ACD
ACTIVE CYBER DEFENSE

ANGRIFFSERKENNUNG ALS FULL-MANAGED-SERVICE 24/7

– ohne eigene umfassende IT-Security-Abteilung

Proaktive Angriffserkennung für ein Höchstmaß an Netzwerksicherheit.

Mit Active Cyber Defense (ACD) erfahren Sie, ob Angriffsaktivitäten in Ihrem Netzwerk stattfinden.

Unser ACD-Team informiert Sie, sobald Handlungsbedarf besteht.

Sie erreichen umgehend ein Höchstmaß an Netzwerksicherheit für Ihr Unternehmen – und entlasten Ihre IT-Security.

Ein direkter Ansprechpartner steht Ihnen gerne persönlich zur Verfügung.

Alle Vorteile von ACD im Überblick:

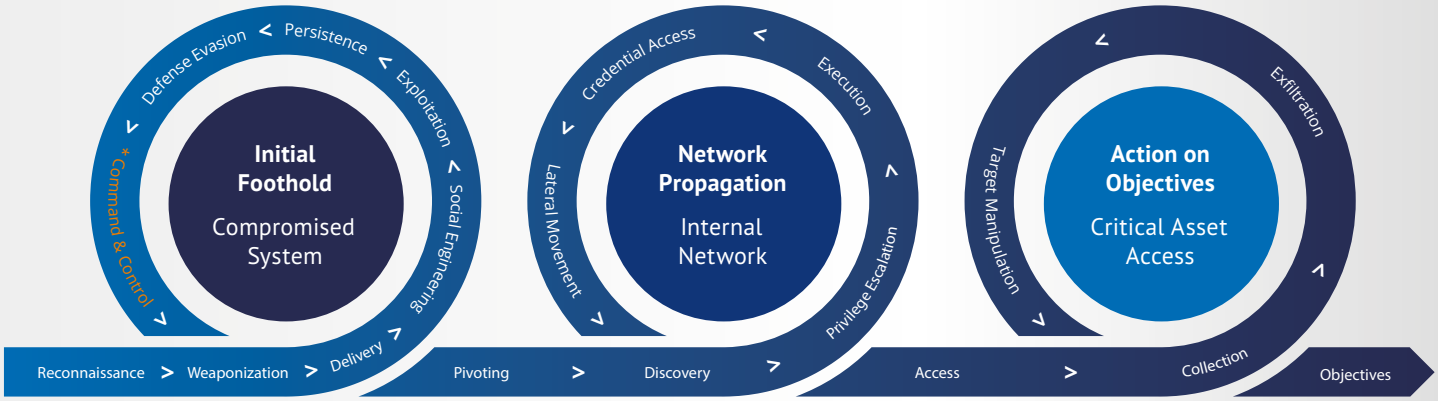
- Alle Daten werden vollständig in Ihrem eigenen Netzwerk EU-DSGVO-konform gehostet.
- Ein Full-Managed-Service zum Festpreis mit finanzieller Planungssicherheit – rund um die Uhr.
- Abhängig von Ihrer Organisation kann ACD sehr schnell innerhalb weniger Tage implementiert werden.
- ACD überwacht und identifiziert Angriffsaktivitäten vollständig „agentless“.
- Unsere ACD-Sensoren werden vollständig transparent im Netzwerk platziert, sodass ein Angreifer keine Chance hat diese zu erkennen.
- ACD geht über eine signaturbasierte Command & Control Detection hinaus.
- Gezielte Incident-Response-Maßnahmen können umgehend eingeleitet werden, noch bevor ein signifikanter Schaden eintritt.
- Es werden alle Systeme Ihrer Organisation überwacht – unabhängig von deren Betriebssystem oder Gerätetyp.

Allgeier CyRis GmbH
Hans-Bredow-Straße 60
28307 Bremen

+49 40 797 249 32
info@allgeier-cyris.de
www.allgeier-cyris.de

ALLGEIER CyRis

Wie erfolgt der Angreifer-Zugriff?



Minuten bis Stunden

Tage bis Wochen

Stunden bis Jahre (Langzeitzugriff)

* Hier setzt unser Allgeier CyRis ACD-Team ein.

Wie hilft Active Cyber Defense, wenn Ihre IT-Sicherheitsmechanismen überwunden werden?

1. Der Angreifer hat automatisiert oder manuell Zugriff auf ein System in Ihrem Netzwerk erlangt.
2. Der Angreifer stellt unmittelbar danach eine Kommunikation zu seiner Command & Control-Infrastruktur her.
3. Die ACD-Tools erkennen diese Artefakte und lösen eine Alarmierung an das ACD-Team aus.
4. Der Alarm wird geprüft. Sofern ein Sicherheitsvorfall bestätigt wird, werden Sie unmittelbar informiert.
5. Ihre Incident Response beginnt – bevor der Angreifer in schädlicher Weise agieren oder sich ausbreiten kann!
6. Auf Wunsch: Das ACD-Team unterstützt Sie bei Ihrer Incident Response.

Gut zu wissen:

- ACD schützt Sie vor den Ausfallkosten, Regressansprüchen und Image-Schäden, die durch Cyber-Kriminalität verursacht werden.
- ACD macht teure zusätzliche Überwachungsmechanismen für Ihr Unternehmen obsolet und kommt ohne monatelange Implementierungsphasen aus (anders als z.B. SIEM-Lösungen).

Allgeier CyRis GmbH
Hans-Bredow-Straße 60
28307 Bremen

+49 40 797 249 32
info@allgeier-cyris.de
www.allgeier-cyris.de

ZUSÄTZLICHE ACD-FEATURES, VON DENEN SIE PROFITIEREN SOLLTEN:

ACD Deception:

- ACD Deception ist ein Modul zur frühzeitigen Erkennung von Angreifer-Aktivitäten in einem Netzwerk.
- Dabei werden sogenannte Canary Tokens als Datei(en) oder Benutzer auf Hosts registriert, die aus Sicht des Angreifers möglichst interessant sind.
- Sobald auf diese Canary Tokens zugegriffen wird, bzw. eine Anmeldung des Canary-Benutzers stattfindet, wird ein Alarm auf der Analyseinstanz des Kunden generiert und an das CyRis SOC und an das ACD-Team eskaliert..
- Das ACD-Team bewertet und meldet den Alarm wiederum dem Kunden über die bereits vereinbarte Meldekette des Active Cyber Defense Services.

ACD Readiness & Response

- ACD Readiness & Response beinhaltet ein Incident-Response-Kontingent und einen IR-Readiness-Workshop.
- Das Kontingent beinhaltet Unterstützung und Beratung im Falle eines IT-Sicherheitsvorfalls (bspw. einer Verschlüsselung).
- Der Workshop umfasst die Vorbereitung des Kunden auf IR-Fälle.

ACD Witness

- Witness ist ein Zusatz- oder Aufbaumodul zu ACD.
- Witness ist Agent-basiert (aktuell nur Windows).
- Witness bietet zusätzliche Möglichkeiten der Überwachung und Analyse, da Windows Logs überwacht werden.
- Witness bietet die Möglichkeit, auch Systeme zu überwachen, die nicht bereits über den Monitoring-Port in der ACD-Basis-Variante überwacht werden (bspw. Homeoffice-Systeme).

ALLGEIER CyRis

Allgeier CyRis GmbH
Hans-Bredow-Straße 60
28307 Bremen

+49 40 797 249 32
info@allgeier-cyris.de
www.allgeier-cyris.de

ALLGEIER
CyRis