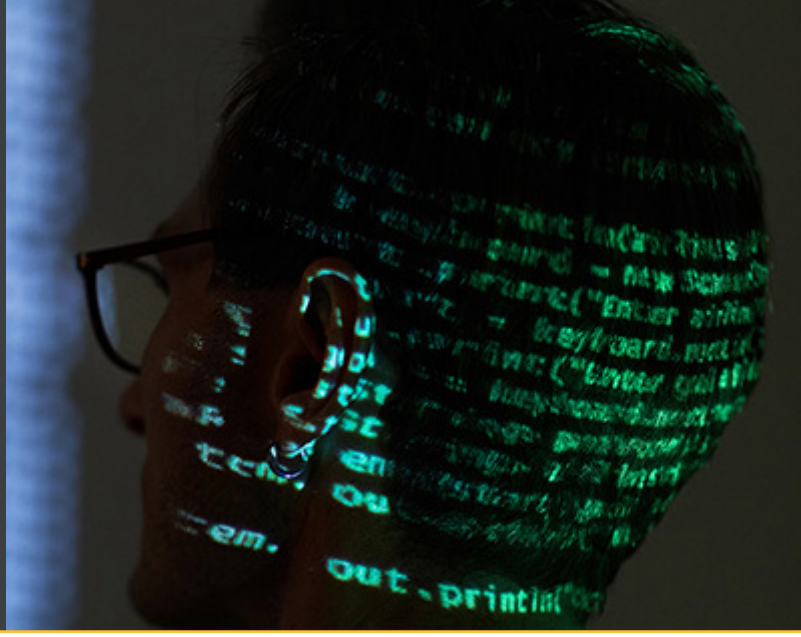
KI-gestützte Network Detection and Response Systeme von Muninn ApS, Kopenhagen



Systemansatz – Cyberangriffe in real-time über Anomalieerkennung abwehren

Die Network Detection und Response Systeme (NDR) von Muninn überwachen das Datenaufkommen in sensitiven IT- und OT-Netzwerken mit künstlicher Intelligenz auf Anomalien; schädliche Prozesse werden in real-time 24/7 blockiert.

Auch bisher nicht erkannte oder durch Insider ausgeführte Angriffe sowie in Netzwerken latent vorhandene Schadsoftware werden erfasst.

Um mit der erforderlichen Schnelligkeit auf Bedrohungen reagieren zu können, setzt Muninn zwei KI-Engines für maschinelles Lernen ein, die Datenaufkommen auf full-package-capture-Basis mit mehr als 120 Parametern überwachen. Bekannte Skripte von Schadsoftware werden berücksichtigt.

Die Systeme von Muninn lassen sich in alle gängigen Netzwerkinfrastrukturen und SIEM-Lösungen integrieren.

Muninn konfiguriert die Product Suite als reine on-premise-Lösung, als in-house-cloud oder beispielsweise in Anbindung an die MS365-Azure-Welt.

Die KI ist dabei auf den Sensoren installiert und muss nicht auf externe Rechenkapazitäten zurückgreifen.

Die Systeme sind GDPR-konform und erfüllen die Anforderungen der NIS2- Richtlinie der EU für KRITIS-Unternehmen.

- Muninn AI Detect erfasst clientless alle Datenquellen in einem Netzwerk und überwacht deren Interaktion auf Anomalien.
- Muninn AI Prevent blockiert in real-time schädliche Prozesse wie unerwünschte Verschlüsselungen.
- Muninn AI Endpoint ermöglicht forensische Untersuchungen auf Endgeräten.

Geschäftsfokus – Gewährleistung dauerhaft höchster Sicherheitsstandards

Muninn gilt als eines der führenden europäischen Unternehmen zur Erkennung und Schließung von Datenlecks und zur Identifizierung von in Netzwerken bereits vorhandenen unerkannten Bedrohungen (Advanced Persistent Threats).

Das Unternehmen ist aus Projekten dänischer Sicherheitsdienste zum Schutz kritischer Infrastrukturen mit dem Ziel hervorgegangen, die besonderen Technologien, wie sie in staatlichen Hochsicherheitsbereichen Anwendung finden, auch der Privatwirtschaft zugänglich zu machen.

Die Systeme von Muninn entsprechen höchsten militärischen und zivilen staatlichen Sicherheitsstandards. Sie sichern Organisationen mit besonderen Sicherheitsanforderungen, wie z.B. das gesamte dänische staatliche Gesundheitswesen, Ministerien, Versorgungsbetriebe, Krankenhäuser und größere Industrieunternehmen ab.

Der Prozess der kontinuierlichen technologischen Weiterentwicklung zum nachhaltigen Schutz der Kundennetzwerke ist Teil der DNA von Muninn; enge Kundenbeziehungen und technologische Schlagkraft sind Voraussetzungen hierfür.

Im Technologievergleich: Breites Analysespektrum und real-time Gegenmaßnahmen

Die Muninn NDR-Systeme sind wesentlich effektiver als herkömmliche Cyber-Security-Ansätze, wie beispielsweise Firewalls:

- **Erkenntnisse** – Neben bekannten Bedrohungsskripten erkennt Muninn auch bisher unbekannte Angriffsprofile sowie Angriffe von Unternehmensinsidern, die hinter Firewalls stattfinden.
- **Reaktionsgeschwindigkeit** – Der Einsatz von KI ermöglicht ein Erkennen und Blockieren schädlicher Prozesse in real-time rund um die Uhr.
- **Umfang von Analysen** – Netzwerke werden auf „full-package-capture"-Basis analysiert.
- **Reaktionen** – Bei erkannten Bedrohungen werden verzugslos vorab definierte Gegenmaßnahmen ergriffen.
- **Anpassungsfähigkeit** – Im Vergleich zu herkömmlichen SIEM -Konzepten müssen bei Muninn Entscheidungsregeln nicht manuell hinterlegt und laufend angepasst werden; die Systeme aktualisieren sich über maschinelles Lernen selbst.
- **Transparenz** – Die Einstufung von Anomalien in Risikoklassen und die daraus abzuleitenden Reaktionen sind transparent.

Im direkten Wettbewerbsvergleich: Hohe Sensitivität bei geringer Anzahl von False Positives

Die Muninn Product Suite ist eine europäische Anwendung. In dezidierten Test- und Auswahlverfahren staatlicher und privater Stellen wurden einige Eigenschaften besonders hervorgehoben:

- **Transparenz** – Alle in einem Netzwerk vorhandenen Geräte werden mit Interaktionen und Protokollen aufgezeigt.
- **Sensitivität** – Mit KI-basierten Alarmen werden über längere Zeiträume vorangetriebene Angriffe in einer chain-of-event-Betrachtung präzise erfasst.
- **Qualität der Analysen** - Die angewandten Algorithmen führen zu einer niedrigen Anzahl von False Positives.
- **Spektrum der Analysen** – Die Betrachtung von mehr als 120 Parametern (treat modells) gestattet einen tiefen Einblick in Netzwerke.
- **Geschwindigkeit** – Die Schnelligkeit der Analysen ermöglicht Gegenmaßnahmen in real-time.

Die Einführung und Installation der Muninn Product Suite ist organisatorisch und technisch unkompliziert:

- Die Installation ist technisch simpel, der Einführungs-prozess strukturiert und damit kalkulierbar.
- Aufgrund des intuitiven Aufbaus der Dashboards und der Datenbank zur Interpretation von Alarmen sind Ausbildungserfordernisse vergleichsweise gering.
- Nach einer Lernphase von wenigen Wochen liefern die Systeme bereits Ergebnisse; die volle Einsatzfähigkeit ist nach ca. 3 Monaten erreicht.
- Eine aufwendige und fehleranfällige Eingabe von Regeln entfällt.

Effektivität und Effizienz der Systeme zeigen sich im Betrieb:

- Die Aussagekraft der Systeme ist hoch – Anwender erhalten strukturierte Analyseergebnisse anstelle manuell auszuwertender Loglisten.
- Der Einsatz der Muninn Product Suite wirkt sich nicht auf die Geschwindigkeit von Netzwerken aus.
- Die Systeme sind transparent und logisch aufgebaut; eventuelle Adjustierungen sind unkompliziert möglich.
- Die Produkte von Muninn sind preislich attraktiv positioniert und auf Großprojekte ausgelegt.

Im Ergebnis entscheiden sich Kunden für eine Integration der Muninn-Produte in Systemlandschaften wie auch beispielsweise von Palo Alto Networks.

Adaptionsfähigkeit – Auch besondere technologische Anforderungen werden erfüllt

Aufgrund seiner Größe und des starken Engineering-Fokus ist Muninn organisatorisch und technisch in der Lage, die NDR-Systeme an besondere Kundenerfordernisse anzupassen.

Folgende beispielhafte Individuallösungen wurden bereits entwickelt:

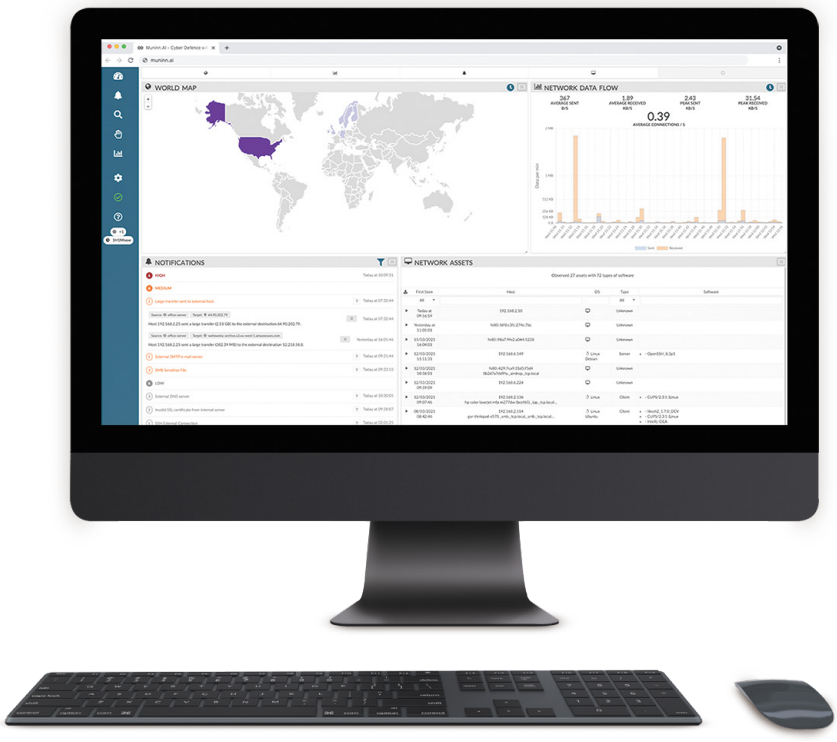
- Zentrale Steuerung und Überwachung mehrerer unabhängiger Netzwerke ohne Aufbau von Cloud-Strukturen.
- Absicherung von internationalen Niederlassungen über private inhouse-Cloudlösungen
- Absicherung von OT-Netzwerken bei mikro-segmentierter Netzwerkstruktur
- Schutz von Netzwerken mit bis zu 650.000 Endgeräten

Kennenlernen – Unkomplizierter Proof-of-Concept-Prozess

Soweit Absprachen zur Vertraulichkeit es zulassen, vermittelt Muninn geeignete Ansprechpartner als Referent zu besonderen Fragestellungen.

Regional Partner stehen bereit, um die Arbeitsweise der Systeme zu demonstrieren.

Bei Interesse werden POCs in den von Interessenten gewünschten Netzwerkumgebungen ermöglicht. Dabei erstellt Muninn Product Suite bereits eine Übersicht über aktuelle Schwachstellen in der IT-/OT-Landschaft, bewertet Risiken und macht konkrete Vorschläge zu deren Beseitigung.



muninn.ai