Privacy Data Sheet for Heimdal
Threat-Hunting and Action Center

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the Heimdal Threat-Hunting and Action Center (TAC). It provides detailed information about the types of data collected, how and where it is processed, and the measures in place to ensure compliance with global privacy regulations. This document serves as a resource for customers to understand the data handling practices of Heimdal Security, ensuring transparency and trust in our commitment to data privacy.

1. Product Summary

Heimdal Threat-Hunting and Action Center (TAC) is a centralized platform designed to detect, analyze, and respond to cybersecurity threats in real-time. The TAC aggregates data from various Heimdal products, providing a unified view of security events and enabling proactive threat hunting and rapid response. By integrating threat intelligence and automated workflows, Heimdal TAC enhances your organization's ability to protect against sophisticated cyber threats and maintain a secure IT environment.

2. Heimdal Threat-Hunting and Action Center – data processing

a. Threat-Hunting and Action Center – data processed

Type of data	Example(s)	Purpose of processing
Hostname	CUSTOMER-PC	To identify the endpoint; User for alert management
File path	c:\users\user\desktop\detections\ \ pe_lab_irc.exe	To identify and manage file- restore, add to allowlist, approve elevation request, add AppControl rules, etc
Available OS Updates	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602	To identify available updates for the endpoint;
Application version	5.1.2.2	To identify specific application versions with vulnerabilities
Application name	Libre Office	To identify specific application with vulnerabilities
IP	180.120.12.45	Identify the source of a brute force attack

b. Threat-Hunting and Action Center – data flow

Heimdal Threat-Hunting and Action Center (TAC) processes various types of data depending on the specific products integrated within the TAC. The data processing involves a comprehensive analysis of security events and activities across the connected systems to detect and respond to threats proactively.

- **Event Data:** The system processes data related to security events, including logs, alerts, and incident reports from integrated Heimdal products. This includes detailed information on potential threats, user activities, and system responses.

- **Threat Intelligence Data:** TAC continuously processes threat intelligence feeds, which include Indicators of Compromise (IoCs) such as malicious IP addresses, domains, and file hashes. This data is critical for identifying and responding to emerging threats.

- **User Activity Data:** Data related to user activities, including login attempts, access to sensitive data, and system changes, is processed to detect unusual behavior that may indicate a security threat.

- **System Configuration Data:** The system processes configuration data from connected endpoints to monitor and manage security settings, ensuring compliance with security policies and enabling automated responses to threats.

- **Incident Response Data:** Data related to incident response actions taken within the TAC, such as quarantine measures, threat neutralization, and system restoration, is processed to ensure comprehensive documentation and auditability.

The specific data types processed within TAC are dependent on the Heimdal products integrated into the Threat-Hunting and Action Center. For detailed information on data processing practices related to individual products, please refer to the specific product data privacy sheets.

All personal data processed within TAC is handled in compliance with applicable privacy laws, ensuring that data is secured, anonymized where possible, and retained only as long as necessary to fulfill its security purposes.

3. Processing Locations

For our Threat-Hunting and Action Center, we offer the following data storage options on Microsoft Azure, allowing customers to choose the location that best suits their regulatory and operational needs:

- **Azure Europe (Netherlands/Amsterdam):** This location is ideal for customers within the European Union who require compliance with GDPR and prefer to maintain their data within the European Economic Area. By choosing this option, customers can ensure their data is stored in accordance with strict EU data protection laws, meeting all necessary data sovereignty requirements.

- **Azure UK (UK/London):** This option offers a dedicated solution for UK-based customers, ensuring that data is stored within the UK. This ensures compliance with local data protection regulations, particularly post-Brexit, and guarantees that data sovereignty is maintained according to UK-specific legal standards.

- **Azure US (US/Virginia):** This storage option is tailored for customers in the United States, providing a solution that aligns with U.S. compliance requirements, including those under HIPAA and other federal and state-specific regulations.

Additionally, it ensures optimal data access speeds and performance for users within the North American region.

If a customer does not specify a preference, by default, data is stored within the European Union, thereby aligning with stringent EU data protection standards.

4. Compliance with Privacy Regulations

Heimdal Security is deeply committed to maintaining compliance with global privacy regulations and upholding the highest standards of data protection. Our solutions are designed and operated in compliance with several key privacy laws and standards, including:

- **GDPR (General Data Protection Regulation):** Heimdal Security adheres to all GDPR requirements, ensuring that personal data is processed lawfully, fairly, and transparently. We have implemented robust measures to protect the privacy rights of individuals within the European Union.

- **UK Data Protection Act 2018:** In the UK, we comply with the Data Protection Act, which complements the GDPR post-Brexit and includes provisions specific to the UK.

- **US Privacy Regulations:** Heimdal Security complies with relevant US privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data protection and other state-specific regulations as applicable.

- **NIS2 Directive:** We align with the Network and Information Security (NIS2) Directive, which sets out the legal measures to boost the overall level of cybersecurity in the EU, particularly concerning critical infrastructure and essential services.

- **ISAE 3000 SOC 2 Certification:** Heimdal Security is certified under ISAE 3000 SOC 2, a widely recognized standard for managing customer data based on five trust service principles: security, availability, processing integrity, confidentiality, and privacy. This certification underscores our commitment to maintaining a secure environment for our customers' data.

5. Storage Period

For the Threat-Hunting and Action Center data is retained for a period of **2 years**. This duration is necessary to ensure effective threat detection and response, as well as to comply with relevant legal and regulatory requirements. After this period, the data is securely deleted from our systems unless longer retention is required by law or necessary for legitimate business purposes.