Heimdal®

Security & Compliance Simplified

Brigantia Compliance Roadshow – March 2025

www.heimdalsecurity.com

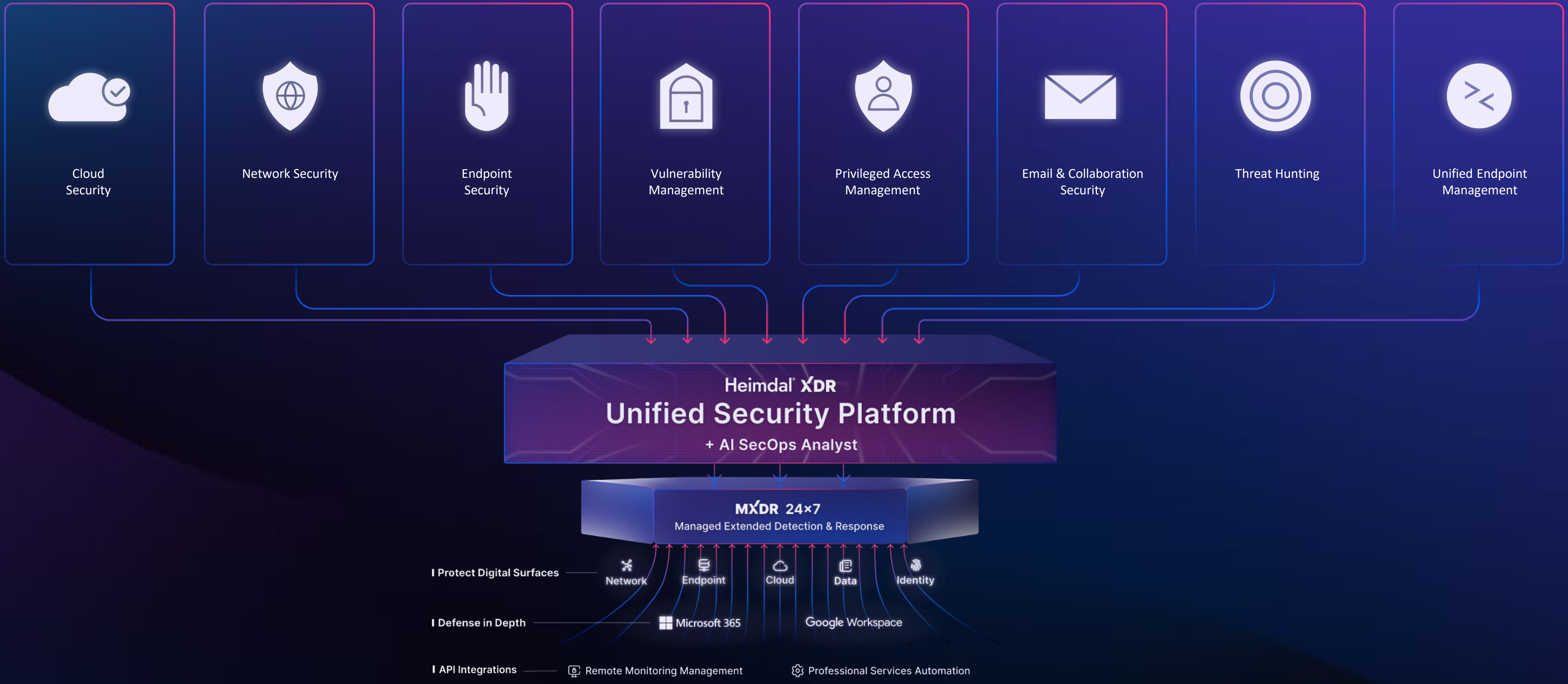
Clelia Di Maio

MSP Customer Success Manager

Empower your MS(S)P with Heimdal's unified security solutions—boosting efficiency and enhancing client protection. Our innovation serves over 16k customers and 1k MS(S)Ps, leading the charge against cyberthreats.

Let's connect and grow your business with advanced cybersecurity that's ready for the future.

Heimdal®



Cloud Security

Network Security

Endpoint Security

Vulnerability Management

Privileged Access Management

Email & Collaboration Security

Threat Hunting

Unified Endpoint Management

Heimdal® XDR

Unified Security Platform

+ AI SecOps Analyst

MXDR 24×7

Managed Extended Detection & Response

I Protect Digital Surfaces

Network

Endpoint

Cloud

Data

Identity

I Defense in Depth

Microsoft 365

Google Workspace

I API Integrations

Remote Monitoring Management

Professional Services Automation

Heimdal®

260M+
Cyber Attacks Prevented

16K+
Organizations Secured

70M+
Vulnerability Patched

Widest XDR Technology Stack in the Industry

TECHNOLOGY RESELLER AWARDS 2024
Cyber Risk Mitigation Vendor of the Year

teiss Awards2024
RUNNER - UP
Best Vulnerability Management Solution

Expert Insights
Top Solution
★★★★★
2023

Awards and Achievements

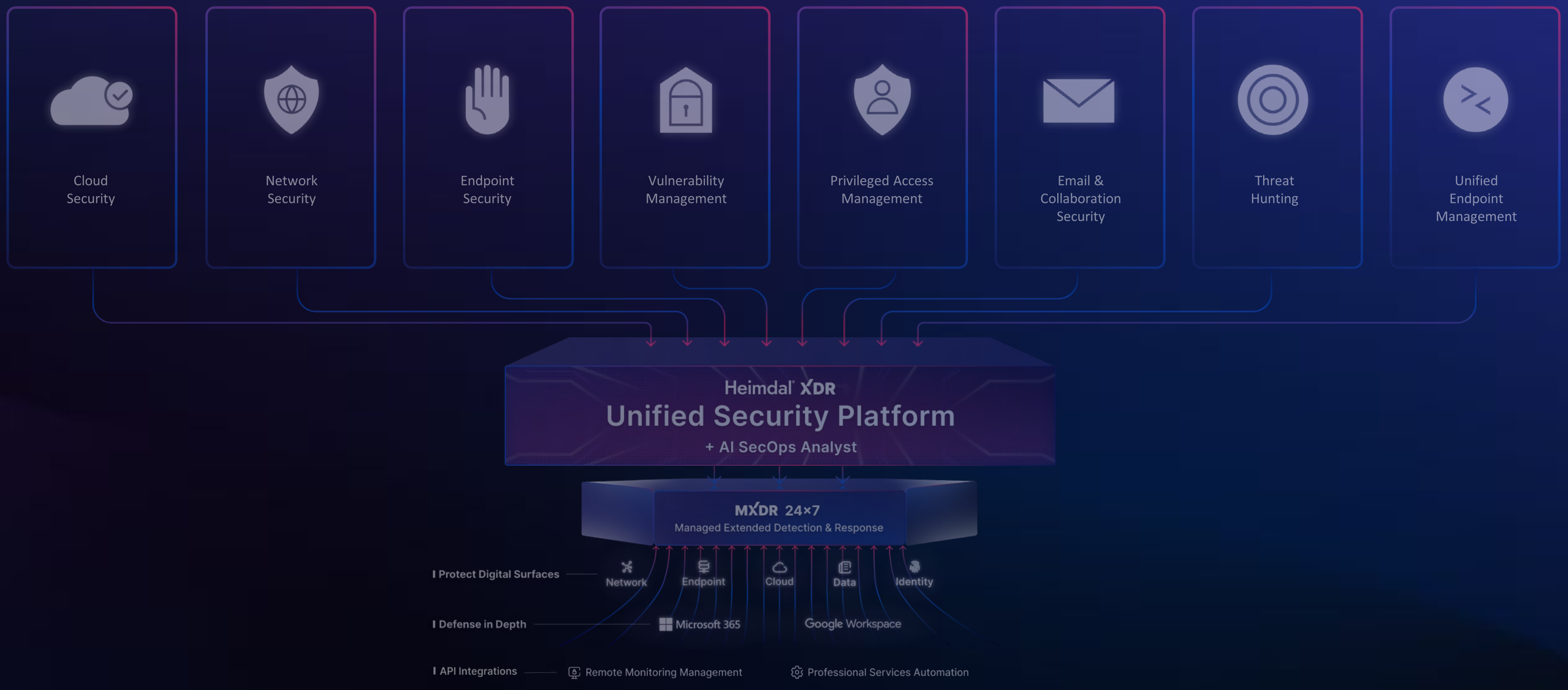
Gartner peerinsights ★★★★★ 4.8/5

Capterra ★★★★★ 4.8/5

Expert Insights ★★★★★ 4.8/5

99.7% Support Satisfaction

KEN HYGIENE SYSTEM · ÖSSUR LIFE WITHOUT LIMITATIONS · NRGi · VINCI ENERGIES · NHS · Lyf & heilsa · dpd · JYSK · Osborne Clarke



Heimdal®

Cyber Essentials and DORA – the easy way

Q: In what year was the
Cyber Essentials scheme launched?

A: 2014

Why, What, How, & When?

- Cyber Essentials (Plus)
- GDPR
- DORA – 35 controls
- SOC 2 type I & II
- NIS 2 – 57 controls
- ISO 27K – 114 controls

Compliance vs Threat focused actions

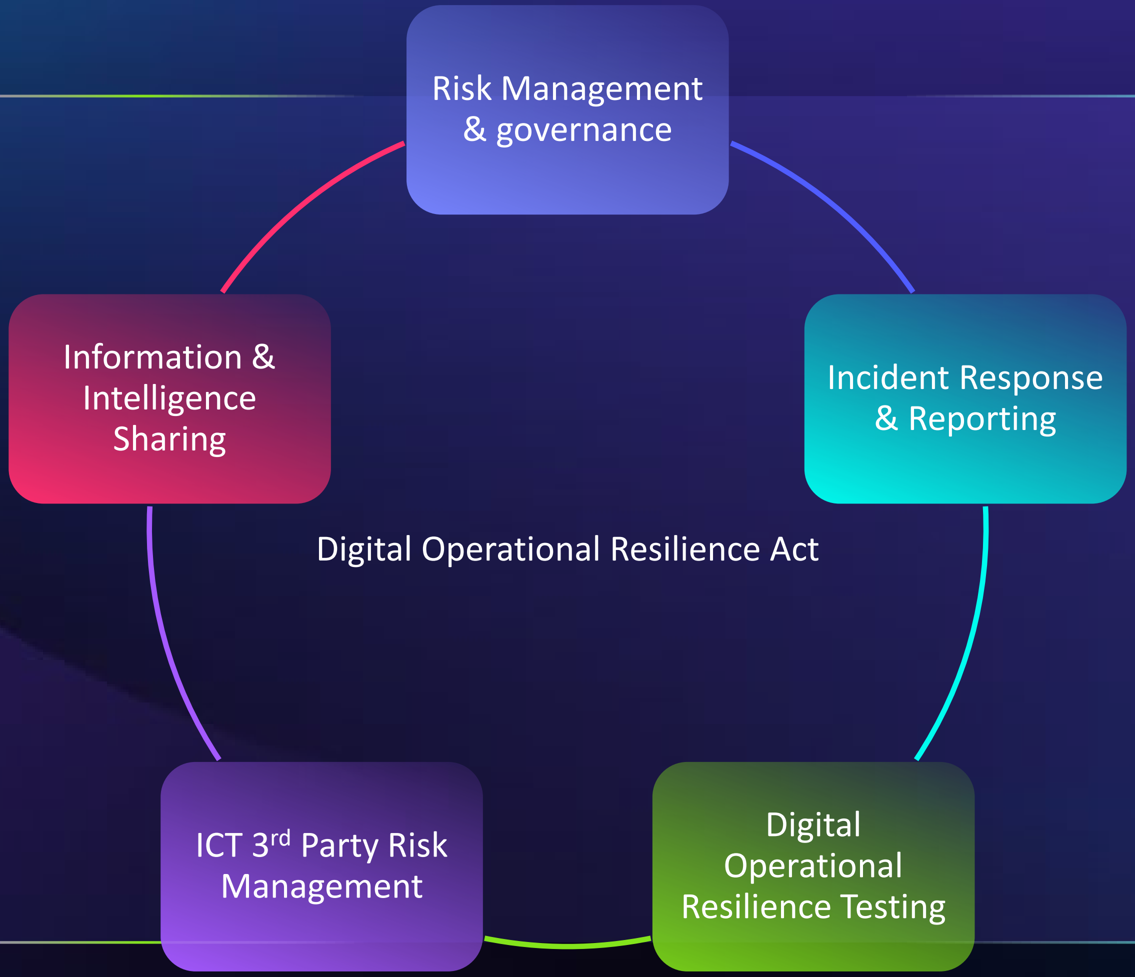
Security

- Continuous monitoring.
- Having the correct basic pillars.
- Focusing on threat based technical controls – not on generating proof.

Compliance

- Audit focused.
- Limitations based on the manhours.
- Repetitive cycles focused on compliance – not threat.

Cyber Essentials and DORA – the easy way


Risk Management & governance
Incident Response & Reporting
Digital Operational Resilience Testing
ICT 3rd Party Risk Management
Information & Intelligence Sharing
Digital Operational Resilience Act

The Five Pillars

1. Establish frameworks to manage ICT risks

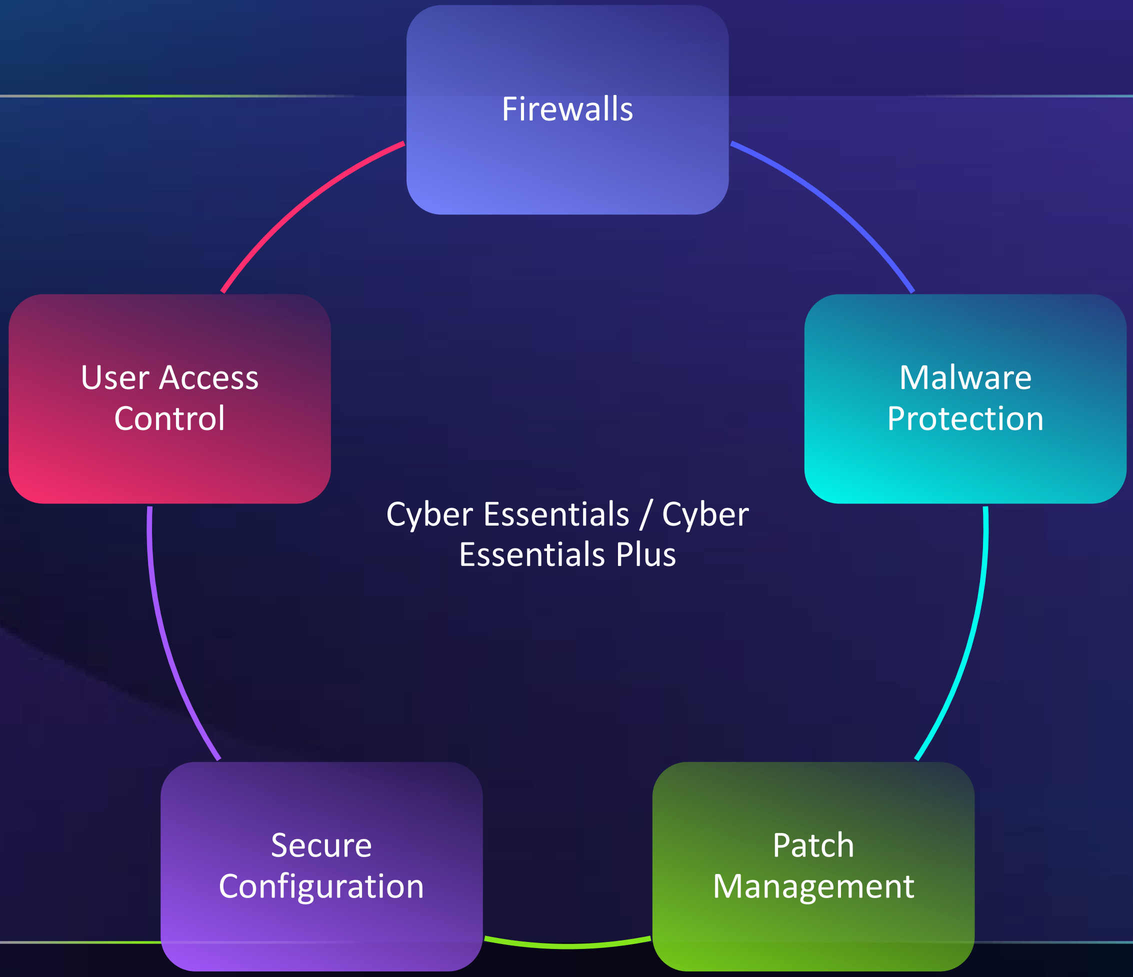
2. Implement procedures for detecting, managing and reporting ICT-related incidents

3. Conduct regular testing of operational resilience

4. Assess and manage risks related to third-party ICT vendors including an exit strategy in case of vendor failure

5. Collaborate and share information about cyber threats with other entities

Cyber Essentials and DORA – the easy way



The Five Pillars

1. Ensure firewalls are properly configured and restrict access to services only to those who need it

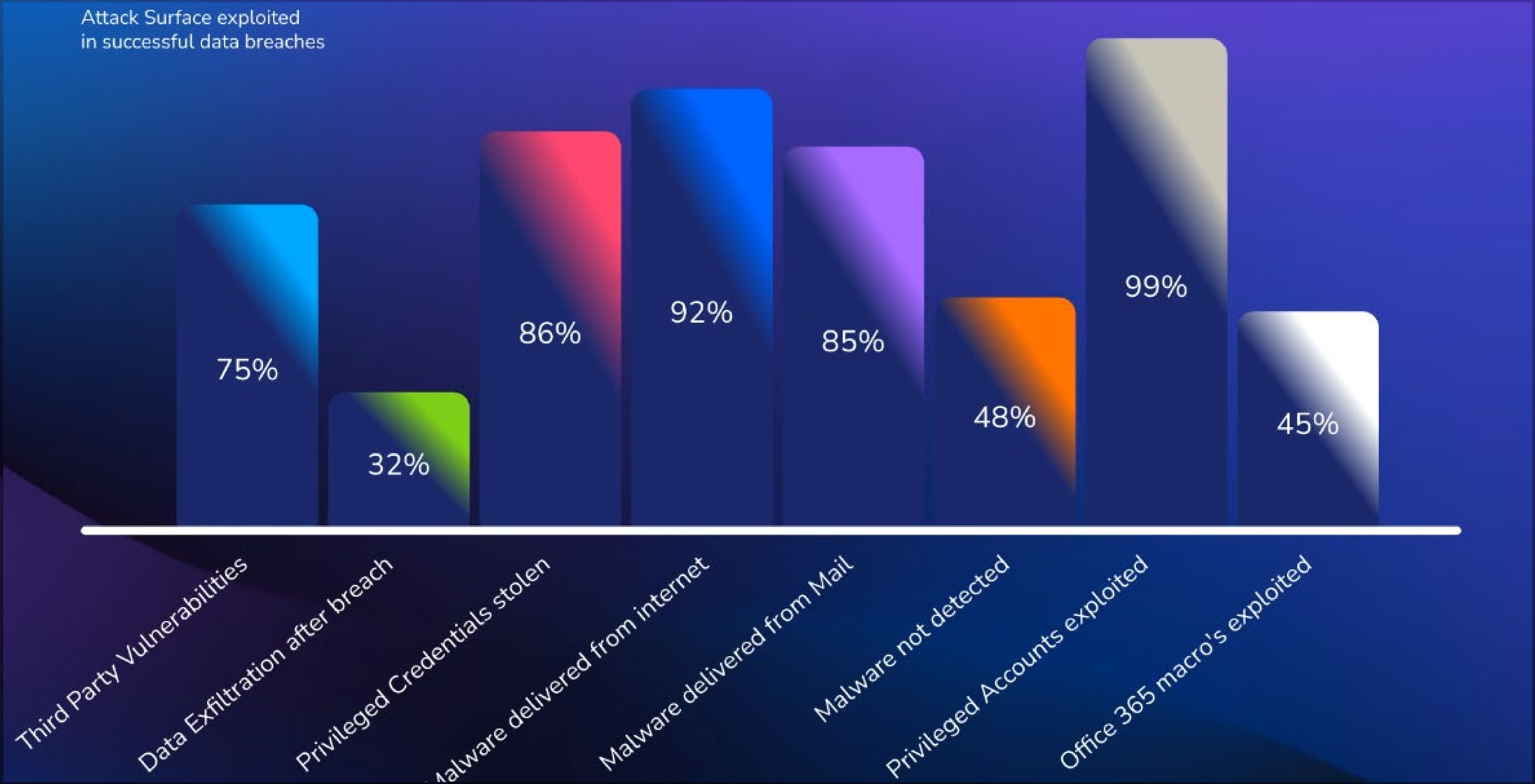
2. Employ anti-malware protection measures and ensure security software is updated regularly

3. Keep all software and operating systems up to date with the latest security patches

4. Ensure all devices and software are configured securely with security features enabled

5. Implement the principle of least privilege, regularly review and remove unnecessary accounts

Cyber Essentials and DORA – the easy way

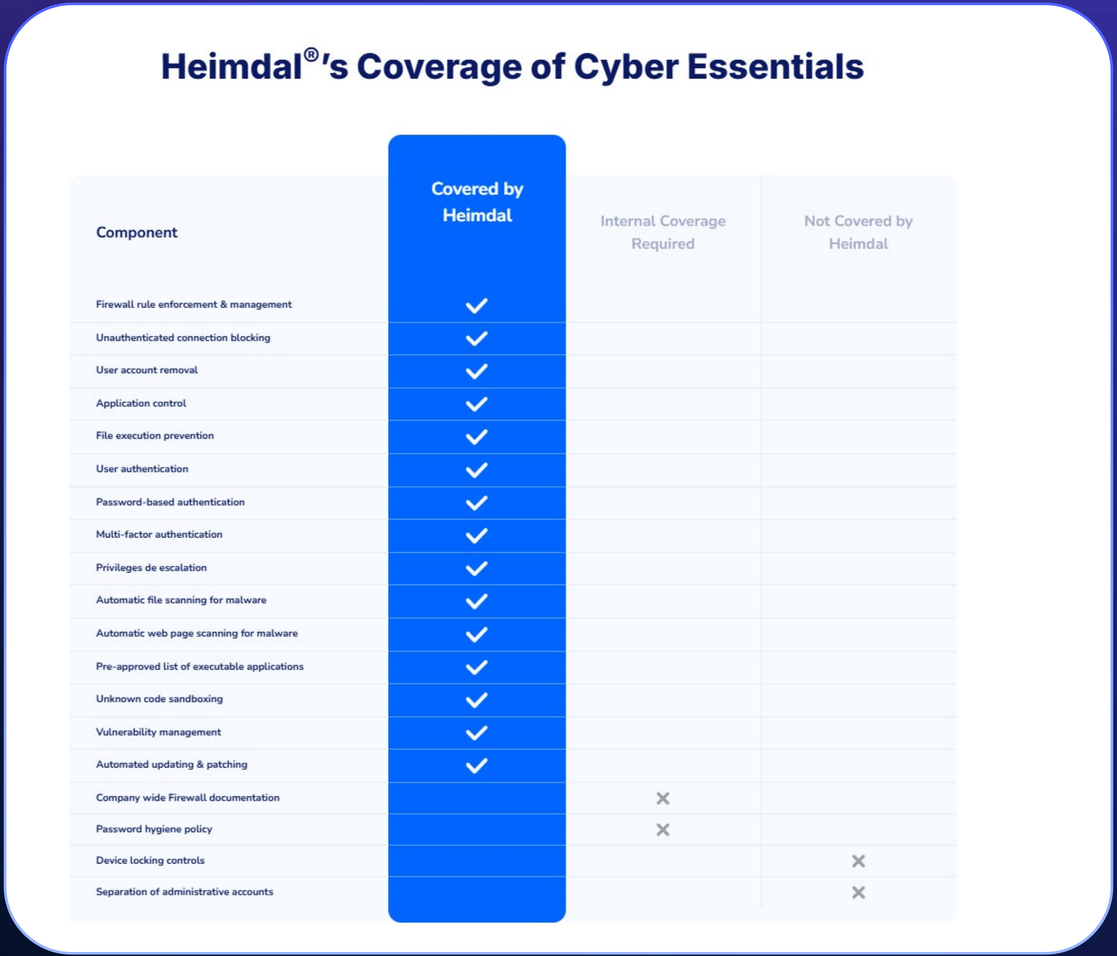


How Heimdal can help

Widest product stack in the industry – high level of coverage achieved with one Agent deployment

Unified XDR platform ensuring complete visibility and swift incident response

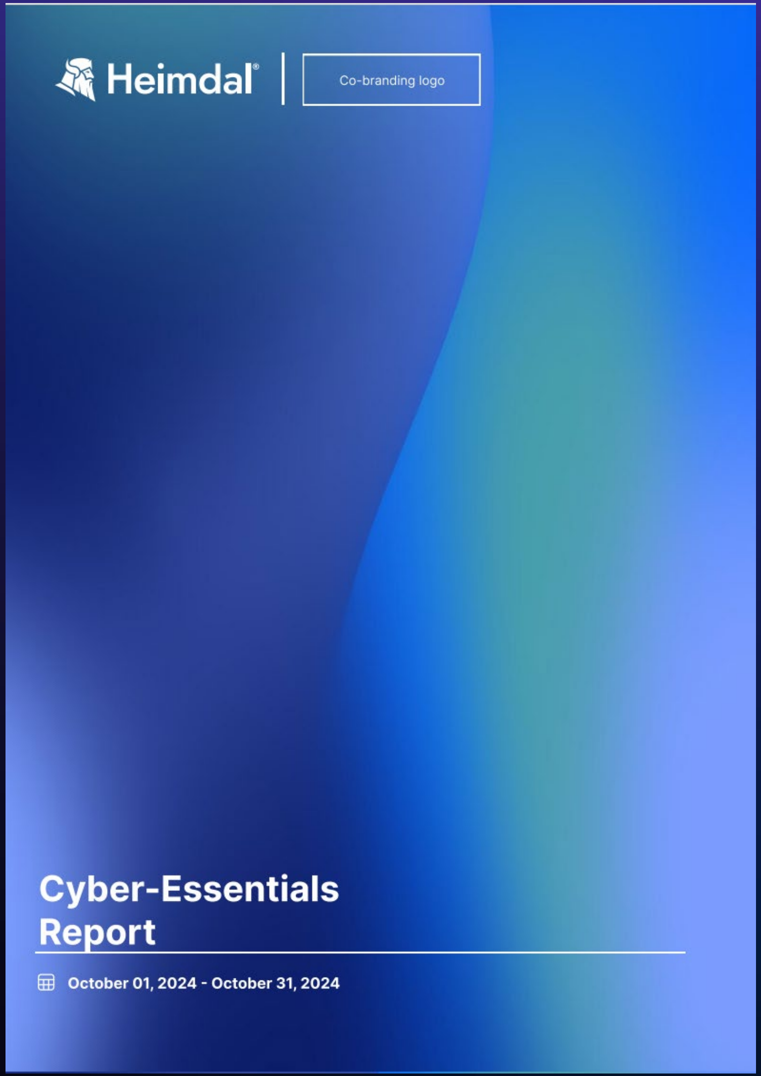
Option to have our managed SOC actively monitoring and responding to alerts



Heimdal®'s Coverage of Cyber Essentials

Component	Covered by Heimdal	Internal Coverage Required	Not Covered by Heimdal
Firewall rule enforcement & management	✓		
Unauthenticated connection blocking	✓		
User account removal	✓		
Application control	✓		
File execution prevention	✓		
User authentication	✓		
Password-based authentication	✓		
Multi-factor authentication	✓		
Privileges de escalation	✓		
Automatic file scanning for malware	✓		
Automatic web page scanning for malware	✓		
Pre-approved list of executable applications	✓		
Unknown code sandboxing	✓		
Vulnerability management	✓		
Automated updating & patching	✓		
Company wide Firewall documentation		✕	
Password hygiene policy		✕	
Device locking controls			✕
Separation of administrative accounts			✕

Automated CE Compliance Report



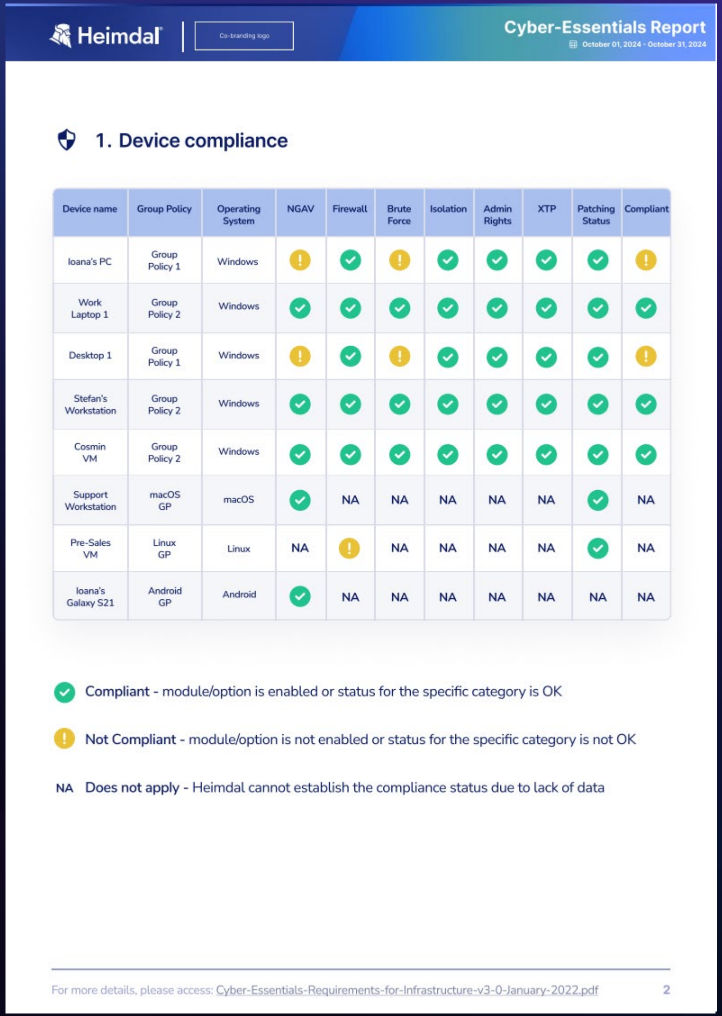
Co-branding logo

Cyber-Essentials Report

October 01, 2024 - October 31, 2024

Automated CE Compliance Report

Heimdal®



Heimdal | Co-branding logo

Cyber-Essentials Report
October 01, 2024 - October 31, 2024

1. Device compliance

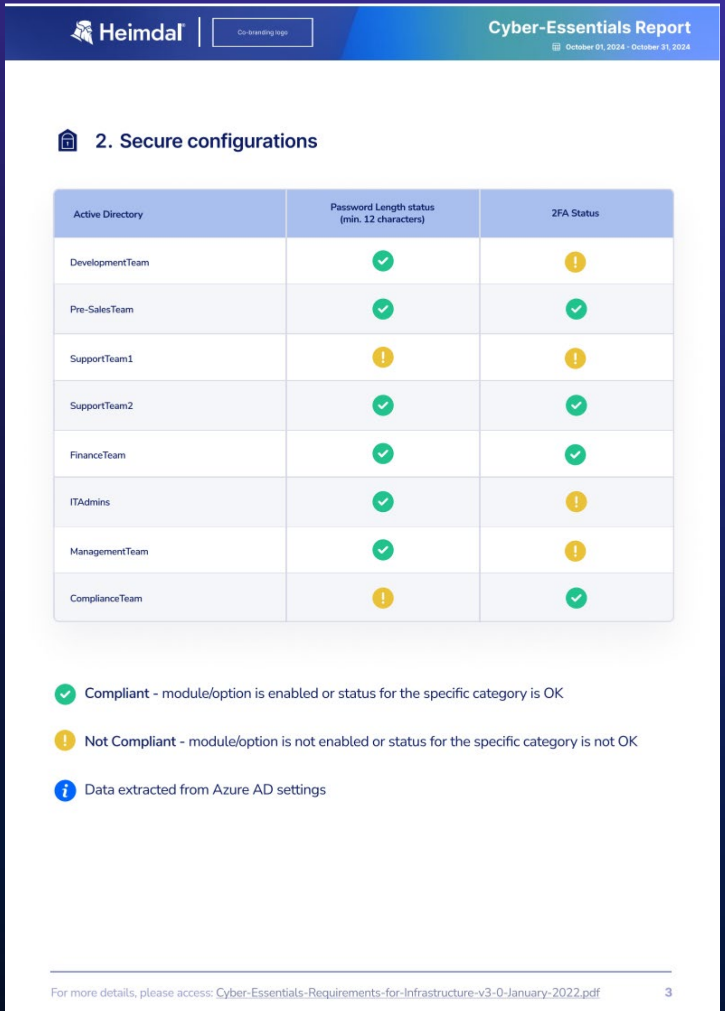
Device name	Group Policy	Operating System	NGAV	Firewall	Brute Force	Isolation	Admin Rights	XTP	Patching Status	Compliant
Ioana's PC	Group Policy 1	Windows	!	✓	!	✓	✓	✓	✓	!
Work Laptop 1	Group Policy 2	Windows	✓	✓	✓	✓	✓	✓	✓	✓
Desktop 1	Group Policy 1	Windows	!	✓	!	✓	✓	✓	✓	!
Stefan's Workstation	Group Policy 2	Windows	✓	✓	✓	✓	✓	✓	✓	✓
Cosmin VM	Group Policy 2	Windows	✓	✓	✓	✓	✓	✓	✓	✓
Support Workstation	macOS GP	macOS	✓	NA	NA	NA	NA	NA	✓	NA
Pre-Sales VM	Linux GP	Linux	NA	!	NA	NA	NA	NA	✓	NA
Ioana's Galaxy S21	Android GP	Android	✓	NA	NA	NA	NA	NA	NA	NA

✓ **Compliant** - module/option is enabled or status for the specific category is OK

! **Not Compliant** - module/option is not enabled or status for the specific category is not OK

NA **Does not apply** - Heimdal cannot establish the compliance status due to lack of data

For more details, please access: Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf 2



Heimdal | Co-branding logo

Cyber-Essentials Report
October 01, 2024 - October 31, 2024

2. Secure configurations

Active Directory	Password Length status (min. 12 characters)	2FA Status
DevelopmentTeam	✓	!
Pre-SalesTeam	✓	✓
SupportTeam1	!	!
SupportTeam2	✓	✓
FinanceTeam	✓	✓
ITAdmins	✓	!
ManagementTeam	✓	!
ComplianceTeam	!	✓

✓ **Compliant** - module/option is enabled or status for the specific category is OK

! **Not Compliant** - module/option is not enabled or status for the specific category is not OK

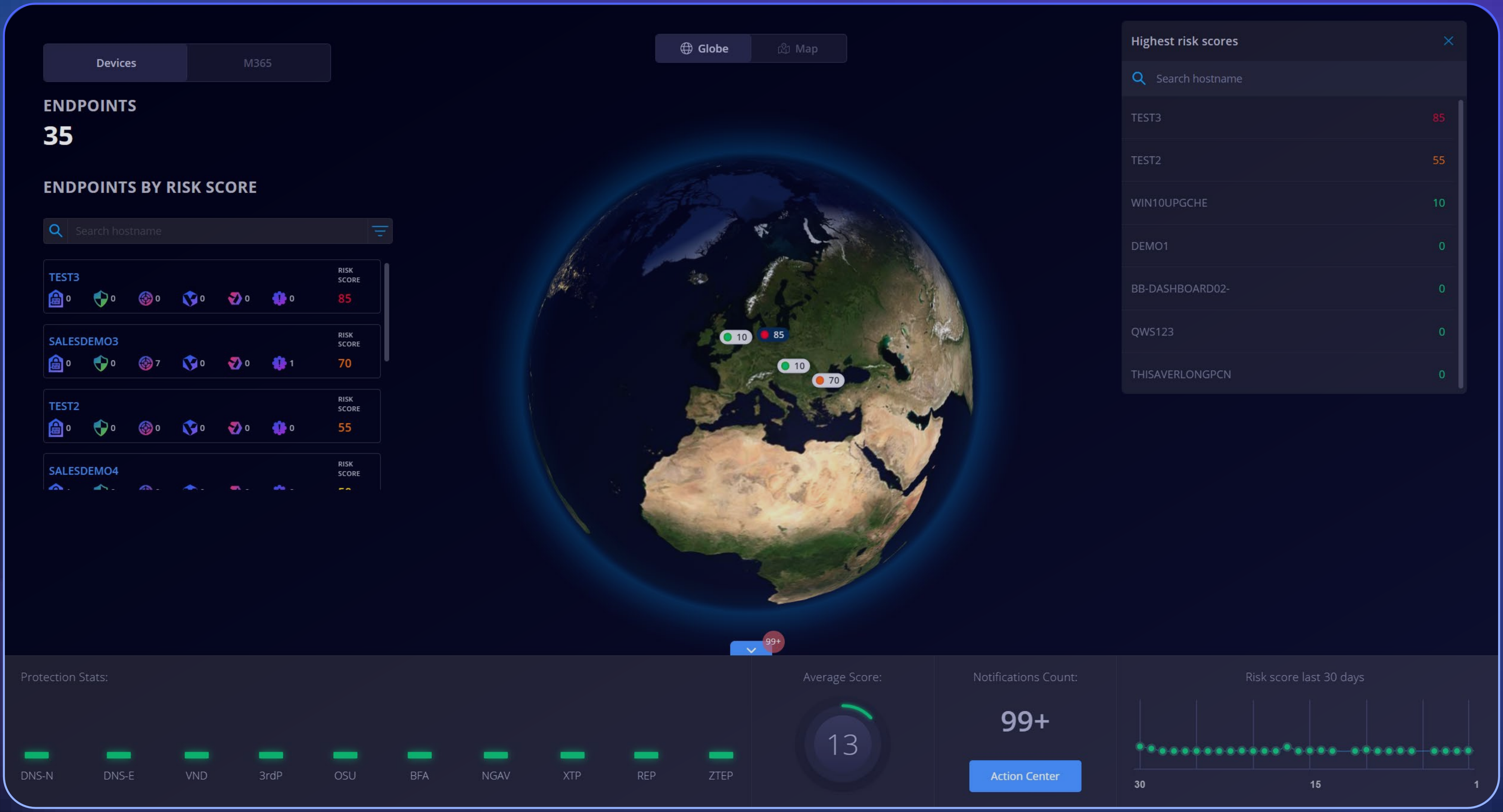
ℹ Data extracted from Azure AD settings

For more details, please access: Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf 3

Q: What is the name of the product Heimdal released in 2023 – our fully integrated SIEM and XDR solution?

A: The Threat-hunting and Action Centre

Threat-hunting & Action Centre security and compliance at a glance



ENDPOINTS

35

ENDPOINTS BY RISK SCORE

Search hostname

TEST3 — 0 0 0 0 0 0 — RISK SCORE 85

SALESDEMO3 — 0 0 7 0 0 1 — RISK SCORE 70

TEST2 — 0 0 0 0 0 0 — RISK SCORE 55

SALESDEMO4 — RISK SCORE

Highest risk scores

Search hostname

TEST3	85
TEST2	55
WIN10UPGCHE	10
DEMO1	0
BB-DASHBOARD02-	0
QWS123	0
THISAVERLONGPCN	0

Protection Stats:

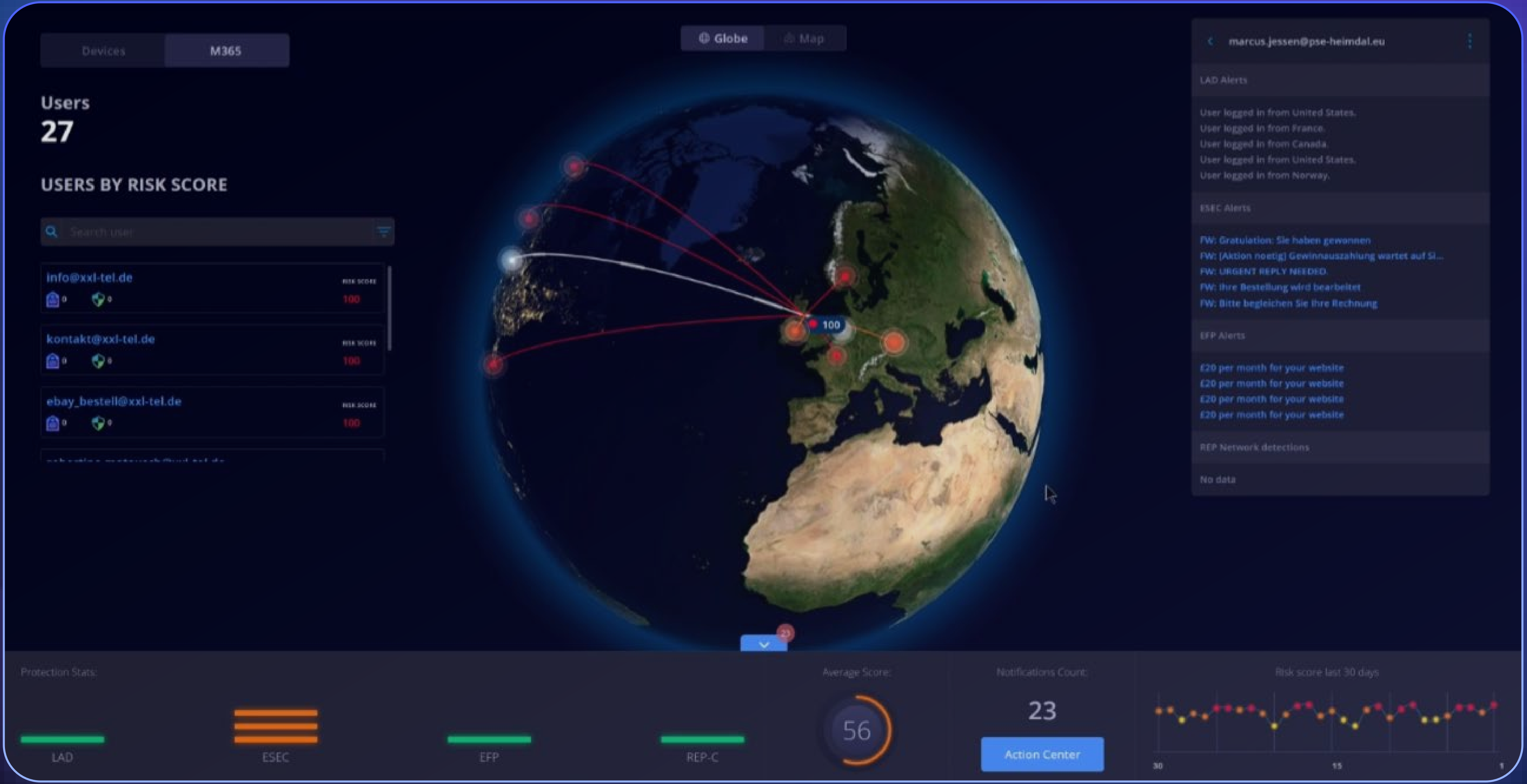
Average Score: 13

Notifications Count: 99+

Action Center

Risk score last 30 days

Threat-hunting & Action Centre security and compliance at a glance



Users
27

USERS BY RISK SCORE

Search user

info@xxl-tel.de 0 0 RISK SCORE 100

kontakt@xxl-tel.de 0 0 RISK SCORE 100

ebay_bestell@xxl-tel.de 0 0 RISK SCORE 100

marcus.jessen@pse-heimdal.eu

LAD Alerts

User logged in from United States.
User logged in from France.
User logged in from Canada.
User logged in from United States.
User logged in from Norway.

ESEC Alerts

FW: Gratulation: Sie haben gewonnen
FW: [Aktion noetig] Gewinnauszahlung wartet auf Si...
FW: URGENT REPLY NEEDED.
FW: Ihre Bestellung wird bearbeitet
FW: Bitte begleichen Sie Ihre Rechnung

EFP Alerts

£20 per month for your website
£20 per month for your website
£20 per month for your website
£20 per month for your website

REP Network detections

No data

Protection Stats: LAD, ESEC, EFP, REP-C

Average Score: 56

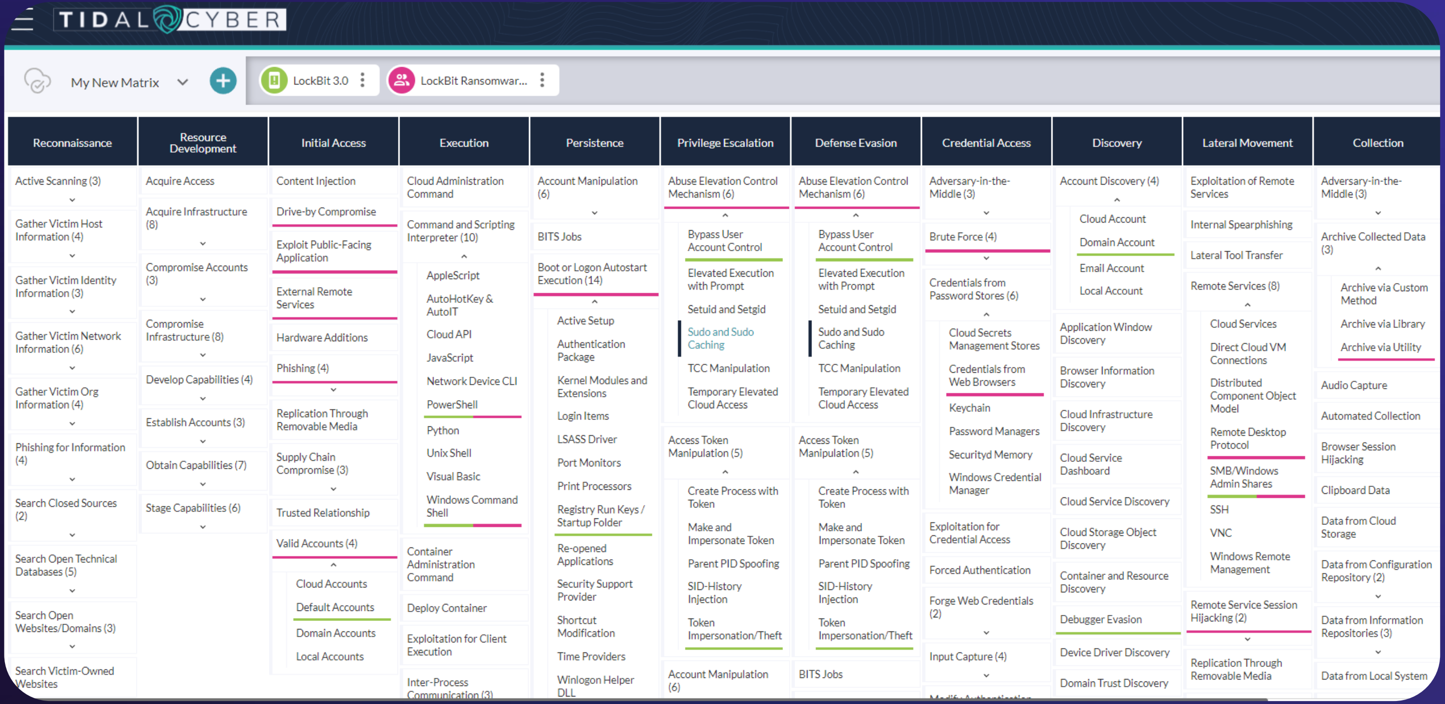
Notifications Count: 23

2 minute tip

https://app.tidalcyber.com/

Use the tidal cyber to map your Products to all known TTP.

You can put in types of ransomware, ransomware groups and then map you vendors to see any gaps in your telemetry, detection and remediation capabilities



Reconnaissance
- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (4)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
- Acquire Access
- Acquire Infrastructure (8)
- Compromise Accounts (3)
- Compromise Infrastructure (8)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (7)
- Stage Capabilities (6)

Initial Access
- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (4)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

Execution
- Cloud Administration Command
- Command and Scripting Interpreter (10)
  - AppleScript
  - AutoHotKey & AutoIT
  - Cloud API
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)

Persistence
- Account Manipulation (6)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
  - Active Setup
  - Authentication Package
  - Kernel Modules and Extensions
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Registry Run Keys / Startup Folder
  - Re-opened Applications
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL

Privilege Escalation
- Abuse Elevation Control Mechanism (6)
  - Bypass User Account Control
  - Elevated Execution with Prompt
  - Setuid and Setgid
  - Sudo and Sudo Caching
  - TCC Manipulation
  - Temporary Elevated Cloud Access
- Access Token Manipulation (5)
  - Create Process with Token
  - Make and Impersonate Token
  - Parent PID Spoofing
  - SID-History Injection
  - Token Impersonation/Theft
- Account Manipulation (6)

Defense Evasion
- Abuse Elevation Control Mechanism (6)
  - Bypass User Account Control
  - Elevated Execution with Prompt
  - Setuid and Setgid
  - Sudo and Sudo Caching
  - TCC Manipulation
  - Temporary Elevated Cloud Access
- Access Token Manipulation (5)
  - Create Process with Token
  - Make and Impersonate Token
  - Parent PID Spoofing
  - SID-History Injection
  - Token Impersonation/Theft
- BITS Jobs

Credential Access
- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (6)
  - Cloud Secrets Management Stores
  - Credentials from Web Browsers
  - Keychain
  - Password Managers
  - Securityd Memory
  - Windows Credential Manager
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)

Discovery
- Account Discovery (4)
  - Cloud Account
  - Domain Account
  - Email Account
  - Local Account
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery

Lateral Movement
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Services (8)
  - Cloud Services
  - Direct Cloud VM Connections
  - Distributed Component Object Model
  - Remote Desktop Protocol
  - SMB/Windows Admin Shares
  - SSH
  - VNC
  - Windows Remote Management
- Remote Service Session Hijacking (2)
- Replication Through Removable Media

Collection
- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
  - Archive via Custom Method
  - Archive via Library
  - Archive via Utility
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System

Maturity Framework

Heimdal®

		Level 1 Chaos	Level 2 Progressing	Level 3 Driving Processes	Level 4 Maturity	Level 5 Excellence
Process	**Usage**	Configuring tools without a documented strategy - Patch & Asset Management - DNS Security	Basic controls deployed - Patch & Asset Management - DNS Security	Commitment to driving processes - Patch & Asset Management - DNS Security - Privilege Elevation & Delegation Management	Tuned deployment strategy for prop - Patch & Asset Management - DNS Security - PEDM - Application Control - Next-Gen Anti-Virus, - PASM - Threat-hunting & Action Center	Pro-active cybersecurity plans using Heimdal XDR
	Controls	Telemetry: 75 Detection: 50 Remediation 50	Telemetry: 100 Detection: 75 Remediation 75	Telemetry: 100 Detection: 85 Remediation 80	Telemetry: 100 Detection: 100 Remediation 95	Telemetry: 100 Detection: 100 Remediation 98
	Staff Education	★☆☆☆☆	★★☆☆☆	★★★☆☆	★★★★☆	★★★★★
	Certification	None	None	Cyber Essentials Cyber Insurance	CIS 18, ISO27001, CE+	CIS 18, NIST ISO27001, ISO27002 SOC2+
Metrics	**Endpoint Coverage (% of Total)**	0-60%	61-70%	71-85%	86-94%	>95%
	Mean time to Investigate (Time)	>45 days	31-45 days	15-30 days	8-14 days	0-7 days
	Mean time to Remediate	>45 days	31-45 days	15-30 days	8-14 days	0-7 days

Heimdal®

Clelia Di Maio

MSP Customer Success Manager, Heimdal

Book a meeting