Heimdal®

eXtended Detection & Response/SOC Service

Heimdal®'s Managed XDR Improves the MDR and XDR Standards

Best of the Best in First-Rate Threat Discovery and Mitigation

Scalable, Customizable & Time Saving

Heimdal XDR powered SOC is your scalable prebuilt Security Operations Center. Based on Heimdal's unique intelligent security stack, we have eliminated the need for time consuming and error prone implementations. Our unified solutions communicate using AI and ML out of the box, with no need for APIs.

Based on our flexible XDR capabilities and modular solutions, the Heimdal XDR powered SOC offers the freedom to customize your desired level of protection through more than 55 different combinations including our award-winning E-PDR.

The Newest Addition to Your Security Team

The Heimdal XDR powered SOC Teams act swiftly to address malicious incidents by blocking domains, quarantining malicious processes & e-mails, applying patches for critical vulnerabilities, as well as isolating infected machines. During and after an incident our teams report the findings, actions, and resolution. Furthermore, they provide actionable steps to prevent future attacks on the affected vectors.

Backed by a next-gen SOAR* platform the SOC teams are capable of proactively mitigate threats by automatically patching of critical vulnerabilities and repetitively monitoring and adjusting all security settings.

*SOAR: Security orchestration, automation, and response

Environment Security. Outsourcing Simplified.

The Heimdal XDR powered SOC teams take ownership of your Heimdal security setup, by proactively monitoring and adjusting your security level in response to new trends and exploits in the threat landscape, keeping you safe from Zero-Day attacks.

Through a structured mix of network and endpoint monitoring, behavioral analysis, Machine Learning tools, and threat intelligence, Heimdal tracks and addresses emerging threats that traditional solutions don't. Your user experience levels up, as you trade fragmented tools and data for a consolidated, cohesive approach to threat identification and response.

Hidden and complex threats are discovered faster, with more accurate investigation results to avoid downtime and loss of productivity.

What You Get with Heimdal XDR Powered SOC

Support Levels:

1

- ✓ Proactively adjusting security levels
- ✓ Real-time correlation against IOC/IOAs
- ✓ Processing alert events
- ✓ Reducing false positives

2

- ✓ Deep analysis of alert events
- ✓ Hunt for & identify new IOCs
- ✓ Uncover full impact on environment

3

- ✓ Isolate impacted endpoints
- ✓ Remove malware and clean infected machines
- ✓ Close vulnerabilities & attack vectors
- ✓ Report findings, actions and next step recommendations

Expand Your Security Level with the Heimdal Suite

The Heimdal XDR powered SOC Service brings to the table an efficient threat detection, analysis, and response service empowering your incident response plan to be quick and effective.
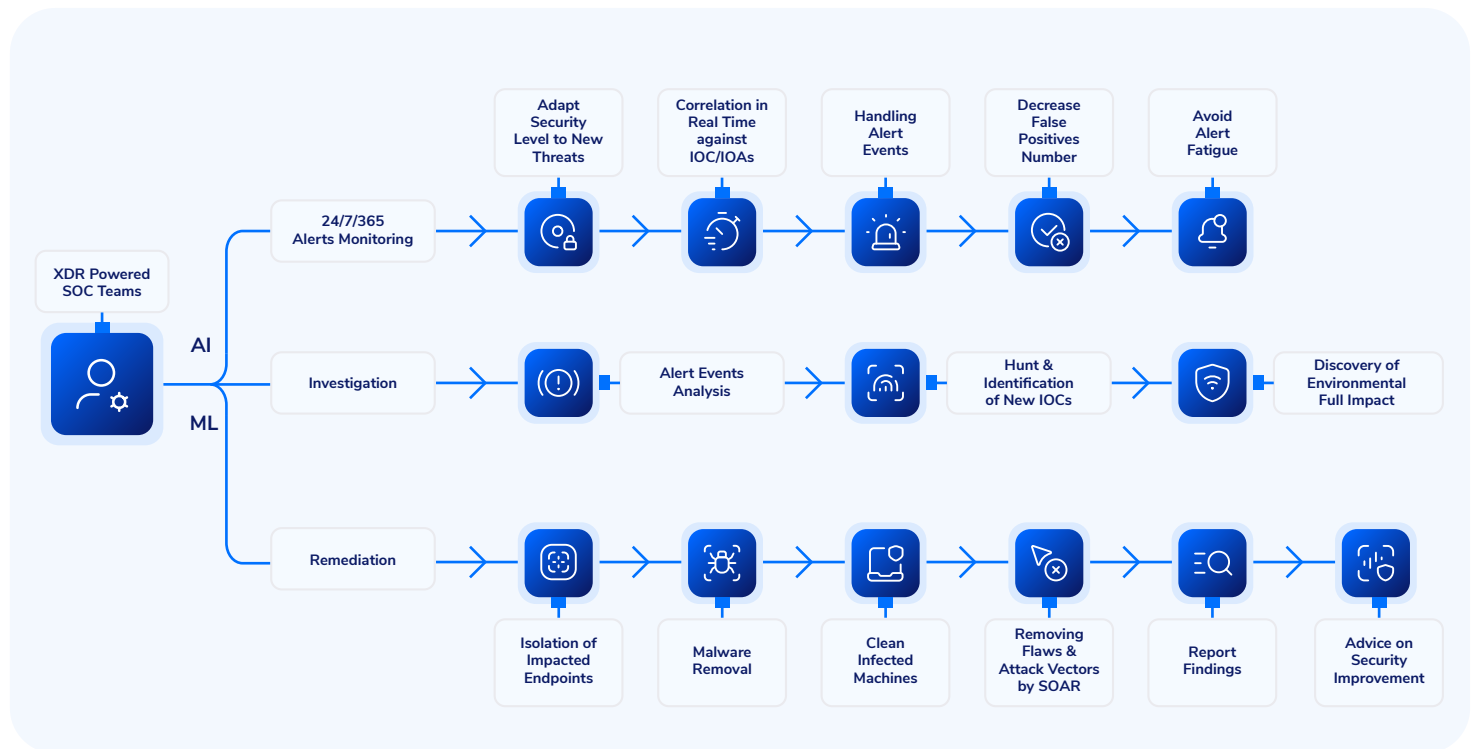
The Service scales with Heimdal's modular product line-up, allowing you to add a response to every security risk.

Expand your security stack with more modules from the Heimdal Unified Suite and take advantage of further benefits like first rate threat hunting, e-mail security, vulnerability management or even ransomware encryption protection.

The XDR powered SOC teams monitor your Heimdal security stack 24/7/365 with the help of artificial intelligence lowering the amount of false-positives and avoiding alert fatigue.

Boost the Effectiveness of Your Cyber-Defenses

Level up your cyber defense with a proactive approach on monitoring, investigation and remediation featured in our Heimdal XDR powered SOC Service.

XDR Powered SOC Teams — AI / ML

24/7/365 Alerts Monitoring → Adapt Security Level to New Threats → Correlation in Real Time against IOC/IOAs → Handling Alert Events → Decrease False Positives Number → Avoid Alert Fatigue

Investigation → Alert Events Analysis → Hunt & Identification of New IOCs → Discovery of Environmental Full Impact

Remediation → Isolation of Impacted Endpoints → Malware Removal → Clean Infected Machines → Removing Flaws & Attack Vectors by SOAR → Report Findings → Advice on Security Improvement
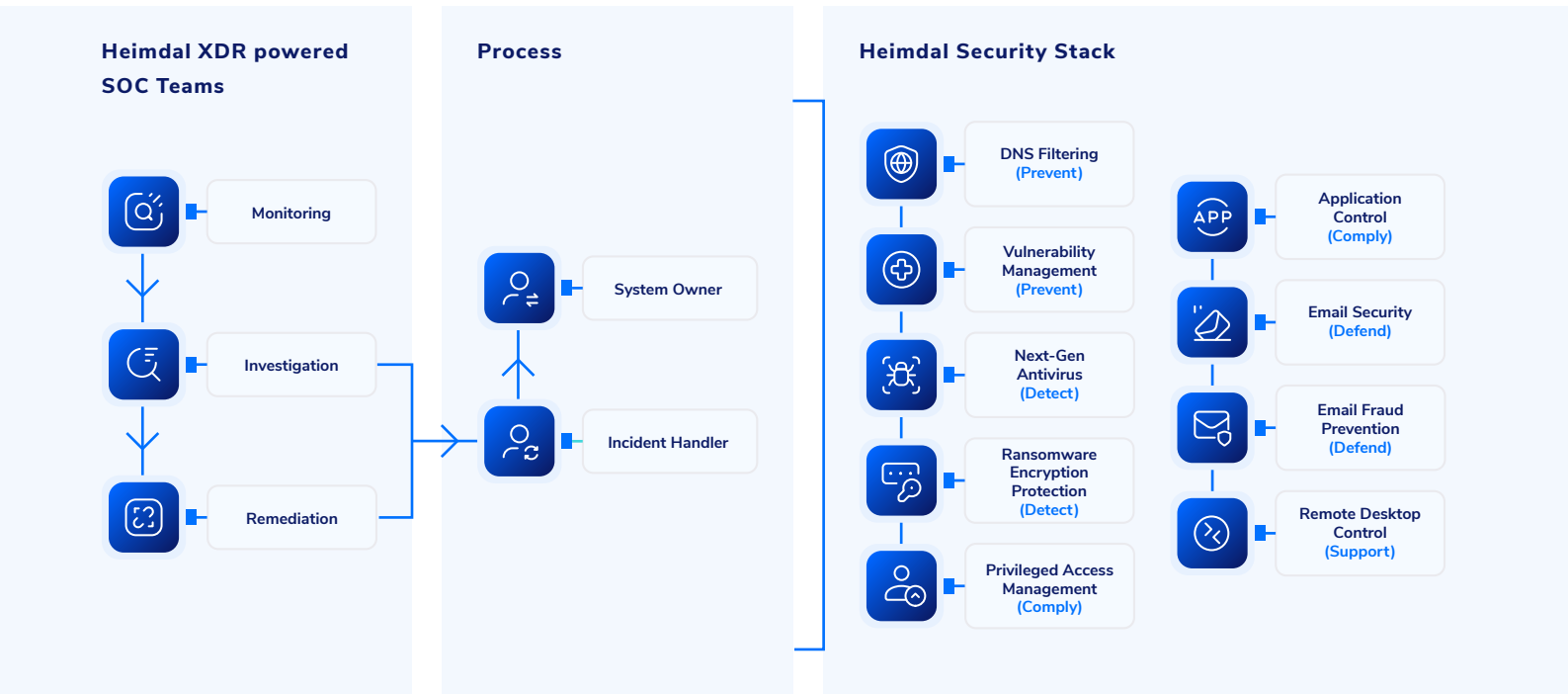
Expert Knowledge and Top-Notch Security at Your Fingertips

Get unparalleled security expertise, reliable threat intelligence, and automation to uplift your cybersecurity. We employ a rapid and decisive response to attacks and provide you with extended, systemized reports on potential risks, malwares, and vulnerabilities.

Heimdal's security professionals go through all sequences of events and continuously inspect users using rights escalations, privileges, app executions and we also proactively supervise your ingoing and outgoing emails. Our agents' ace in the hole is that they operate by playbooks aligned to the MITRE attack framework making sure you benefit from top-notch security.

Built on Heimdal's Security Stack, XDR Powered SOC Service Provides You with a Reliable Process

The Heimdal XDR powered SOC Service is designed to work to your entire benefit, being built on top of Heimdal's Security stack, not on any third-party integration. The XDR powered SOC teams consist of humans who employ AI support to provide you with a seamless and reliable designated process.

Heimdal XDR powered SOC Teams

- Monitoring
- Investigation
- Remediation

Process

- System Owner
- Incident Handler

Heimdal Security Stack

- DNS Filtering (Prevent)
- Vulnerability Management (Prevent)
- Next-Gen Antivirus (Detect)
- Ransomware Encryption Protection (Detect)
- Privileged Access Management (Comply)
- Application Control (Comply)
- Email Security (Defend)
- Email Fraud Prevention (Defend)
- Remote Desktop Control (Support)

Heimdal XDR Powered SOC Comes with an Extensive Spectrum of Benefits

- Effortless setup & implementation
- Say goodbye to complicated setup and enjoy actual usage
- Product ownership that triggers proactive settings adjustment
- A full security stack that enables to manage everything from our end

- Easy Setup
- Effortless Implementation
- Proactively Adjusting Settings

Heimdal XDR powered SOC

- Actual Usage
- Product Ownership
- Complete Security Stack
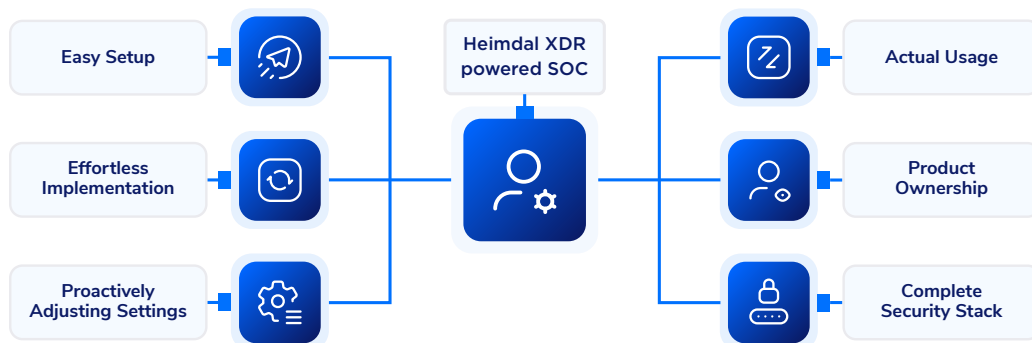
We Value Your Time

Benefit from continuous monitoring 24/7/365 and boost your productivity with less time spent on threat hunting. Especially if you lack your own incident response team, time is precious and with XDR, you can get straight to the conclusions and visibility that matters!

The Support Team Is Here for You

Contact your Heimdal's Technical Support Department to help you with:

- Technical Issues
- Questions
- Feedback
- Bug Reports
- Warranty Claims

How You Can Reach Us

corpsupport@heimdalsecurity.com

UK +44 1445 700309 | US +1 (855) 220-2405 | DK +45 78 75 03

Or choose the easy path and go to our website directly here, click on the Support button, then on the Submit a request button or click on the Support button from your Heimdal Dashboard to make a request.

About Heimdal®

Founded in 2014 in Copenhagen, Denmark, Heimdal® is a **leading European provider of cloud-based cybersecurity solutions.**

The company offers a multi-layered security suite that combines threat prevention, patch and asset management, endpoint rights management, and antivirus and e-mail security which together secure customers against cyberattacks and keep critical information and intellectual property safe.

Heimdal has been recognized as **a thought leader in the**

industry and has won multiple awards both for its solutions and for its educational content.

Currently, **Heimdal's cybersecurity solutions are deployed in more than 50 countries** and supported regionally from offices in 15+ countries, by 175+ highly qualified specialists. Heimdal is ISAE 3000 certified and secures **more than 3 million endpoints** for over 11,000 companies.

The company supports its partners without concessions on the basis of predictability and scalability, creating sustainable ecosystems and **strategic partnerships.**

HEIMDALSECURITY.COM