



IT Security

the new normal in the digital
society

Moritz Wenz

Cisco Systems

Advanced Threat Solutions



before we start



CISCO  SEC

everything becomes digital



UBER

Ride

Drive

Cities

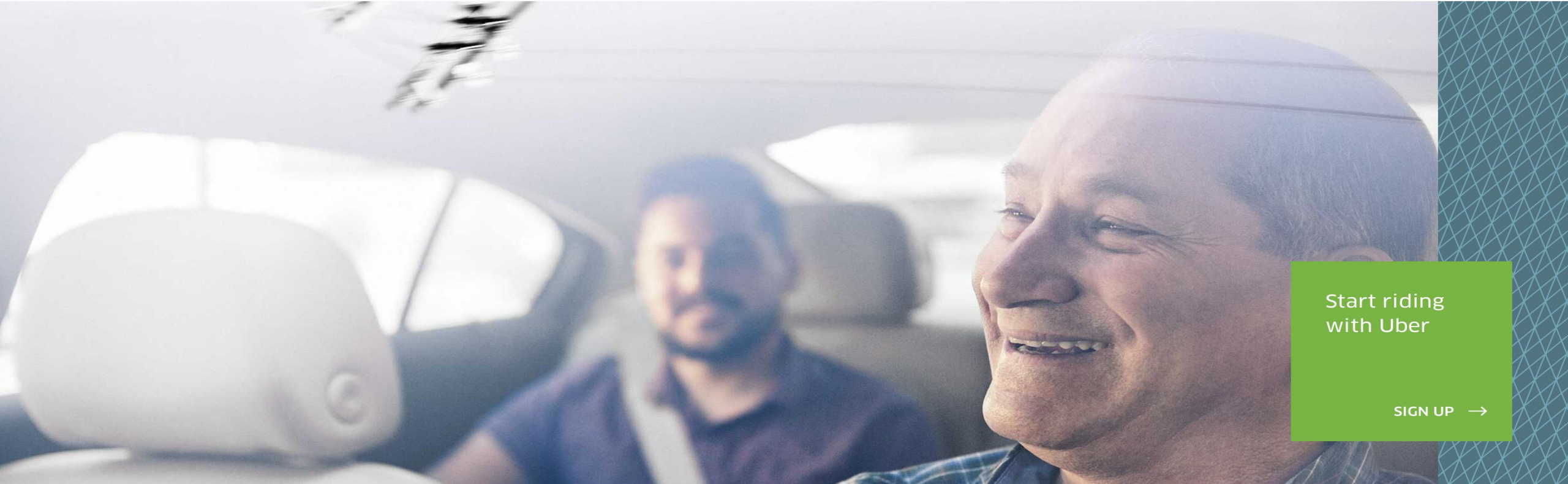
HELP

SIGN IN

BECOME A PARTNER

Get there

Your day belongs to you



Start riding
with Uber

SIGN UP →

how we make experiences



Jetzt Gastgeber werden

Reisen

Nachrichten •

Hilfe

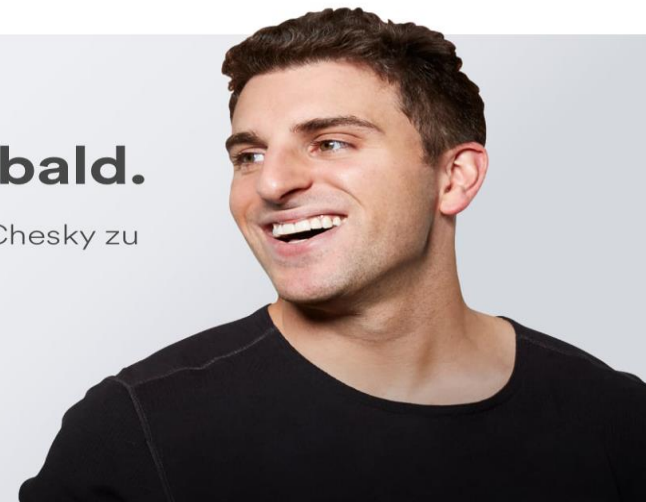
Sei dort zuhause. Buche einzigartige Unterkünfte und erlebe die Stadt wie ein Einheimischer.

Wo Reiseziel, Stadt, Adresse	Wann Check-in → Check-out	Gäste 1 Gast	Suche
---------------------------------	------------------------------	-----------------	-------

Das nächste Abenteuer startet bald.

Schau am 17. November vorbei, um von unserem CEO Brian Chesky zu hören, wie die Reise weitergeht.

Erinnert mich dran



Our live and how we see data privacy



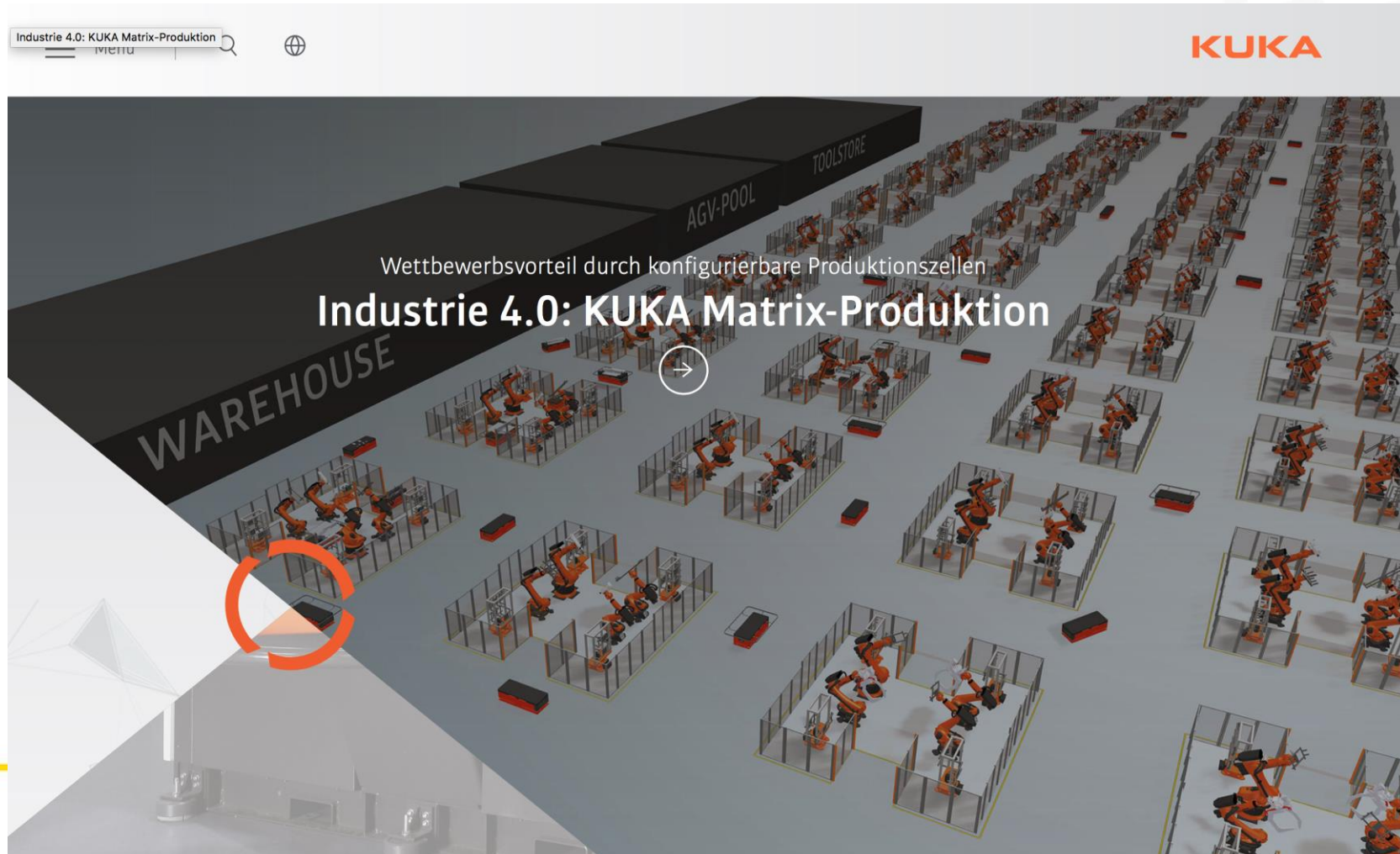
Deutsch English (UK) Español Français (France) 中文(简体) العربية Portuguese (Brasil) Italiano 한국어 हिन्दी 日本語 +

Registrieren Anmelden Messenger Facebook Lite Handy Freunde finden Banner Nutzer Seiten Orte Spiele
Standorte Stars Gruppen Momente Instagram Über uns Werbeanzeige erstellen Seite erstellen Entwickler Karriere Datenschutz
Cookies Datenschutzhilfe Impressum/Nutzungsbedingungen Hilfe

Facebook © 2016



How we produce



THE POWER OF AUTOMATION



Everything becomes programmable



A screenshot of a printer's control interface. On the left is a "Menu" with options: Printer status, Utilities, AirPrint settings, Google Cloud Print setup, Firmware update, and Manual (Online). On the right is the "Printer status" section, which shows "Ready to print." and "Estimated ink levels" for Magenta (M), Black (BK), Yellow (Y), PGBK, and Cyan (C), each with a corresponding colored bar.



State of Emergency



National Vulnerability Database

Current amount of CVEs: 80110

So lets accept two things

1. There is no perfect software and there will be „never“ one
2. Attackers will find new vulnerabilities and use them

Different actors

1. States and Intelligence Agencies
2. Criminal organizations
3. Hacktivists
4. Several more



Go to Market



1. SaaS (Malware tools, DDoS,...)
2. Ransomware (not new but with Bitcoin...)
3. CyberWeapons Dealer (Vupen, Hacking Team,..)
4. Credit Card Data
5. Fraud
6. ...

How it works




Shodan Developers Book View All...

SHODAN Adria airways Explore Enterprise Access Contact Us

Exploits Maps

TOP COUNTRIES



Slovenia 2

TOP ORGANIZATIONS

Telekom Slovenije d.d. 2

Total results: 2

195.88.82.214
Telekom Slovenije d.d.
Added on 2016-11-02 23:41:18 GMT
 Slovenia
[Details](#)

SSL Certificate

Issued By:
|- Common Name: **iRoseCA**
|- Organization: **i-Rose d.o.o.**

Issued To:
|- Common Name: ***.msp.telekom.si**
|- Organization: **i-Rose d.o.o.**

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters
Fingerprint: nginx/Hardcoded 1024-bit prime

HTTP/1.1 401 Unauthorized
Server: openresty/1.9.7.3
Date: Wed, 02 Nov 2016 23:41:03 GMT
Content-Length: 0
Connection: keep-alive
SPRequestGuid: 38f6d0d6-2192-42a3-b9f5-ac121972b9dd
WWW-Authenticate: Basic realm="adria-airways-tehnika.msp.lan"
X-Powered-By: ASP.NET
MicrosoftSharePointTeamS...

195.88.82.229
Telekom Slovenije d.d.
Added on 2016-10-22 13:10:52 GMT
 Slovenia
[Details](#)

SSL Certificate

Issued By:
|- Common Name: **iRoseCA**
|- Organization: **i-Rose d.o.o.**

Issued To:
|- Common Name: ***.msp-test.telekom.si**
|- Organization: **i-Rose d.o.o.**

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 401 Unauthorized
Server: openresty/1.9.7.1
Date: Sat, 22 Oct 2016 13:10:39 GMT
Content-Length: 0
Connection: keep-alive
SPRequestGuid: 21441434-c96b-409b-be0f-7bae563345a1
WWW-Authenticate: Basic realm="adria-airways-tehnika-test.msp.lan"
X-Powered-By: ASP.NET
MicrosoftSharePoint...

SEC

How it works



Version 1.9.15.1 - 3 June 2016

CVE-ID

CVE-2016-4450

[Learn more at National Vulnerability Database \(NVD\)](#)

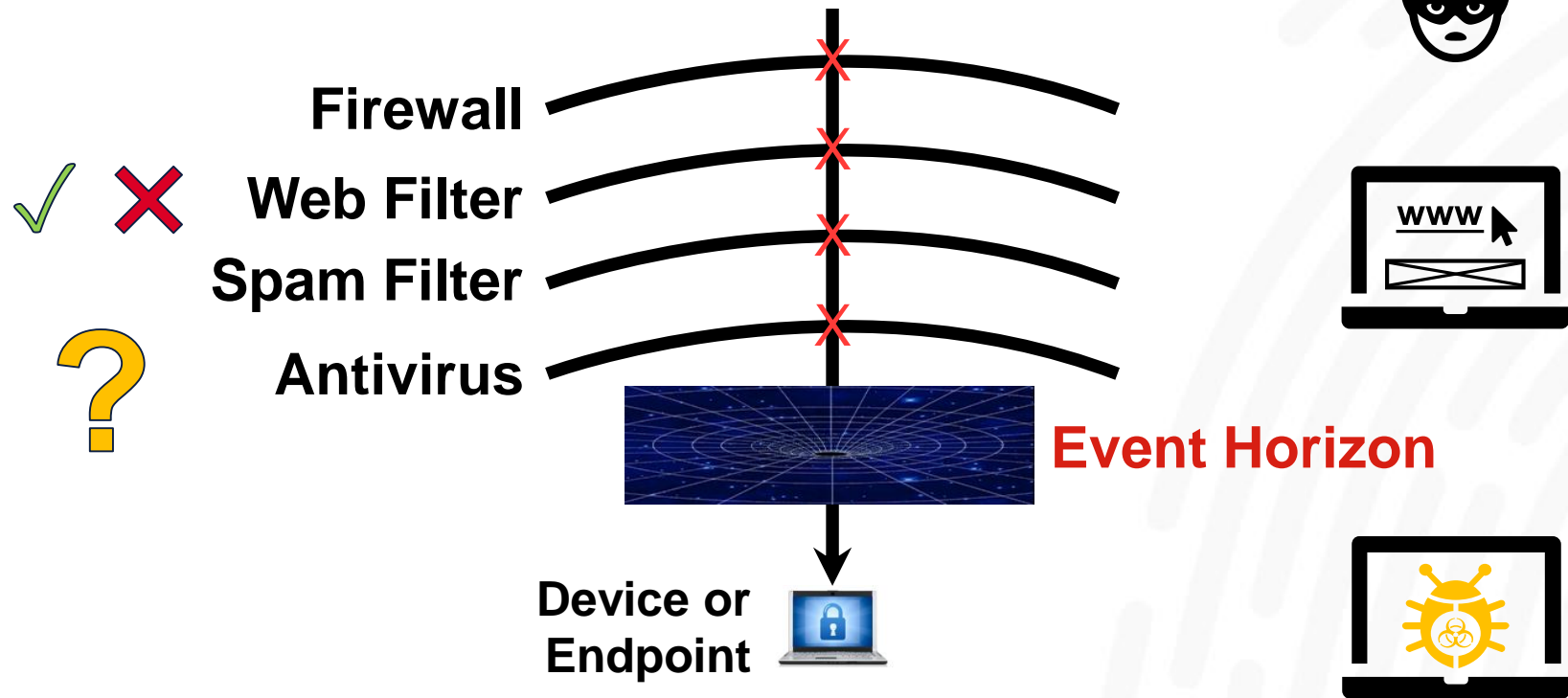
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

os/unix/nginx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.

- feature: added restydoc documentation indexes for the official [nginx](#) core and most of the official openresty components.

Defence in depth is broken





So we are screwed right ?



We are coming a long way



CISCO  SEC

What we are doing



Worldwide [change] | Log In | Account | Register | My Cisco

Products & Services | Support | How to Buy | Training & Events | Partners

Trust and Transparency Center

Overview | Trust Principles | Built-in Security | Data Protection | Transparency and Validation

Cisco 2016 Midyear Cybersecurity Report

Get new threat intelligence and trend analysis.

[Download Now](#)

Protection From Cyberattacks

Cisco's holistic approach to security and trust. (PDF - 514 KB)

[Read At-A-Glance](#)

News

[Connectivity at What Cost?](#)
Involving citizens in digital transformation

[Preparing to Act Fast when Disaster Strikes](#)

Featured Content

[Cisco 2016 Midyear Cybersecurity Report: Executive Perspectives - Video \(8:16 min\)](#)

[Unified Security Metrics - Whitepaper \(PDF - 10 KB\)](#)

[Data Breaches: Protect Your Organization with an Incident Response Program - Whitepaper \(PDF - 10 KB\)](#)

[Cisco Spark Security and Privacy - Whitepaper \(PDF - 700KB\)](#)

[Cisco IT and InfoSec Partner to Protect Infrastructure and Data - Case Study](#)

[Security and Trust in the Age of Digitization - Video](#)

Overview

The Cisco Trust and Transparency Center is dedicated to providing you with the information, resources and answers to your cybersecurity questions that help you manage risk.

At Cisco, we believe security is everyone's business. We are accountable for trustworthy product development, value chain security, customer data protection, and transparency that earn the verifiable trust of our customers, partners, shareholders and employees.

Trustworthy, Transparent and Accountable

See our trust principles and learn about our commitment to maintaining strong protections for our customers, products and company.

Security from Development to Service

Understand how we build security into everything we do.

Data Protection and Privacy

Learn about our data protection program and privacy policy.

Transparency Report

See law enforcement requests for customer data.





SOFTWARE



COMMUNITY



VULNERABILITY REPORTS



ADDITIONAL RESOURCES

TALOS



ABOUT TALOS



JOIN OUR TEAM



CONTACT US



BLOG

We Keep Your Network Safe.

Talos is the industry-leading threat intelligence organization. We detect and correlate threats in real time using the largest threat detection network in the world to protect against known and emerging cyber security threats to better protect your organization.



TALOS BLOG

CRASHING STACKS WITHOUT SQUISHING BUGS: ADVANCED VULNERABILITY ANALYSIS

NOVEMBER 15, 2016 6:29 PM

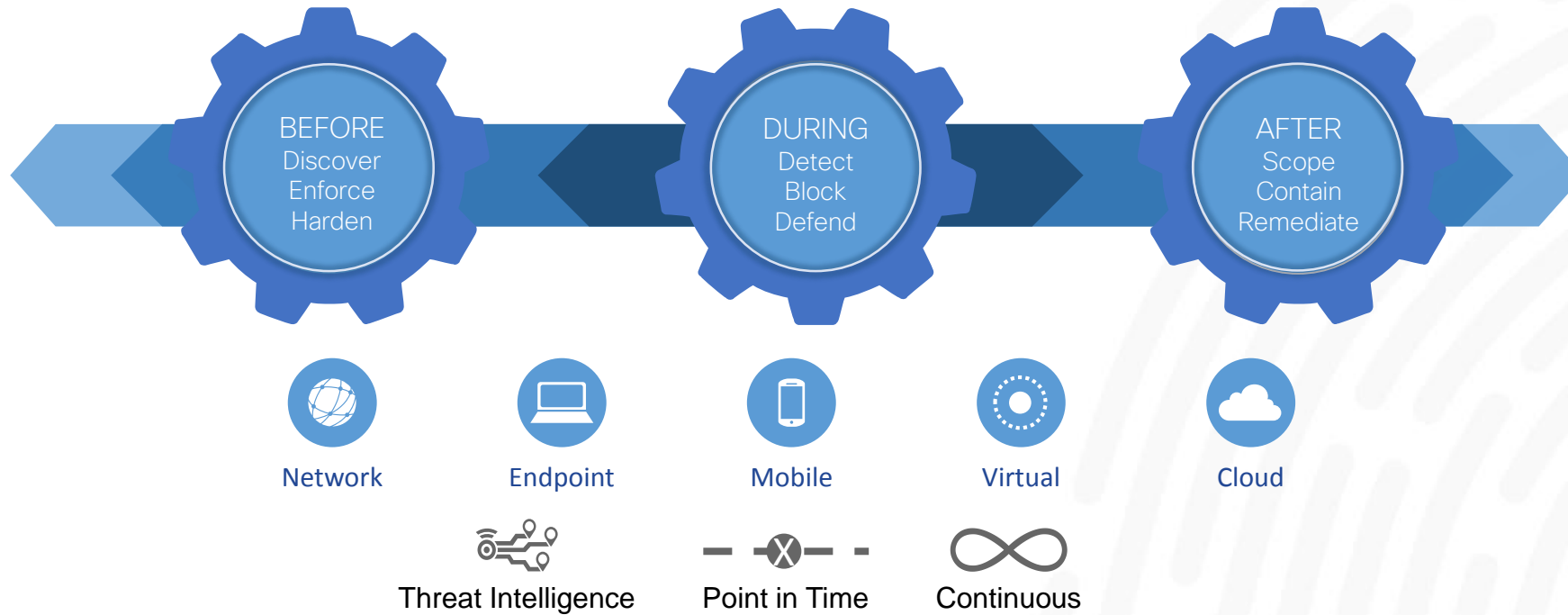
HOLGER UNTERBRINK

This post is authored by Marcin Noga with contributions by Holger Unterbrink

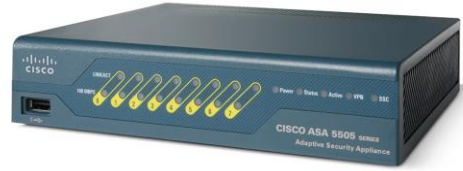
OVERVIEW

Crash triaging can be a long and complicated process; by using proper tools and having an optimal approach, we can make this a bit easier and less time consuming. In this post we describe a triaging strategy and toolset based on two examples of vulnerability classes:

We are coming a long way



New approaches



Lancope®



SOURCEfire®



CloudLock



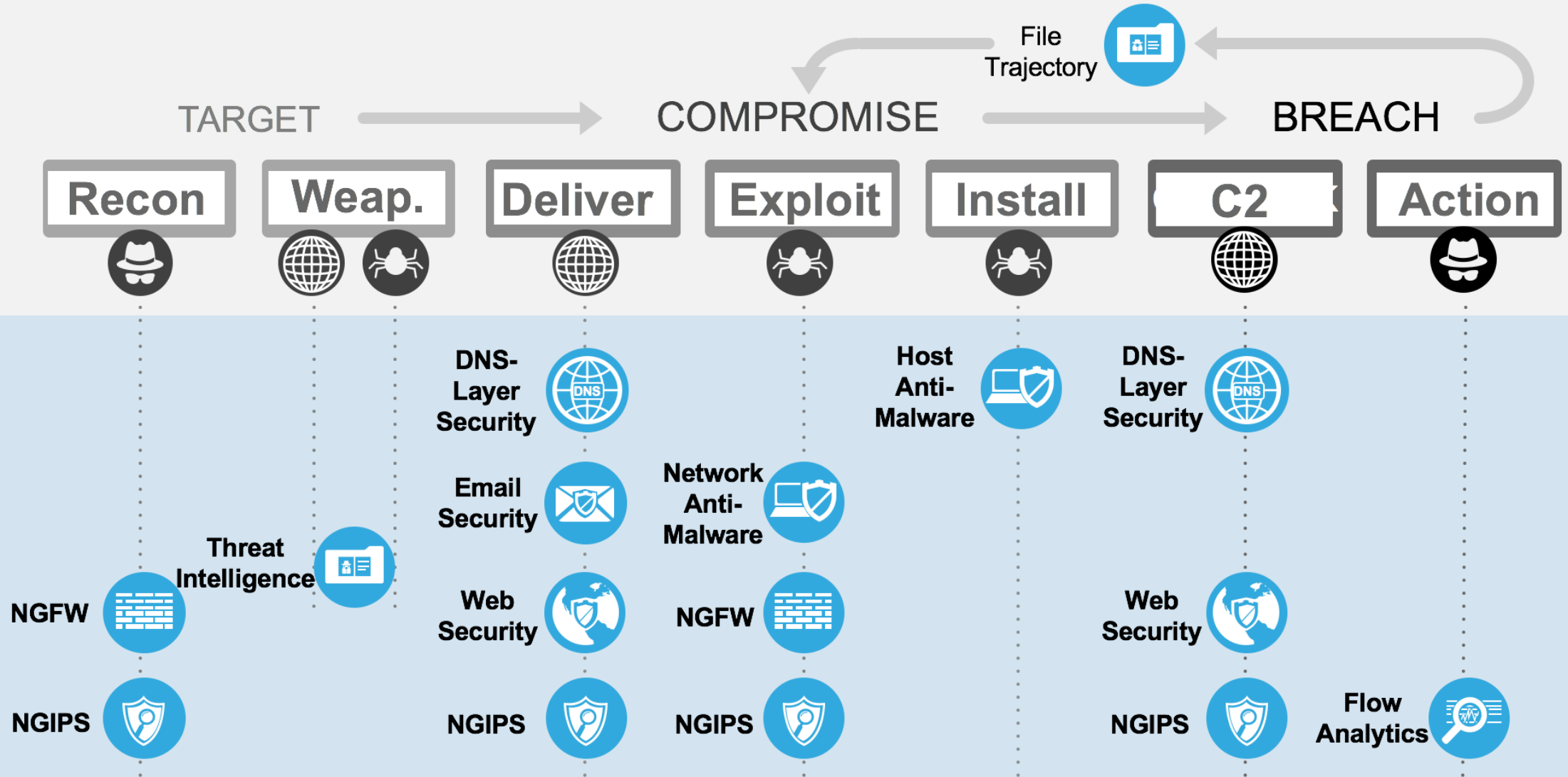
CISCO  SEC

End-to-End "Kill Chain" Defense Infrastructure

 **INFRASTRUCTURE**
USED BY ATTACKER

 **ATTACKER**

 **FILES/PAYLOADS**
USED BY ATTACKER





Thank you

Moritz Wenz
Cisco Systems
mwenz@cisco.com

