your organization.

- Two models for server hosting are available:
  - Cb Response SaaS offering
  - Open Systems hosted server in the Mission Control secure data centers
- Installation and maintenance of server operating system
- Operations and configuration backup of EDR server
- Definition of the administrative contacts and escalation procedures
- Analysis, testing and installation of software patches and upgrades

EDR client agent

- Provisioning of patches and agents to you for deployment

Deployment of the client agent software to the endpoints is the responsibility of the customer.

Access

- The customer has full read access to the Cb Response interface
- Live log forwarding in syslog format to customer log destinations or the MDR SIEM

Integrated Service Management

For the MDR and EDR services, engineers work with you as part of the Security Operations Center (SOC) of Open Systems in one of two roles:

- **DevOps Security Engineers**:
  - Perform initial triage of alerts
  - Investigate each incident for certitude of whether the incident is real or a false positive
  - Escalate true positives and suspicious behaviors
- **Designated Security Analysts**:
  - Are responsible for each account and supported by the entire Open Systems SOC team
  - Investigate the harm done by the incident and respond to it, e.g. isolate host, contain the threat, clean the computer
  - Do proactive threat hunting

Baselining or learning phase

- Activate alliance feeds
- Initial feed tuning (minimizing false positives)

Custom indicators of compromise (IOCs)

- Creation of watchlists from customer-provided IOCs (md5 hashes and domains)
- Installation of blocklists for customer-provided hashes of executables

Other watchlists can be created but will be charged according to the work necessary.

24x7 Operations by Mission Control – our integrated NOC and SOC

Installation

- Definition of technical configuration
- Definition of the administrative contacts and escalation procedures

Alert handling

- Triage of incoming alerts (plausibly separate true positives from false positives)
- Suspicious events are reported to you together with a proposal for next steps
- Feed tuning: reduction of false positives and new rules to increase sensitivity to detecting further attacks
- Creation of watchlist from your provided indicators of compromise (IOCs)
- Escalation of alerts (true positives) to you or host isolation according to agreed-upon procedures

24x7 monitoring

- 24x7 proactive monitoring
- Event notifications (by email or SMS), automatic log file analysis and reporting
- Prompt response to detected critical events
- Unlimited number of escalations, tickets, support calls
- Direct support by Open Systems engineers
- Log retention:
  - Logs will be stored for 60 days
  - Alerts will be stored permanently

Troubleshooting and maintenance

- Debugging of incidents within the periods defined in the SLA
- Analysis, testing and installation of software patches and upgrades

Mission Control Portal

- Delegated administration
- Ticketing

VANREIN COMPLIANCE
HIPAA Compliance Verified by VanRein Compliance 2020

swiss safety center ISO/IEC 27001 certified system

Open Systems services are ISO 27001 certified.

NETWORK DETECTION AND RESPONSE (NDR)

Get holistic situational awareness of your network to act on cyberattacks immediately.

NDR

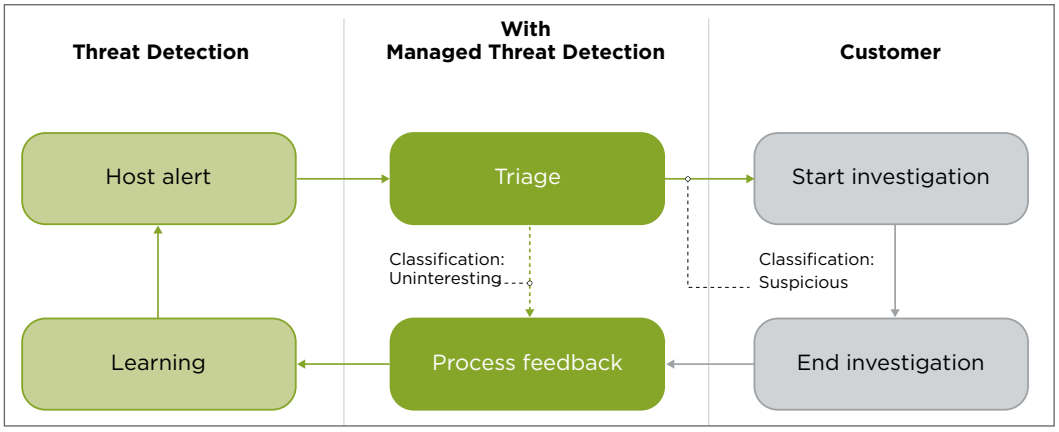
Protect your network by eliminating blind spots

The key to managing network breaches is finding them quickly. Network Detection and Response closes the gap between traditional detection and security monitoring and more complex SIEM/SOC solutions.

- Global event collection
- Threat score algorithm
- Notification of high threat score
- Global dashboard
- Local dashboard for delegated administration
- Drill down from global overview to event details
- Host view including context information
- Event categorization (see Managed and Unmanaged NDR)
- Exclusion lists for events and hosts (see Managed and Unmanaged NDR)
- Combination of protocol, signature and anomaly-based inspection
- Multiple sources of threat intelligence signatures
- Packet capture utility
- Inspection of encrypted HTTPS traffic in combination with Secure Web Gateway

Managed NDR

- Notification of high threat score to Mission Control operations
- Process-based event validation and classification by Mission Control
- Process-based escalation by Mission Control



Managed NDR: Open Systems engineers perform the triaging process.

Managed NDR is available for the Enterprise Plus package of Secure SD-WAN, or as part of Managed Detection and Response (MDR).

Unmanaged NDR

You manage the triaging process internally. Your analysts can access detailed contextual and event information for their analyses.

Unmanaged NDR: you manage the triaging process internally.

Integrated Service Management

Service Delivery Platform

- Industrial strength hardware: on your premises, or at a data center, or as a virtual platform in the cloud
- Hardened operating system
- Multi-release boot configuration for fallback and recovery
- Database-supported and automatic configuration compilation
- IPv6 compatible
- Log file distribution via syslog forwarding

24x7 Operations by Mission Control – our integrated NOC and SOC

Installation

- Definition of technical configuration
- Definition of the administrative contacts and escalation procedures
- Creation of the network topology diagram
- Preconfiguration, delivery and functional verification tests of the Open Systems service with all required hardware and software components
- Initial learning phase for optimal tuning to specific environment

24x7 monitoring

- 24x7 proactive monitoring, event notifications (by email or SMS), automatic log file analysis and reporting
- Prompt response to detected critical events
- Unlimited number of escalations, tickets, support calls
- Direct support by Open Systems Security Engineers

Change management

- Enforced change management processes by comprehensive ticketing system and built-in sign-off procedures
- Review of change requests by Open Systems Security Engineers, clarifications and feedback in case of hidden risks
- Strong user authentication with audit trail

Troubleshooting and maintenance

- Real-time auditability with integrated ticketing system
- Debugging of incidents within the periods defined in the SLA
- Replacement of defective or outdated hardware and restoring of functionality
- Analysis, testing and installation of software patches and upgrades
- Predefined disaster recovery processes

Reporting and logging

- Real-time executive overview
- Real-time network utilization and system load statistics
- Real-time reporting of configuration settings and logs
- Compliance report: Service Organization Controls 1 Type 2 (SOC 1)

Coverage of technology risk

- Hardware and software are replaced free of charge if defective, outdated or if the quality or availability of the implemented systems are no longer guaranteed by the manufacturer

Mission Control Portal

- Strong user authentication with audit trail
- Delegated administration
- Ticketing
- Real-time monitoring and reporting
- Strong user authentication with audit trail
- Full audit log
- Real-time view of operational key figures and statistics
- View of relevant configurations
- Self-service and debugging tools

VANREIN COMPLIANCE
HIPAA Compliance Verified by VanRein Compliance 2020

Open Systems services are ISO 27001 certified.

Approved for public use.