



# Cyber Resilienz

## Moderne Detection & Response Ansätze

Holger Müller, CTO & Lead Architect, Cisco Systems

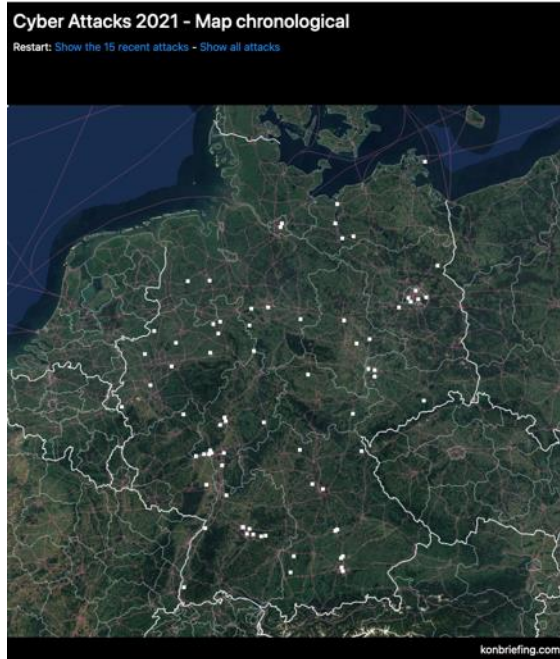
Verwaltung, Bildung und Gesundheit

Janek Maiwald, CTO Deutsche Gesellschaft für Cybersicherheit



# Öffentl. bekannte Cyber Attacken in Deutschland auf einen Blick

Von September 2021 bis 20. September 2022 aus Verwaltung, Bildung und Gesundheit in Deutschland

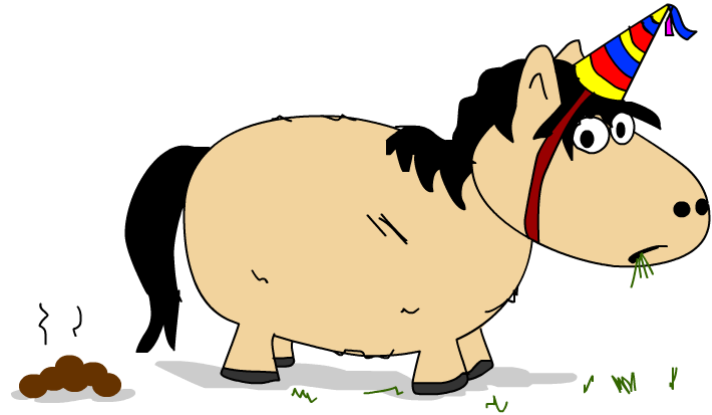


- Bundeswahlleiter
- Stadt Leipzig
- Bundestag
- Sozialdienst Olching
- Kreis Wesel
- Stadtwerke Wismar
- Stadt Dessau
- Universität Leipzig
- Kommunalservice Mecklenburg
- Stadt Schwerin
- Stadt Neustadt-Glewe
- Landkreis Ludwigslust-Parchim
- Stadt Witten
- DVZ IT Provider Land Mecklenburg-Vorpommern
- Verwaltung LAiV Land Mecklenburg-Vorpommern
- Evangelisches Familien-Bildungsstätte Giessen
- Nürnberg Institute of Technology
- Mittelschule Enger
- Mediatixx GmbH (Medical)
- Stadt Sassnitz
- Realschule Enger (NRW)
- Privates Gymnasium Königswinter
- Verbandsgemeindeverw. Seehausen
- Bayrische Krankenhaus Gesellschaft
- Stadtwerke Pirna
- Klinikum Braunschweig
- Leipziger Stadtreinigung
- Zahnarztpraxis Düsseldorf
- Stadt Schmalkalden
- CompuGroup Medical SE
- Unfallkasse Thüringen
- Ev. Schule St. Marien Neubrandenburg
- Medizin Campus Bodensee
- Pfarrei Heilig Kreuz Winnweiler
- FH Münster
- Kunstmuseum Stuttgart
- Museum Ulm
- Hochschule Anhalt
- BBS Goslar
- Stadtverwaltung Bochum
- Stadt Suhl in Thüringen
- BBS Cloppenburg
- Stadt Dingolfing
- TH Aschaffenburg
- Fraunhofer Institut Halle
- Donau-Stadtwerke Dillingen
- Stadt Schriesheim
- Uni-Bibliothek Leipzig
- Hochschule für Technik und Wirtschaft in Berlin
- Bundespolizei und Bundestag
- Stadt Murnau
- Stadt Bissingen
- Stadtreinigung Kassel
- Päd. Hochschule Freiburg
- FH Münster
- Komm DL. Hessen
- Stadt Burladingen
- Uni Wuppertal
- AMEOS Klinikum Neuburg
- Gymnasium Gunzenhausen
- IHK Verbände
- Stadt Stockach
- Stadt Egelsbach
- Gemeinde Dorn-Dürkheim
- Caritasverband

# Veraltete Denkmuster und Arbeitsweisen in einer Zeit des rasenden Stillstandes



# Wie IT-Hersteller und IT-Dienstleister Cyber Sicherheit positionieren und verkaufen 😊



Wie die Realität oft aussieht 😞

Reibungsverluste & Frustration

Effizienz, Wirksamkeit

Kontinuierliche Erkennung

Erkennung von Vorfällen und Angriffen,

Bewertung von Bedrohungen

Security Operations Management

Planung und Reaktion auf Vorfälle

Abhilfemaßnahmen

9:41



## Geschäftsführer

Messages

Neue Cyberbedrohung -  
Weißt du davon?  
Sind wir o.k.?

Bin dran.  
Moment noch.



Message



# Security Operations Management

Reibungs-  
verluste &  
Frustration

Effizienz,  
Wirksamkeit

Kontinuierliche  
Erkennung und  
Bewertung von Risiken &  
Bedrohungen

Planung von  
Abhilfemaßnahmen

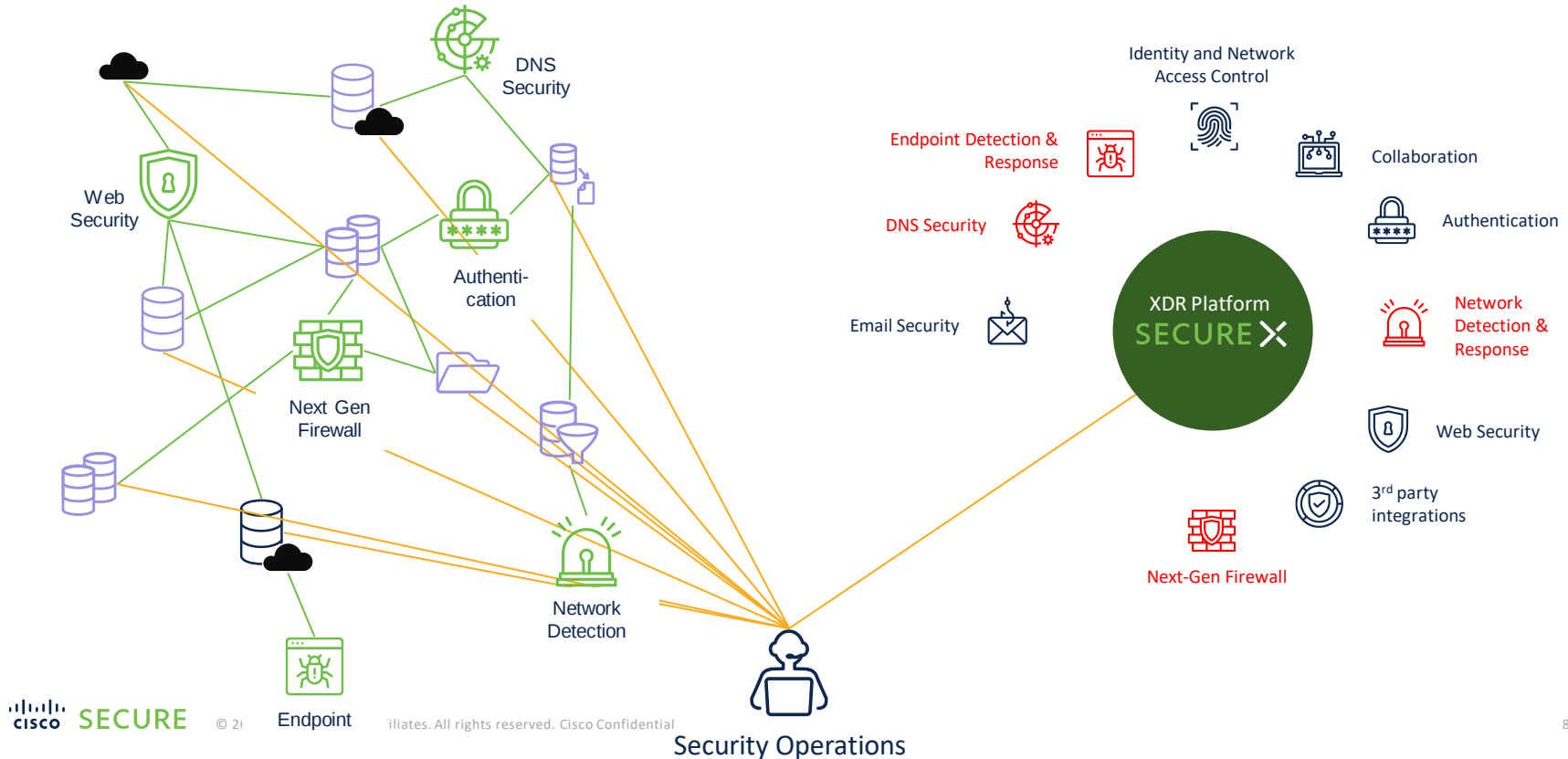
Kont. Erkennung  
von Vorfällen und  
Angriffen,

Analyse und  
Reaktion auf  
Vorfälle

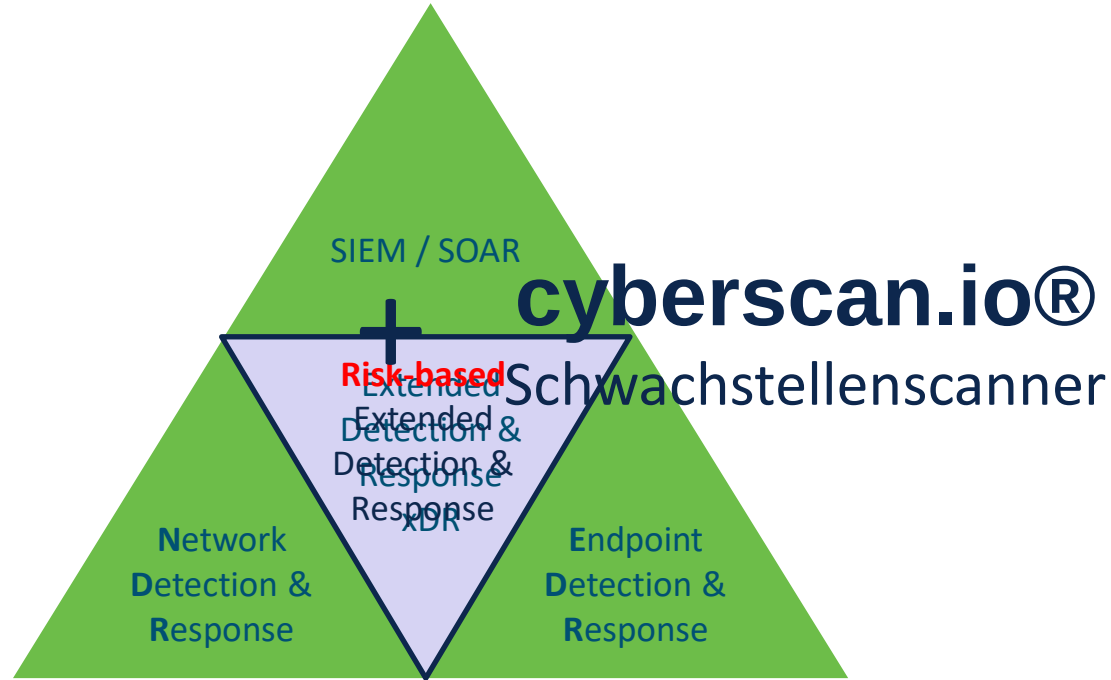
# Herkömmlich

## Komplexität als größtes Problem

# Stand der Technik



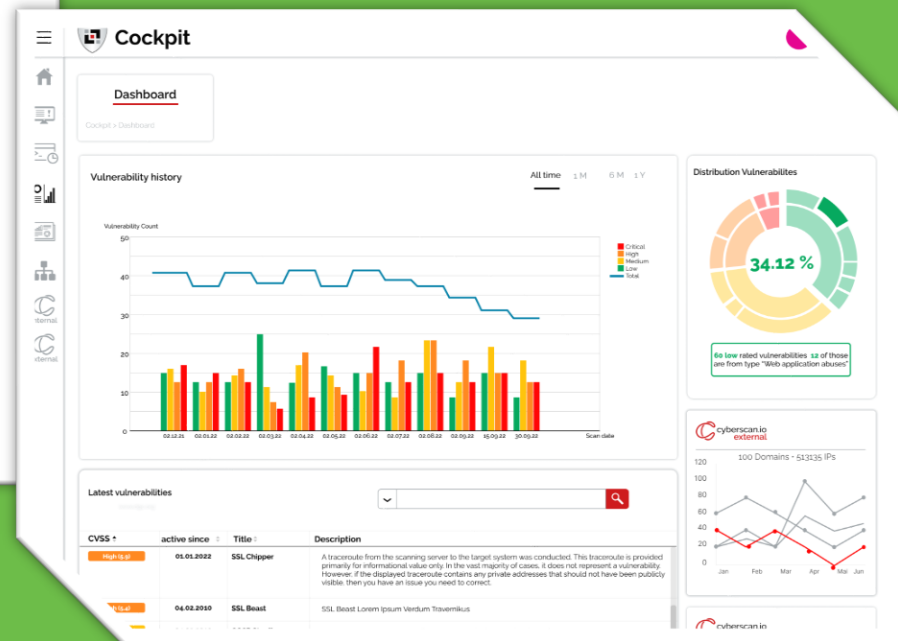
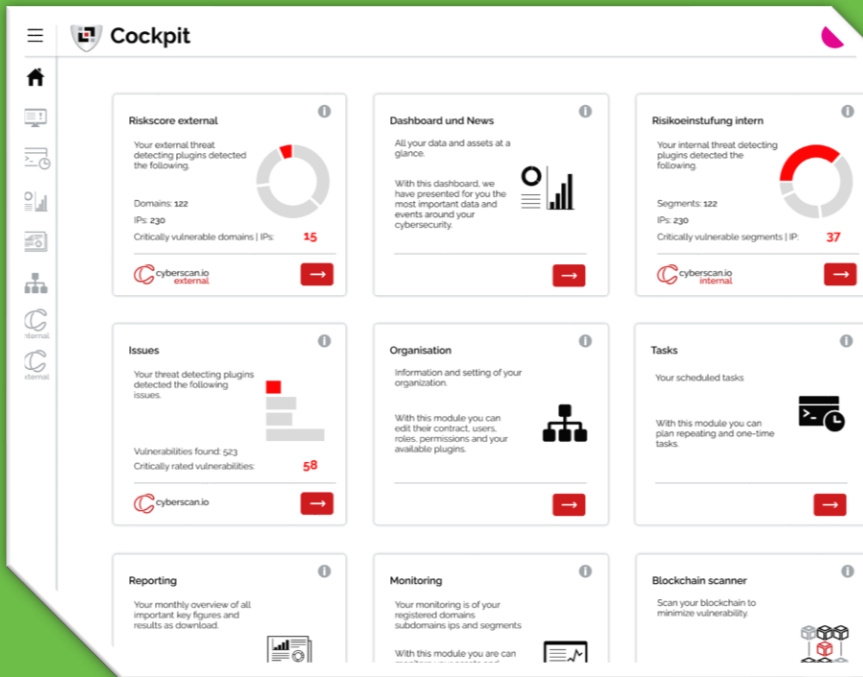
# Technologische Fähigkeiten zur Bedrohungserkennung und -abwehr



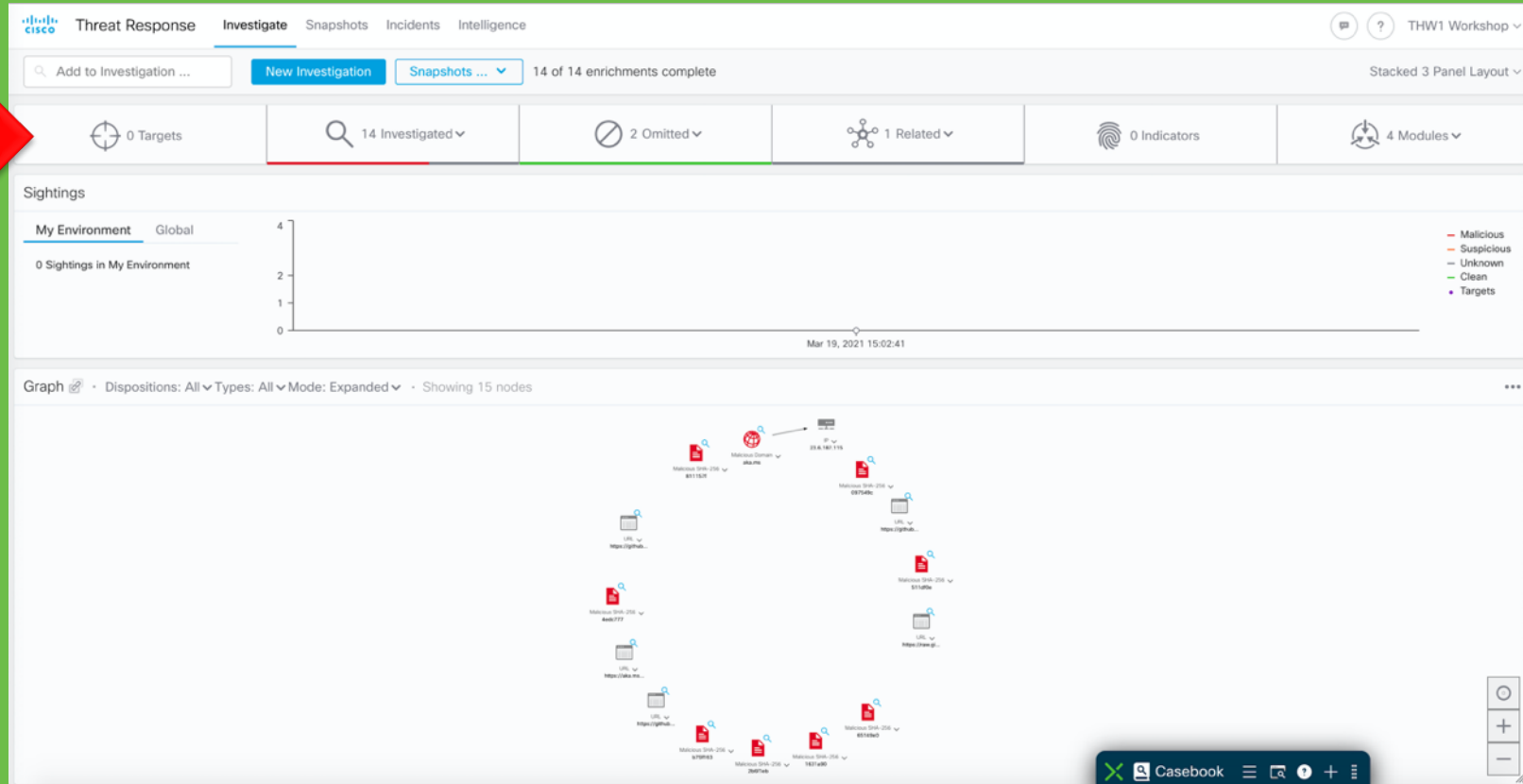
XDR Plattform Secure X ist integraler Bestandteil unserer Lösungen (kostenfrei)

.... und wie genau sieht  
das nun in der Praxis  
aus?

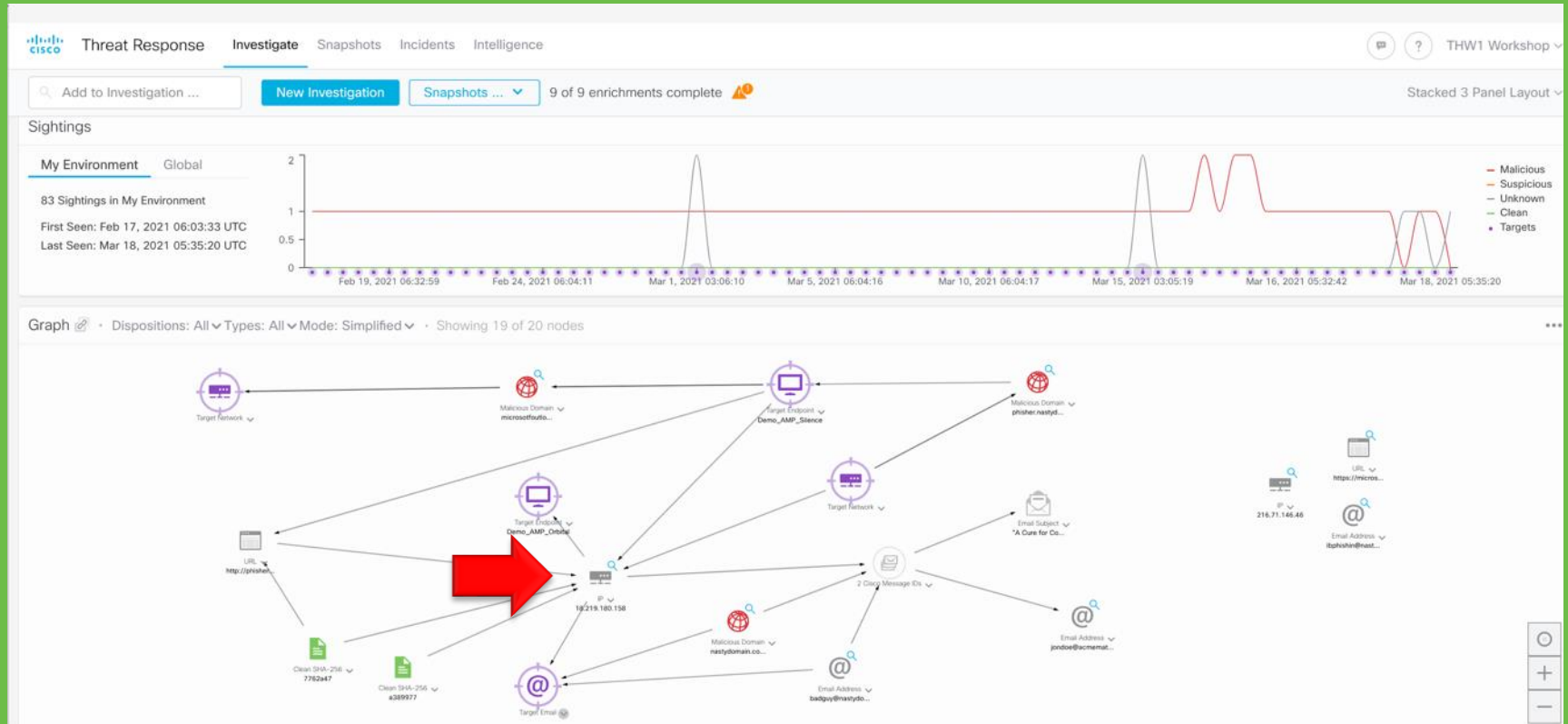
# Kontinuierliches Erkennen von Schwachstellen



# Proaktives Erkennen von Auffälligkeiten

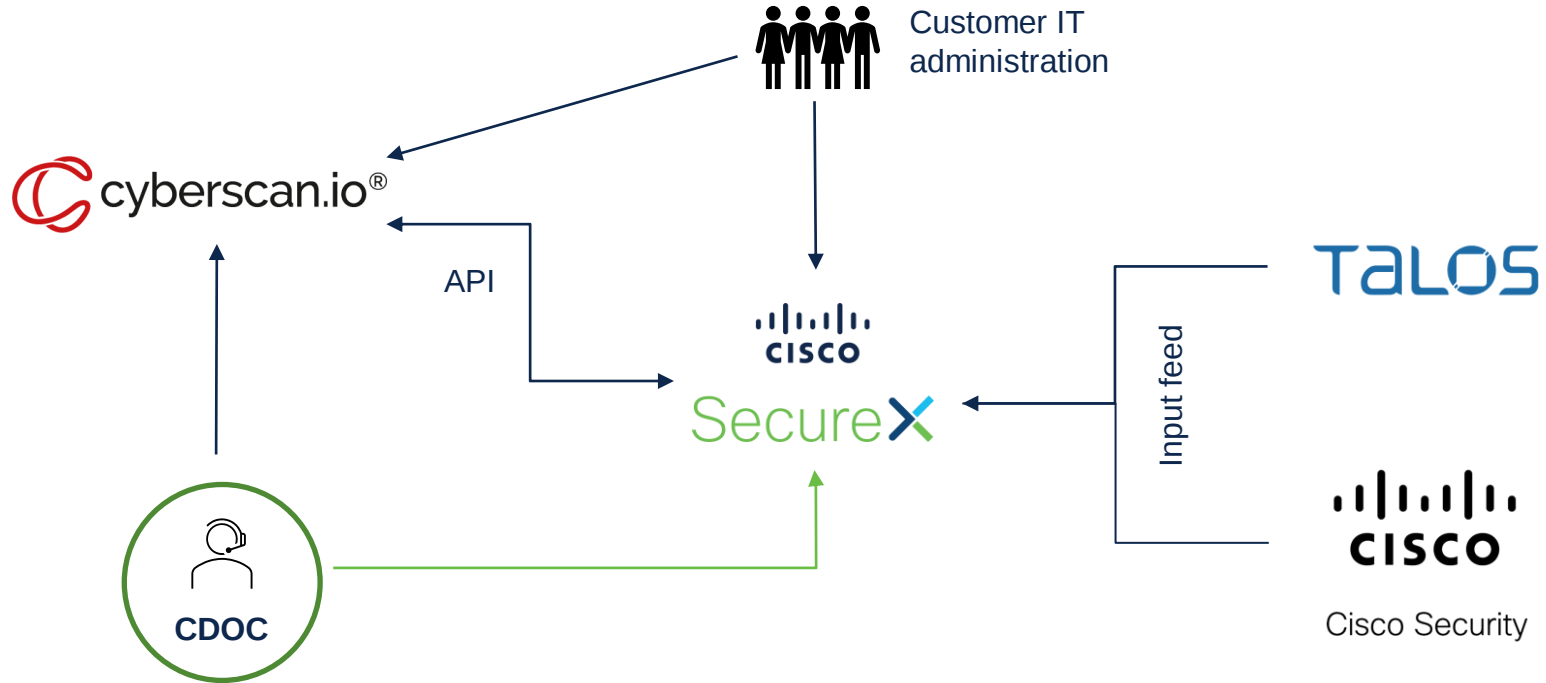


# Kontinuierliche Angriffserkennung und -reaktion



... und wer könnte das für  
mich tun und mich  
lediglich informieren,  
wenn ich  
Handlungsbedarf habe?

# Cyber Defense Operations Center der DGC





Halle 7A  
Stand A-418



Halle 7  
Stand 447

