SERVICES INCLUDED

Data Collection

- **Log Data:** Skadi will collect logs from various sources such as operating systems, applications, network devices, and security appliances for the purposes of detecting and preventing cyber threat. Skadi maintains 90 days of log data in varied data tiers.
- **Network Traffic Analysis:** Skadi captures and analyzes network traffic to identify patterns, anomalies, and potential security threats. This can include monitoring for unusual communication patterns or unauthorized access attempts.
- **Endpoint Data:** Skadi gathers information from individual devices (endpoints) such as computers, servers, and mobile devices. This may include data on installed software, user activity, and system events. No PII is collected and maintained.

Data Analysis

- **Behavioral Analysis:** Skadi will utilize machine learning, AI and statistical analysis to establish baseline behavior for users and systems in order to detect deviations from these baselines which can indicate potential security incidents.
- **Behavioral Analysis:** Skadi will use commercially reasonable efforts to identify unusual patterns or activities, such as unexpected spikes in network traffic, irregular user behavior, or abnormal system, that may indicate a security threat.

Visibility

- **Behavioral Analysis:** Skadi will utilize machine learning, AI, and statistical analysis to establish baseline behavior for users and systems in order to detect deviations from these baselines which can indicate potential security incidents.

24/7 Alerting and Monitoring

- **Real-time Alerts:** Skadi's alerting system identifies specific events or patterns that may indicate a security incident and sends alerts to Skadi's security teams in real-time.
- **Continuous Monitoring:** Skadi utilizes a continuous monitoring process to ensure that Skadi's security teams are aware of changes and events as they happen. This helps in early detection and response to security incidents.

Incident Response

- **Incident Triage:** Skadi assesses the severity and scope of a security incident to determine the appropriate response in near-real time. This involves categorizing and prioritizing incidents based on their potential impact on your organization.
- **Forensic Analysis:** If an incident occurs, Skadi performs in-depth forensic analysis to understand the root cause of a security incident, trace the attacker's activities, and gather evidence for remediation.

Automation

- **Automated Response:** Skadi has implemented automated responses to certain types of security incidents. For example, automatically blocking IP addresses associated with malicious activities or isolating compromised systems from the network.
- **Workflow Automation:** Skadi streamlines incident response workflows through automation to improve efficiency and reduce the time it takes to mitigate security threats.

Dark/Deep Web Monitoring

- Skadi proactively and regularly monitors and analyzes the deep and dark web for Client information, which may indicate a security issue, and for other breaches that impact Client.

Penetration Testing

- **Pen Testing Services:** Periodically, Skadi conducts penetration tests to identify and address vulnerabilities by simulating real-world attacks. This helps Skadi understand Client's security posture from an external perspective. Client acknowledges and agrees that Skadi will perform these tests randomly and without prior Client consent in order to maintain test integrity.

Endpoint Protection

- **Anti-virus and Anti-Malware:** Skadi will deploy endpoint tools that detect and remove malicious software on individual devices, providing an additional layer of defense against malware and other threats.

Threat Intelligence

- **Threat Feeds:** Skadi will correlate Client activity to threat intelligence feeds which provide up-to-date information on known malicious actors, indicators of compromise (IoCs), and emerging threats.

Vulnerability Management

- **Vulnerability Scanning:** Skadi conducts regular scans of Client's assets to identify and assess vulnerabilities in software, systems, and networks, and reports the results to the Client for the Client's remediation.

SKADI CYBER DEFENSE
UNYIELDING.
UNCEASING.
UNMATCHED.