



Cybersecurity-Asset- und Risikomanagement

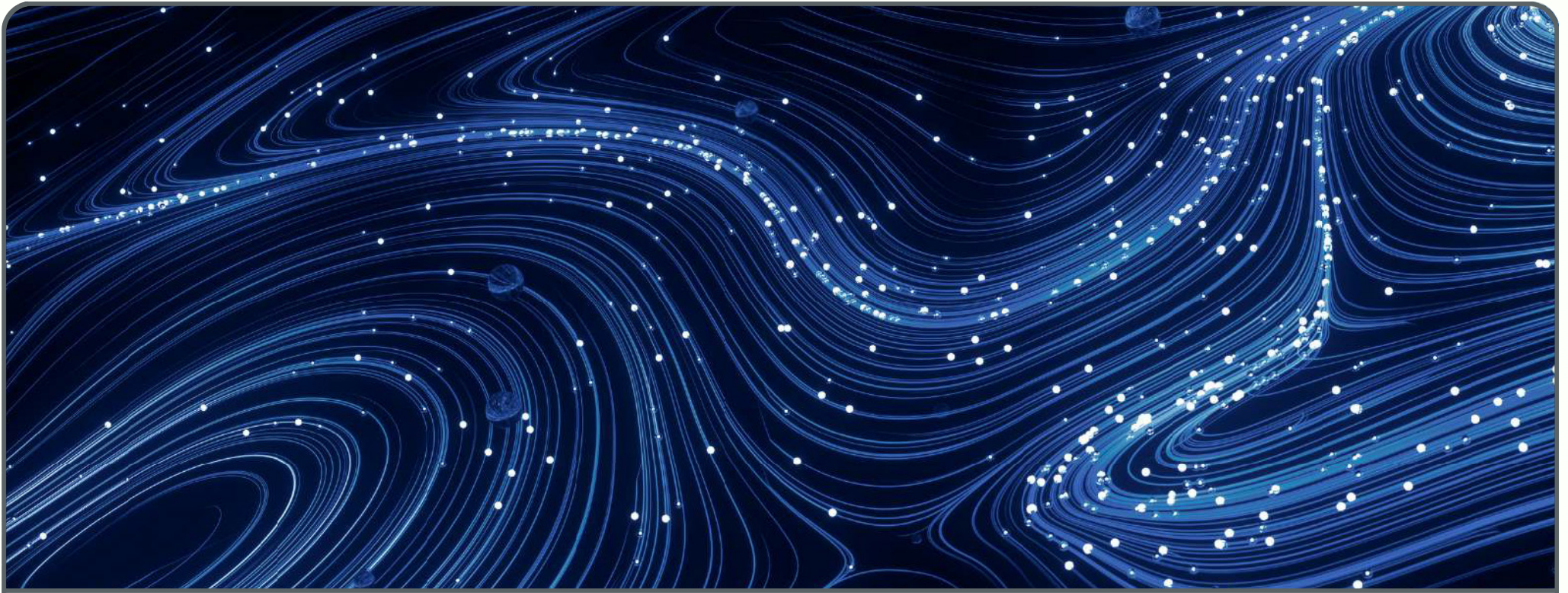
Warum Sichtbarkeit und Kontext entscheidend sind



www.sechard.com



sales@sechard.com



Die Sichtbarkeitslücke: Eine der größten Sicherheitsbedrohungen

Mit der Expansion von Unternehmen in lokale, Cloud- und Remote-Infrastrukturen ist die Anzahl vernetzter Assets exponentiell gestiegen. Ohne eine zentrale Asset-Inventarisierung arbeiten Sicherheitsteams im Blindflug – sie übersehen falsch konfigurierte Server, nicht verwaltete Geräte und nicht autorisierte Anwendungen.

Aber Sichtbarkeit allein reicht nicht aus.



sales@sechard.com



www.sechard.com





Von der Entdeckung zur verwertbaren Erkenntnis

Effektives Risikomanagement erfordert die Verknüpfung von Assets mit Risikobewertungen, kontextbezogenen Daten und Maßnahmen zur Behebung.

Das bedeutet: Nicht nur wissen, was verwundbar ist, sondern warum es wichtig ist – z. B. ob es sich um einen kritischen Server für Finanzoperationen handelt oder ein vergessenes Gerät, das Ihr internes Netzwerk gefährdet.

Genau hier versagen traditionelle CMDBs und Excel-Tabellen.



sales@sechard.com



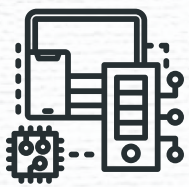
www.sechard.com





SecHard: Eine einheitliche Plattform für Asset- und Risikomanagement

Der integrierte Ansatz von SecHard vereint Asset-Erkennung, Risikobewertung, Schwachstellenerkennung und automatisierte Härtung in einer agentenlosen Plattform:



Umfassende Asset-Erkennung

Erkennt automatisch Geräte, Anwendungen, Server, IoT, OT u. v. m. – egal ob sie jetzt online sind oder morgen hinzugefügt werden.



Kontextbewusste Risikobewertung

Kombiniert technische Daten wie Schwachstellen, Härtungsstatus und Berechtigungsniveau mit Geschäftsrisikofaktoren aus GRC-Systemen, um einen realistischen Risikowert zu berechnen.



Echtzeit-Konfigurationsmanagement

Überwacht Systemintegrität, verfolgt unautorisierte Änderungen und erzwingt automatisch Sicherheitsrichtlinien.



Nahtlose Integration mit GRC-Tools

Importiert und exportiert Risikodaten, sodass SecHard kein Datensilo bleibt, sondern Teil Ihrer Governance-Struktur ist.



Automatisierte Behebung

Risiken nicht nur erkennen, sondern mit automatisierten Patches, Hardening und Zugriffskontrollen beseitigen.

Warum ist das wichtig?

Wenn Risiken nur nach technischer Schwere bewertet werden, können hochkritische Systeme übersehen oder kleine Probleme überbewertet werden. SecHard richtet Cybersecurity-Risiken an operativen Auswirkungen aus – damit sich Sicherheitsteams auf das konzentrieren, was wirklich zählt.

Bereit, alles zu sehen?

Mit SecHard wird Asset- und Risikomanagement nicht nur eine Checkliste, sondern eine strategische Funktion, die Resilienz, Compliance und Security-ROI vorantreibt.

Demo vereinbaren und entdecken, wie SecHard Ihre Sichtbarkeit und Risikostruktur in einen einheitlichen, automatisierten und intelligenten Prozess verwandelt.



Warum auf Angriffe reagieren, wenn man Risiken vorher beseitigen kann?

Die meisten Cybersecurity-Lösungen reagieren nach einem Angriff – doch warum warten?

SecHard beseitigt Risiken, bevor sie zu Bedrohungen werden – durch Systemhärtung, Compliance-Durchsetzung und Reduktion der Angriffsfläche.

 SECHARD
Complete Zero Trust

Dashboard

Resource

PAM

TACACS

Security Zone

Hardening Zone

Security Zone

Vulnerability Zone

Connection Zone

Multi Resource Conf

Backup & Restore

Records

Mac Addresses

Ports

Alarms

Maps

Management

User Management

Asset Management

Task Management

Hardening Zone

Search Name

Switch

Cisco

Cisco IOS Ser

Standart Benchmark v4.0.1

	1.01 Enable aaa new-model	1.01 Set the hostname	1.02 Set the ip domain name	1.02 Enable aaa authentication login	1.03 Set no interface tunnel	1.03 Set modulus to greater than or equal to 2048 for crypto key generate rsa	1.03 Enable aaa authentication enable default	1.04 Set seconds for ip ssh timeout	1.04 Set ip verify unicast source reachable-via	1.05 Set maximum value for ip ssh authentication-retries	1.05 Set login authentication for line tty	1.06 Set version 2 for ip ssh version	1.06 Set login authentication for line vty	1.07 Set aaa accounting to log all privileged use commands using commands 15	1.08 Set aaa accounting connection	1.09 Set aaa accounting exec	1.10 Set aaa accounting network	1.11 Set aaa accounting system	2.01 Set ip access-list extended to forbid Private Source Addresses from External Networks	2.01 Set no cdp run	2.01 Set privilege 1 for local users	2.02 Set transport input ssh for line vty connections	2.02 Set no ip bootp server	2.02 Set inbound ip access-group on the External Interface	2.03 Set no service dhcp	2.03 Set no exec for line aux 0	2.04 Create access-list for use with line vty	2.04 Set no ip ident	2.05 Set access-class for line vty	2.05 Set service tcp-keepalives-in	2.06 Set exec-timeout to less than or equal to 10 minutes for line aux 0
F1 Switch - 172.16.0.2	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
F1 Switch - 172.16.0.26	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
F1 Switch - 10 - 3N16-1	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗
Cisco Intercity Dudullu Servisier 2950	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Cisco Akyacht 2960 2	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
F1 Switch - 172.16.0.14	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓

Verhindern, Schützen, Einhalten

Noch bevor
Bedrohungen
entstehen.

Vorteile von SecHard

- ✓ **Prävention statt Reaktion**
 - Systeme härten, bevor Bedrohungen entstehen
- ✓ **Compliance-gesteuerte Sicherheit**
 - Regulatorische Anforderungen flächendeckend erfüllen
- ✓ **Nahtlose Integration**
 - Funktioniert mit bestehenden Sicherheitsplattformen
- ✓ **Automatisierte Risikominimierung**
 - Angriffsflächen mühelos reduzieren

Warum auf einen Angriff warten?

Sichern Sie Ihre Infrastruktur jetzt.

Die meisten Cybersicherheitslösungen reagieren während oder nach einem Angriff – sie erkennen Bedrohungen, blockieren Eindringversuche und reagieren auf Sicherheitsverletzungen. Doch wenn sie aktiv werden, ist der Schaden oft bereits entstanden. SecHard verfolgt einen anderen Ansatz.

Wir erkennen nicht nur Bedrohungen – wir beseitigen Risiken, bevor sie entstehen. Mit Systemhärtung, Sicherheitskonfiguration, Risikobewertung und Zugriffskontrolle stärken wir Ihre Infrastruktur von innen heraus. So bleiben Ihre Systeme widerstandsfähig, konform und sicher – ganz ohne ständige Notfallmaßnahmen.



Ein echter Plattformansatz für Sicherheit

Sicherheit bedeutet heute nicht mehr nur Einzellösungen – sondern Plattformisierung. SecHard integriert sich nahtlos in Ihre Sicherheitslandschaft und ergänzt Lösungen wie Palo Alto, Trellix und Symantec. Während diese sich auf Angriffserkennung und Reaktion konzentrieren, fokussiert sich SecHard auf proaktive Risikobeseitigung.

Das Ergebnis? Eine ganzheitliche Sicherheitsstrategie, die Resilienz stärkt, Compliance erhöht und Ihrem Unternehmen den besten Schutz gegen moderne Bedrohungen bietet.



sales@sechard.com



www.sechard.com

SecHard Cyber Hygiene Plattform

Eine Plattform. Volle Sicherheit. Maximale Resilienz.

SecHard bietet eine einheitliche Cybersicherheitsplattform, die ganzheitliche Cyber-Hygiene operationalisiert. Die Plattform automatisiert zentrale Maßnahmen wie Asset-Erkennung, Konfigurationsmanagement, Schwachstellenbewertung, Systemhärtung und Zugriffskontrolle – alles in einer einzigen integrierten Lösung

Die SecHard Cyber Hygiene Plattform ist eine modulare Softwarelösung, die darauf ausgelegt ist, grundlegende Sicherheit und Resilienz direkt in Ihrer Umgebung aufzubauen. Sie unterstützt die Einhaltung zahlreicher Branchenstandards und Frameworks, darunter CBDDO, CIS V7.1, CIS V8, CMMC, HIPAA, ISO 27001, ISO 27002, NIST 800-171r2, NIST 800-207A, NIST 800-210, NIST 800-53r5, PCI DSS, SOX, DSGVO, KSA SAMA, KSA ECC und das Egypt Financial Cyber Security Framework Digital v1.

Die Module der Plattform arbeiten nahtlos zusammen und bieten ein umfassendes Set an Werkzeugen zur Stärkung Ihrer Sicherheitslage. Dazu gehören: Security Hardening, Privileged Access Manager, Asset Manager, Vulnerability Manager, Risk Manager, Device Manager, Performance Monitor, Key Manager, TACACS+ Server und Syslog Server.

Kontaktieren Sie uns noch heute, um zu erfahren, wie SecHard Ihre Cybersecurity-Ziele unterstützen kann!





Hat Ihnen dieser Inhalt gefallen?



Doppelt
tippen



Kommentar
hinterlassen



Mit Freunden
teilen



Für später
speichern

+ Folgen



sales@sechard.com



www.sechard.com