Threat-Hunting and Action Centre battlecard

Company overview

Heimdal®

Heimdal offers an end-to-end, proactive, unified cybersecurity suite built to defend against next-gen threats. The unique, multi-layered approach provides comprehensive protection across all areas. Through Heimdal, you can experience advanced protection across your organisation.

Product – Threat-Hunting and Action Centre (TAC)

TAC key features include:

- Provides security leaders, operation teams, and MSPs the ability to detect and respond to next-gen threats across IT landscapes or customer bases
- Detailed data of IT environments, endpoints and networks helping teams proactively classify security risks, hunt detected irregularities, and neutralise persistent threats in a secure environment
- The capability to run and execute commands including file scans, malware quarantines, software patches, machine isolation on the go
- One-click resolutions can take place whilst investigating incidents or threats using deep analysis reporting modules
- Engineered and designed by Heimdal security experts from the ground up allows security teams to move away from manual security operations

Benefits

- Empowers teams of all levels (CIOs, CISOs, Heads of Security, Security Ops and IT Admins and MSPs)
- Clear visibility of risk in a single view
- Real-time threat-centric view of digital risk
- Cost saving – balance budget & skill gap within a security department
- Reduced MTTD, risks are pre-scored by priority indicators
- Faster MTTR with instant action and resolution centre for smaller teams
- Speedy customer onboarding and management with multi-tenant architecture
- Single pane of glass monitoring
- Resolve incidents at the point of risk with pre-scored indicators
- Upskill teams and scale operations as a customer base grows

	Heimdal® TAC	Azure Sentinel
Real-time threat detection	Y	Y
Patch management	Y	N
Automated response	Y	Y
Machine learning	Y	Y
Integration with SIEM	Y	Y
Phishing prevention	Y	N
DNS security	Y	N
Behaviour analysis	Y	Y
Endpoint detection and response	Y	Y
Endpoint visibility	Y	Y
Cost	**Heimdal offers competitive pricing suitable for SMEs whereas CrowdStrike has far higher pricing, making it unsuitable for smaller businesses.**	

Objection handling

How do I know to go for TAC or MXDR?
If you have your own SOC team, TAC is the best option for you. If you don't have a dedicated team providing 24/7 support and monitoring, MXDR is the right choice for you.
Can it integrate with our existing SIEM platform?
Yes, Heimdal integrates with SIEM platforms that have available APIs, however, TAC is a SIEM within itself, incorporating multiple Heimdal products into one space.