3KV
a member of HPI group

AWAKE Kompakt

ARISTA

AWAKE SECURITY PLATFORM

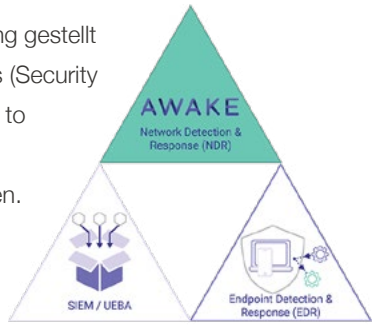
AWAKE So wie der menschliche Verstand Sinne und Kognition einsetzt, um Gefahren zu erkennen und darauf reagieren zu können, kann AWAKE feindliche Cyber-Security-Bedrohungen erkennen und darauf reagieren. AWAKE stellt Anomalien fest, verarbeitet und analysiert diese und liefert den IT-Verantwortlichen zugängliche Erkenntnisse.

AWAKE ist eine NDR (Network Detection und Respond)-Lösung, um Bedrohungen vorausschauend zu erkennen, zu kategorisieren und nach Priorität zu sortieren. Sie verschafft vollständige und umfassende Transparenz der gesamten Netzwerkkommunikation, Endpunkte und Ereignisse. Jeglicher Datenverkehr wird IT-Security-Verantwortlichen auf effektive Art und Weise sichtbar und verständlich.

Experten haben nicht genügend Zeit und Organisationen nicht genügend Experten, um die gestiegenen Herausforderungen durch die exponentielle Zunahme von zum Teil auch nicht managebaren Geräten (IoT, OT), veränderten Arbeitsbedingungen der Mitarbeiter und veränderten Cyber-Attacken auf das Netzwerk bewältigen zu können. Nur durch granulare Analyse des Datenverkehrs kann das erforderliche Sicherheitsniveau im Unternehmen erhöht werden.

Bei AWAKE kommt künstliche Intelligenz zum Einsatz, die mit menschlichem Fachwissen kombiniert wird, um Bedrohungsszenarien im Detail bewerten zu können. Selbst verschlüsselter Datenverkehr wird sicherheitsrelevant auf Anomalien geprüft, um die Bedrohungslage situativ beurteilen zu können.

Netzwerk- und Kontextdaten werden zur Verfügung gestellt und dadurch auf Schlüsselindikatoren eines SOCs (Security Operations Center) – in der Regel die „Mean Time to Detection“ und die „Mean Time to Response“ auf Cyber-Attacken zu minimieren – positiv einzuwirken.



Eine API-Integration in Sicherheitsplattformen erlaubt zusätzlich eine Response-Orchestrierung.

Was passiert in Ihrem Netzwerk ohne Ihr Wissen? Sie sind sich nicht sicher? Dann kommt AWAKE ins Spiel und gibt Aufschluss darüber, was in Ihrem Netzwerk passiert, wo und wann etwas passiert und welche Risiken diese Ereignisse für Ihre Netzwerksicherheit bergen.

Die AWAKE Security Plattform ist die einzige NDR-Lösung, die stichhaltige Antworten in dieser Ausprägung liefert. Auffälligkeiten werden vielmehr detailliert beschrieben und anschließend einer Risiko-Einschätzung unterzogen. Durch die Kombination von künstlicher Intelligenz und menschlichem Fachwissen modelliert AWAKE selbstständig das Verhalten von internen und externen Angriffen und sucht nach ihnen.

WIE FUNKTIONIERT AWAKE?

Virtuelle oder physikalische Sensoren werden an definierten Stellen – Campus, Datacenter, IOT Endpunkten oder Cloud Infrastrukturen – implementiert. Diese Sensoren ermitteln alle Netzwerkaktivitäten von Layer 2 bis Layer 7. Die Security relevanten Daten, die an die AWAKE Nucleus Plattform (Cloud basierend oder On-premise) gesendet werden, entsprechen ca. 3 % des gesamten Datenverkehrs.

Endgeräte, Nutzer und Anwendungen werden profiliert und analysiert. Sämtliche Daten werden am Ort der Erfassung aufbewahrt und so sind Datenschutz und Compliance in Echtzeit gewährleistet.

Es werden keine lokalen Daten in die Cloud gesendet – die Analyse wird vor Ort durchgeführt – alle Informationen verbleiben in der AWAKE Nucleus Appliance.

Ausschließlich die Daten, die zur Analyse des Datenverkehrs benötigt werden, werden aus der Cloud bezogen.

Device-Klassifizierung:

Die Klassifizierung der Devices wird anhand verschiedener Parameter vorgenommen:

- Typ/Art des Devices
- Betriebssystem
- Seit wann aktiv und wann zuletzt aktiv?
- Welche User haben das Device genutzt?
- Welche IP-Adressen, welche Applikationen, welche Protokolle nutzt das Device?
- Welche ähnlichen Devices sind im Netzwerk vorhanden?
- Wird das Endgerät mit einem EDR-System geschützt, welches der AWAKE Plattform zusätzliche Informationen zur Verfügung stellen kann?

Diese Klassifizierungen werden durch passives Monitoring durchgeführt – es muss kein Agent auf dem Device installiert werden. Die so gesammelten Informationen können in Kontext gebracht werden, um Anomalien in Ihrem Netzwerk festzustellen.

Risiko-Klassifizierung

AWAKEs standardisiertes Risiko-Dashboard bietet Ihnen einen umfassenden Einblick in die Risiken Ihrer Organisation, einschließlich Geräten mit riskantem Verhalten, Modellübereinstimmungen (um Gruppen zu klassifizieren) und verdächtigen Domänen.

Für das Aufspüren von Gefahren kommt AML (Adversarial Modelling Language) zum Einsatz. AWAKE setzt AML ein, um Angreifer anhand von verdächtigem Verhalten zu

identifizieren, anstatt nur nach spezifischen Indikatoren für einen Angriff zu suchen. Dies erfordert ein Verständnis der Entitäten im Netzwerk, die Identifizierung von Ausnahmeerscheinungen und verdächtigen Kommunikationsmustern.

Durch den Einsatz von verschiedenen Modellierungstechniken können mehrdimensionale Analysen durchführt werden, die Faktoren wie Zeit, Entitäten, Häufigkeit, Protokolle und Angriffsstufen umfassen, und zu vereiteln. Dieser Ansatz macht die Verteidigung effektiver und widerstandsfähiger, da die Erkennung eines verdächtigen Verhaltens nicht auf IOCs (Indicator of Compromise) basieren, die der Angreifer nach Belieben ändern kann. Im Grunde genommen bietet diese Technik die Möglichkeit, selbst die komplexesten Verhaltensweisen von Angriffen zusammenzufügen und daraus Schlüsse zu ziehen.

Threat Hunting Support

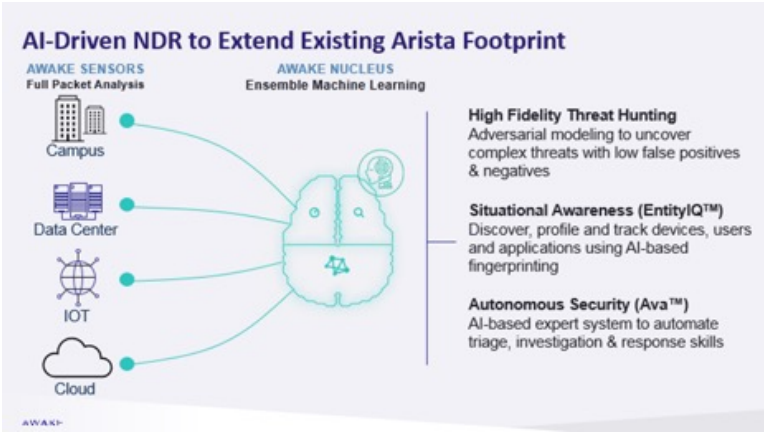
Das System liefert vorberechnete Antworten auf Fragen, die Threat-Hunting-Experten stellen würden. D.h., es nutzt die gleiche Systematik wie ein menschlicher Experte bei der Investigation. Das System übernimmt dabei systematisch und automatisch Aufgaben und liefert Resultate der Investigation, die mit rein menschlichem Arbeitseinsatz in diesem Umfang nicht möglich wäre oder mit enormem Zeit- und Kostenaufwand verbunden wäre.

Dadurch ergibt sich ein enormer Zeitvorteil u.a., um festzustellen, ob es sich um einen falschen Alarm oder eine echte Bedrohung handelt, um dann bei Bedarf schnellstmöglich reagieren zu können.

Alle Auffälligkeiten werden nicht nur festgestellt und detailliert beschrieben, es wird auch festgehalten, warum die Auffälligkeit ein Risiko darstellt und welche nächsten Investigationsschritte empfohlen werden. Ferner wird der „Abfrageweg“ – sprich der „AML Code“ angezeigt, so dass nachvollziehbar ist, wie das System zu den gewonnenen Erkenntnissen gekommen ist. Dieser AML Code lässt sich vom Security-Verantwortlichen auch auf spezifische Anforderungen anpassen.

AWAKE VIRTUAL ASSISTANT (AVA)

Um Anomalien mit hohem Automatisierungsgrad aufzuspüren zu können, ist der AWAKE Virtual Assistant – kurz AVA – für Security-Verantwortliche ein sehr effektives Werkzeug. Er definiert dabei eine Situation – eine Auffälligkeit – die er detailliert untersuchen möchte. AVA, der virtuelle Assistent, startet den Bearbeitungsprozess und liefert kontextbasiert ermittelte Analyseergebnisse in kürzester Zeit – sowie auch die nötigen Dokumentationsnachweise, wie das Analyseergebnis ermittelt wurde. AVA umfasst einen großen Pool von vordefinierten Abfragemechanismen, die von professionellen Threat-Hunting-Experten permanent zur Verfügung gestellt und aktualisiert werden.



KOMPAKTES AWAKE-PORTFOLIO / SUBSCRIPTION/SLAS

Arista/AWAKE: Network Detection & Response Appliances

NDR Appliances	
Nucleus Appliances	
DCA-NDR-A5	ASP All-In-One Physical Appliance, up to 5Gb/sec Bandwidth
DCA-NDR-NB10	ASP Nucleus Physical Appliance, up to 5Gb/sec Bandwidth
Sensor Appliances	
DCA-NDR-S5	ASP Sensor Physical Appliance, up to 5Gb/sec Bandwidth
DCA-NDR-S1	ASP Sensor Physical Appliance, up to 1Gb/sec Bandwidth
Sensor virtual Appliances	
ASP Virtual ESXI Sensor Subscription License for 1-Month, up to 1Gb/sec Bandwidth	
ASP Virtual ESXI Sensor Subscription License for 1-Month, up to 500Mb/sec Bandwidth	
ASP Virtual AWS Sensor Subscription License for 1-Month, up to 1Gb/sec Bandwidth	
ASP Virtual GCP Sensor Subscription License for 1-Month, up to 1Gb/sec Bandwidth	

Zu den Nucleus- und den Sensor-Appliances stehen verschiedene Software Subcriptions zur Verfügung, sowie entsprechende SLA Agreements für die NDR-Hardware.

AWAKE-Recording

Auf Anfrage können wir Ihnen gerne eine Aufzeichnung zur Verfügung stellen, welches Ihnen das System kompakt und granular in nur 45 Minuten vorstellt.

Für detaillierte Informationen über das komplette Arista Portfolio steht Ihnen unser Arista Kompakt zur Verfügung!

IHR ARISTA KONTAKT

- **Anja Staufenberg**
  Channel Partner Manager
  Mobil: +49 (0)172 270 00 72
  Email: anja@arista.com

IHRE 3KV ANSPRECHPARTNER

- **Philipp Matitschek**
  Vendor Manager Solutions
  Tel. +49 (0)89 800 656-22
  Fax: +49 (0)89 800 656-66
  Email p.matitschek@3kv.de

- **Norbert Wöllner**
  Vendor Manager Arista Networks
  Tel. +49 (0)89 800 656-60
  Fax: +49 (0)89 800 656-66
  Email n.woellner@3kv.de