Controlware Security Day 2022

Cyber Sicherheit unternehmensweit neu denken

Holger Müller, CTO & Lead Architect für Länder, Kommunen, Bildung und Gesundheit
homuelle@cisco.com

22. September 2022

Vorstellung

- 1999-2013 IBM Deutschland
  - zuletzt in der Rolle als Global Lead Architect für IBM-eigene IT
  - Mit-Erfinder des IBM Patent: US2014/0373007A1
    Provisioning a secure customer domain in a virtualized multi-tenant environment
  - Mit-Autor des IBM Redbooks – „IBM and Cisco: Together for a World Class Data Center“
- 2013-2022 Cisco Systems
  - Begonnen als Data Center Solution Architect
  - Seit 5 Jahren in der Rolle als CTO und Lead Architect für Länder, Kommunen, Bildung und Gesundheit
  - „Übersetzer und Brückenbauer“ von Business Anforderungen in IT und umgekehrt
- Interessen
  - Familie (verheiratet und 2 Söhne)
  - Fußball in jeglicher Art
  - Reisen mit dem e-Mountainbike

Was Euch in meinem Impulsvortrag erwartet …

1. Was höre ich von anderen Kunden, primär von C-Level und IT-Entscheidern?

2. Warum ist eine Risiko-orientierte IT-Sicherheit essentiell und wie können wir organisationsweit Klarheit und Orientierung geben?

3. Welche Möglichkeiten und Mehrwerte (technisch und operativ) bieten unserer Lösungen und Plattformen, um das Cyber Risiko kontinuierlich zu minimieren

“Zeit des rasenden Stillstandes”

Umsetzungsdilemma

Klarheit und Orientierung

Erfolgreiche Umsetzung
und Mehrwerte generieren

Welches gemeinsame Verständnis sollte jeder in der Organisation haben und wie sollte der Wandel gestaltet werden?

Cyber Sicherheit auf das nächste Level heben

gesetzl. Mindest-anforderungen	obligatorische Schutzmaßnahmen	Risiko-orientierte Cyber Security	Business-enabling Cyber Security

"Endliches Spiel"

Gefühlte Sicherheit

RISIKO REDUZIEREN

AGILITÄT ERHÖHEN

"Unendliches Spiel"

Cyber Sicherheit neu denken


Proaktive Erkennung und Bewertung von Schwachstellen & Risiken
Kont. Erkennung von Vorfälle/Angriffe
Security Operations Management
Planung von Abhilfemaßnahmen
Analyse und Reaktion auf Vorfälle
Kont. Verbesserung der Sicherheitsarchitektur

Grenzen existieren oft nur im Kopf anhand von veralteten Denkmustern und Glaubenssätzen

Es gilt IT-Sicherheit ganzheitlich “neu zu denken”

Kontextbetrachtung anhand von vier Fokusbereichen und Sicherheitskontrollen

Fokusbereiche mit entsprechenden Sicherheitskontrollen

 Nutzer	Wer bist du und welche Rechte hast du?	Identitäts- und Rechtemanagement ist von zentraler Bedeutung inkl. Kontext Analyse
 Endgerät	Wie vertrauenswürdig ist dein Endgerät und was ist sein aktueller Gesundheitszustand?	Kontinuierliche Überprüfung des Gesundheitszustandes des Endgerätes (Posture Check) inkl. Angriffserkennung und Reaktion
 Netzwerk	In welchem Netzwerk bist du und wie vertrauenswürdig und abgesichert ist es?	Kontinuierliche und ortsunabhängige Prävention, Angriffserkennung und Reaktion - egal in welchem Netzwerk
 Apps & Data	Auf welche **kritischen** Daten und Applikationen willst du zugreifen und bist du dafür autorisiert?	Jeder Zugriff auf kritische Anwendungen und Daten wird authentifiziert und autorisiert

Wichtig: Vertrauen ist flüchtig –> Kontinuierliche Überprüfung

Integration macht den entscheidenen Unterschied

Kritische Sicherheits-kontrollen zur Prävention

Sich eitsniv auf nä es Lev eben

Erkennung und Reaktion

Erkennung und Reaktion

Erkennung und Reaktion

Ganzheitliches, proaktives & automatisiertes Security Monitoring, Angriffserkennung, Analyse und Reaktion auf Vorfälle

Security Operations Management

Welche Möglichkeiten und Mehrwerte ergeben sich daraus und wie sehen die Lösungen aus?

Wie sich die Arbeitswelt verändert hat …

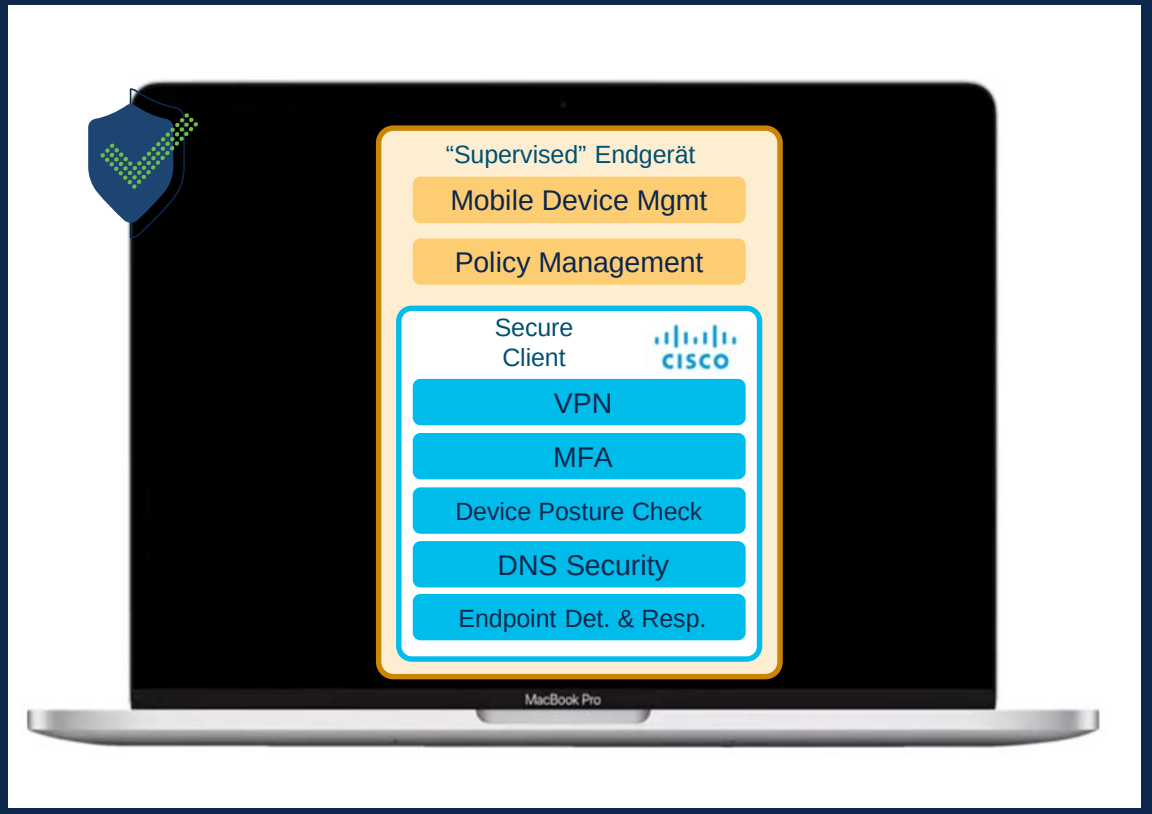
… und dabei Daten, Applikationen und Services aus dem Rechenzentrum nutzen

… und dabei Daten, moderne Applikationen und Web-Anwendungen von überall nutzen

Cisco Lösungen als Fundament

Intergration von verschiedenen Fähigkeiten machen den Unterschied

Meraki inkl. MDM und Umbrella als sichere Arbeitsumgebung



Cisco Secure Client

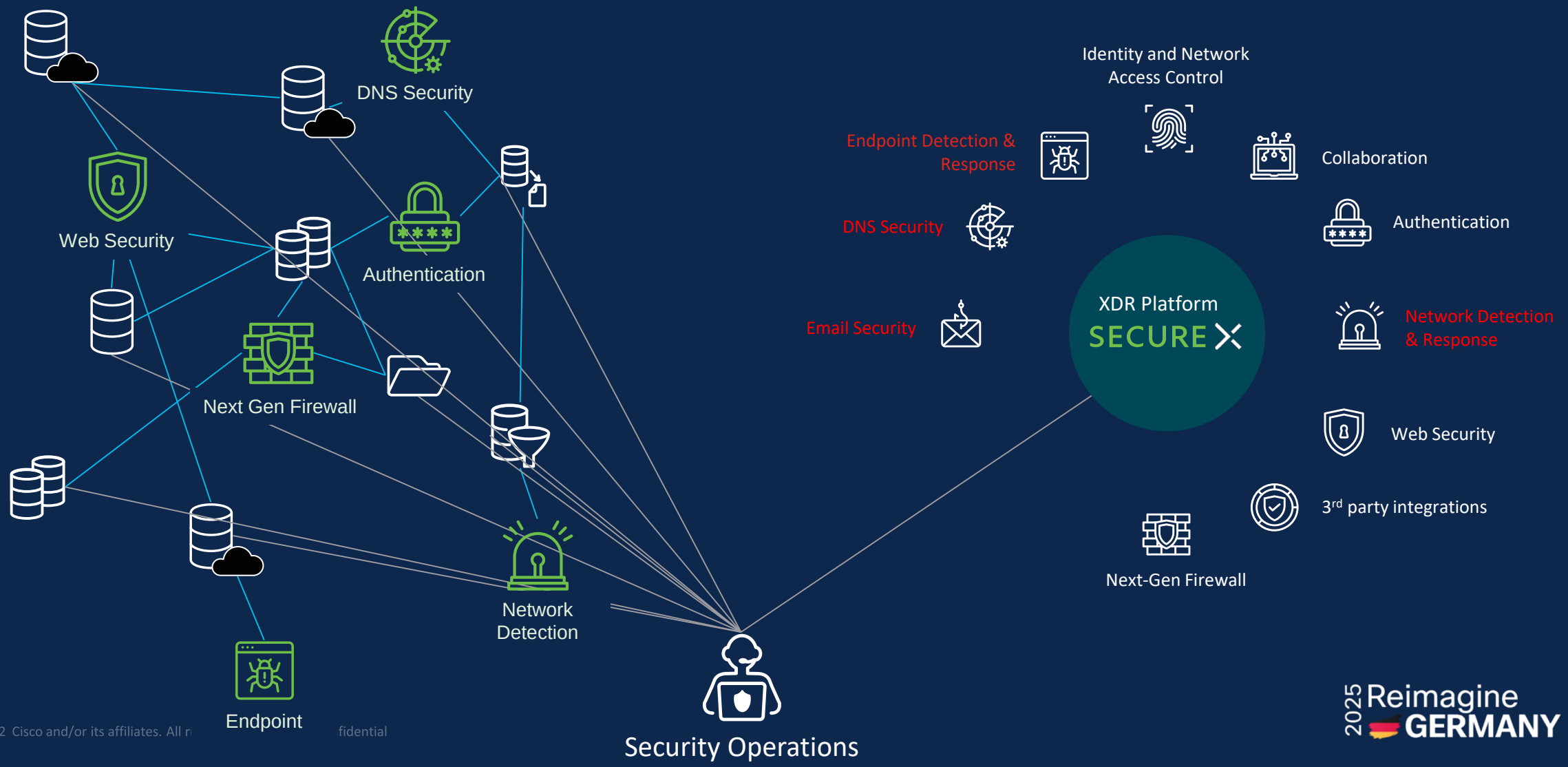
auch für Windows, iOS, Android, Linux, Chrome

Gerade auch als “managed Service” für Kunden interessant

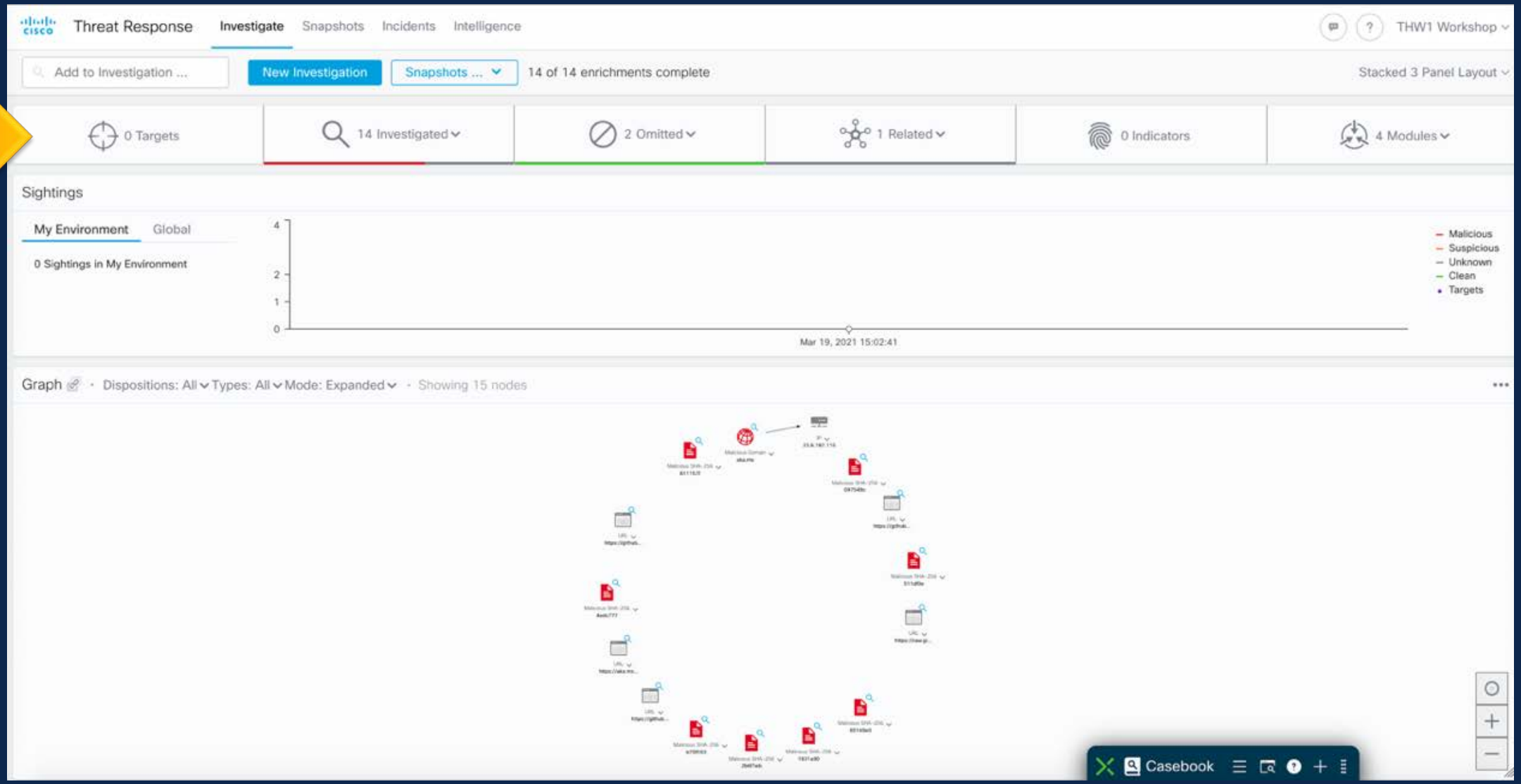

SIEM / SOAR
Extended Detection & Response xDR
Network Detection & Response
Endpoint Detection & Response
Threat Intelligence
Operations Management
Threat Hunting
Incident & Response
Security Monitoring von Endgeräten

Threat Hunting

Herkömmlich — Komplexität als größtes Problem — Stand der Technik



Proaktive Angriffserkennung mit Cisco Secure X



Incident & Response

Kontinuierliche Erkennung, Analyse und Reaktion auf Vorfälle

“Eine Angriffserkennung ohne Kontext ist möglich, aber sinnlos”

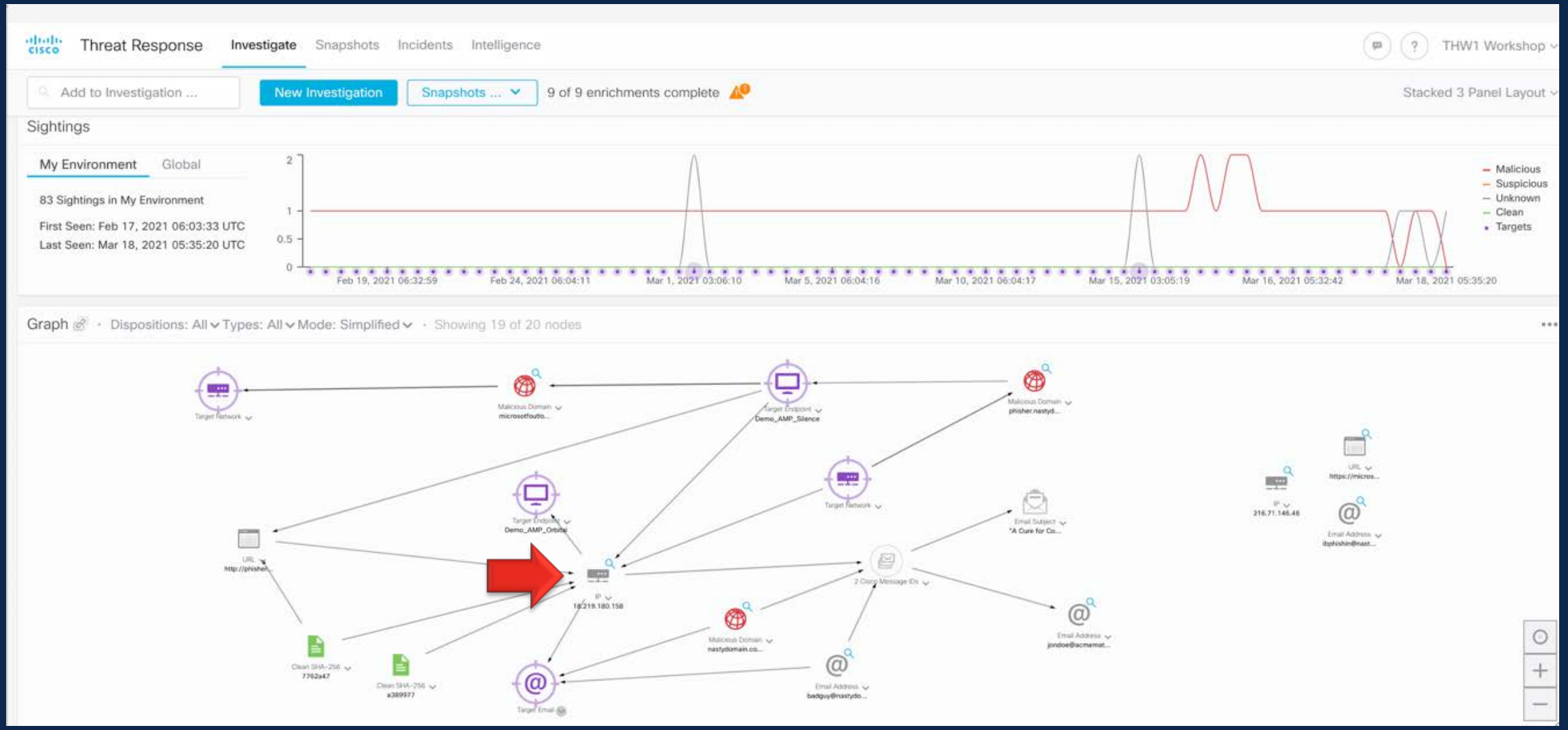
Es gilt organisationsübergreifend wichtige Fragen zu beantworten:

- **WER** oder **WAS** ist alles betroffen?
- **WIE** kam der Angriff in unsere IT?
- **WANN** fand das erste Eindringen statt?
- **WO** genau hat er sich quer bewegt und sich ausgebreitet?

Aber vor allem:

- **WAS NUN?**

Kontinuierliche Angriffserkennung mit Cisco Secure X



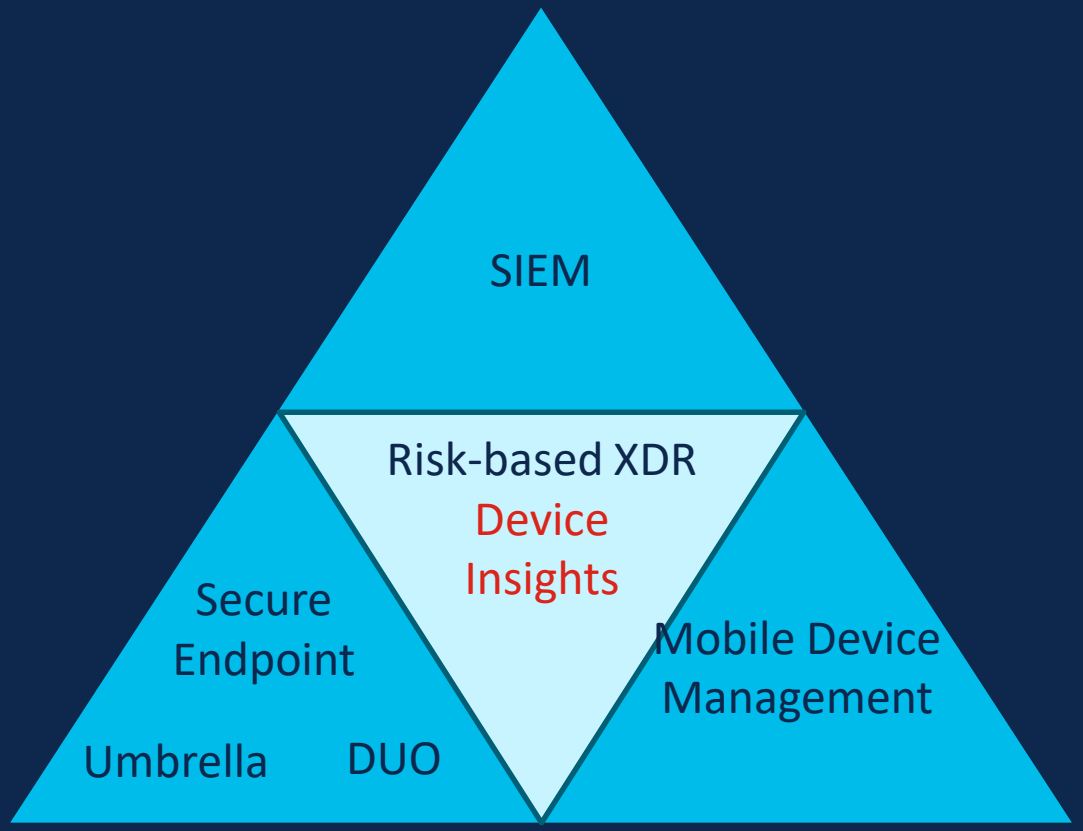
Security Monitoring von Endgeräten

Frühestmögliche Erkennung und Bewertung von Schwachstellen und Risiken, um Cyberangriffen zuvorzukommen

Es gilt organisationsübergreifend wichtige Fragen zu beantworten:

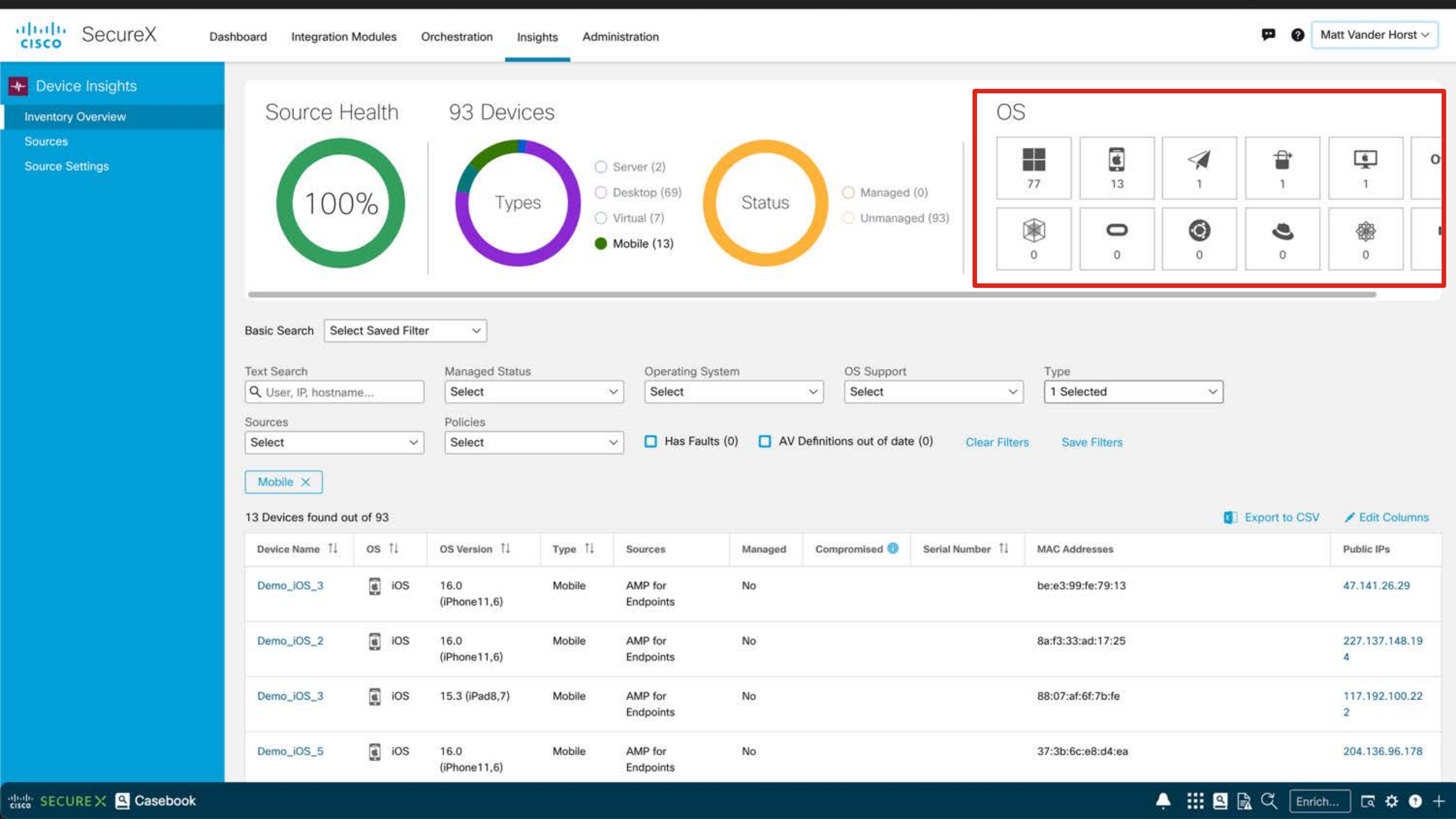
- **WELCHE Arten von Endgeräten** sind angeschlossen?
- **WER hat Zugriff** auf dieses Gerät
- **WO** befinden sich diese Geräte?
- **WELCHE Schwachstellen** haben diese Geräte?
- **WELCHE Sicherheitsagenten** sind installiert?
- **WELCHE Updates** sollten unbedingt gemacht werden?

Moderne pro-aktive Erkennung & Bewertung von Risiken mit entsprechenden Abhilfemaßnahmen



XDR Plattform Secure X ist integraler Bestandteil unserer Security Lösungen (kostenfrei)

- Fokus auf angeschlossene Endgeräte und deren Kontext
- Unterstützte Klassen von Endgeräte sind:
  - Desktop
  - Server
  - Mobile
  - Virtual
- Angreichert durch Mobile Device Management von Cisco Meraki, Microsoft Intune, VMWare Airwatch, Mobiliron und jamf


SecureX
Dashboard
Integration Modules
Orchestration
Insights
Administration
Matt Vander Horst
Device Insights
Inventory Overview
Sources
Source Settings
Source Health
100%
93 Devices
Types
Server (2)
Desktop (69)
Virtual (7)
Mobile (13)
Status
Managed (0)
Unmanaged (93)
OS
77
13
1
1
1
0
0
0
0
0
Basic Search
Select Saved Filter
Text Search
User, IP, hostname...
Managed Status
Select
Operating System
Select
OS Support
Select
Type
1 Selected
Sources
Select
Policies
Select
Has Faults (0)
AV Definitions out of date (0)
Clear Filters
Save Filters
Mobile
13 Devices found out of 93
Export to CSV
Edit Columns
Device Name
OS
OS Version
Type
Sources
Managed
Compromised
Serial Number
MAC Addresses
Public IPs
Demo_iOS_3
iOS
16.0 (iPhone11,6)
Mobile
AMP for Endpoints
No
be:e3:99:fe:79:13
47.141.26.29
Demo_iOS_2
iOS
16.0 (iPhone11,6)
Mobile
AMP for Endpoints
No
8a:f3:33:ad:17:25
227.137.148.194
Demo_iOS_3
iOS
15.3 (iPad8,7)
Mobile
AMP for Endpoints
No
88:07:af:6f:7b:fe
117.192.100.222
Demo_iOS_5
iOS
16.0 (iPhone11,6)
Mobile
AMP for Endpoints
No
37:3b:6c:e8:d4:ea
204.136.96.178
SECURE X
Casebook
Enrich...

Device Insights
Inventory Overview
Sources
Source Settings

Windows Microsoft Windows 10 Enterprise 10.0.19042

Managed: No Refresh from Orbital Live Query

Details

Associated Users	
Last Active	2022-03-21T10:32:51.985Z
Location	NA
Hostname	SNEHPATE-WIN10
Local IPs	192.168.246.102
Public IPs	64.100.2.99
Macs	00:50:56:b8:55:bd
Hardware Id	1f8bfbff00050654
Serial Number	vmware-42 38 c8 b9 91 1a e8 a9-b5 6b ab d3 bd 4c c2 27

Vulnerabilities

Vulnerabilities
1

Windows Security Center

Firewall: Enabled	Automatic Updates: Enabled
AntiVirus: Poor	AntiSpyware: Enabled
User Account Controls: Enabled	

Installed Security Products

Windows Firewall	Firewall	Enabled, Up to Date
Microsoft Defender Antivirus	Antivirus	Enabled, Not Up to Date

Cisco Secure Endpoint (AMP)

Isolation	Not Isolated
Orbital	Enabled

Connector GUID:
f870e243-05e9-4c1a-96c2-ba07f0eb9970

Seen in Sources

Umbrella

Last Seen:	2022-03-21T02:39:18.000Z		
Policy:	SecureX-DNS-Policy		
Client Type:	AnyConnect	Client Version:	4.8.204 5
Reported OS:	Windows	Reported OS Version:	10

Open Cisco Umbrella Dashboard in New Window

Orbital

Last Seen:	2022-03-21T10:32:51.985Z
Computer SID:	S-1-5-21-4272947542-4249360855-11149 50033

AMP for Endpoints

Last Seen:	2022-03-21T08:44:05.000Z
Policy:	SecureX-Desktops
Group:	SecureX-Desktops

Ich hoffe ich konnte Ihnen Anregungen geben…

1. … was es heißt das Sicherheitsniveau auf das nächste Level zu heben
2. … wie sich das Security Operations Management vereinfachen läßt anhand von Cisco SecureX
3. … welche Business-Mehrwerte und Möglichkeiten unsere ganzheitliche Architektur und unsere Technologien ermöglichen
4. … wie und wo wir Sie gemeinsam mit der Controlware unterstützen können


Future Ready
2025 Reimagine
GERMANY