

HARTMANN



Secure Network Services at HARTMANN GROUP

Security über DNS – in der Praxis

Stefan Staub
DDI User Group

About me

Stefan Staub

Senior Manager Security & LAN

Paul Hartmann AG

im Unternehmen seit 1999



Agenda

- Introduction HARTMANN GROUP
- Why IT Security
- Is DNS a risk?
- DNS Security Challenges
- Time Travel to Secure Network Services
- BloxOne Threat Defense in action

HARTMANN at a glance



Global footprint

in more than 30 countries



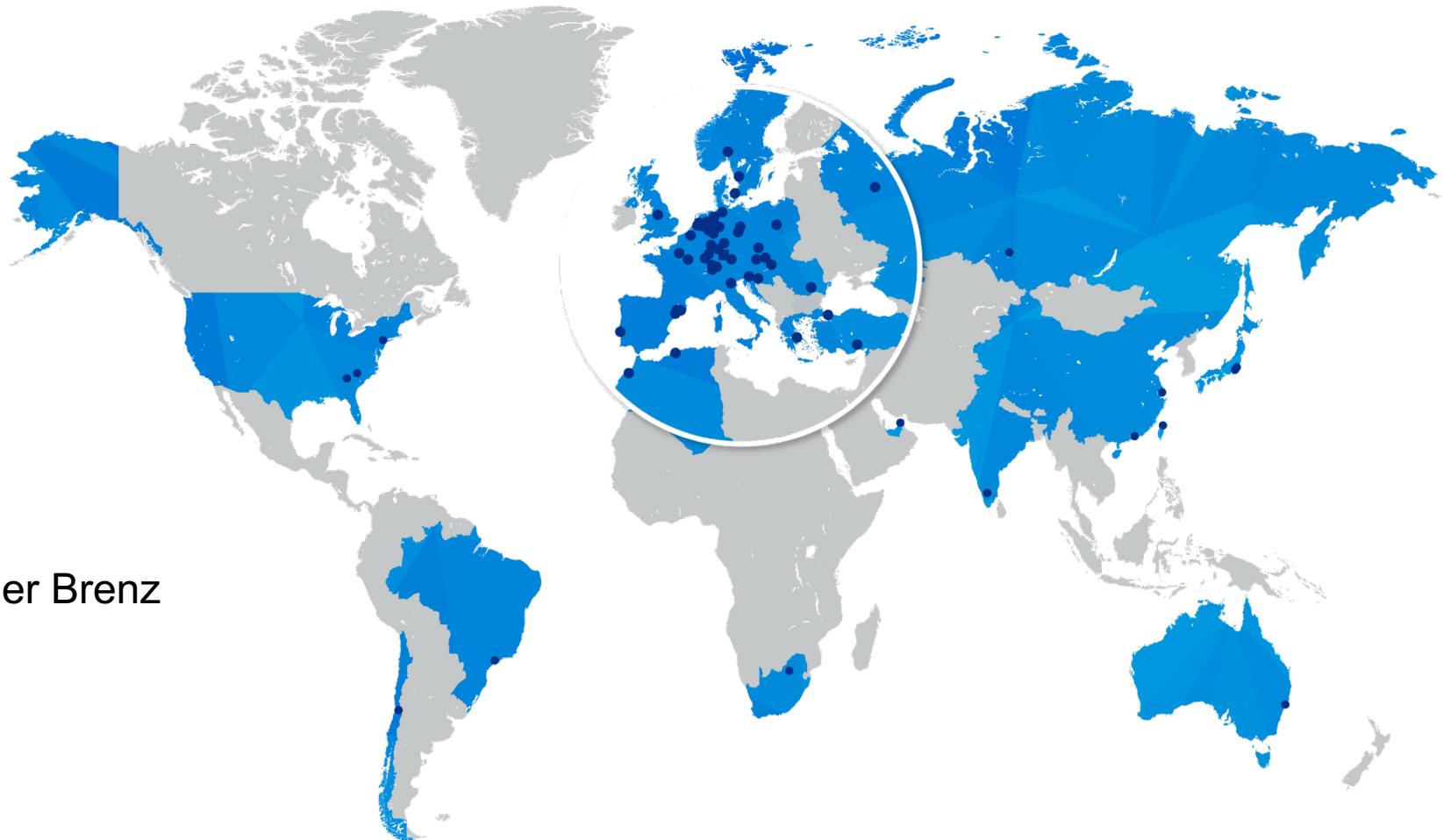
€ 2.43 bn

global sales



11,000+

employees worldwide



Divisions of HARTMANN



Why IT Security?

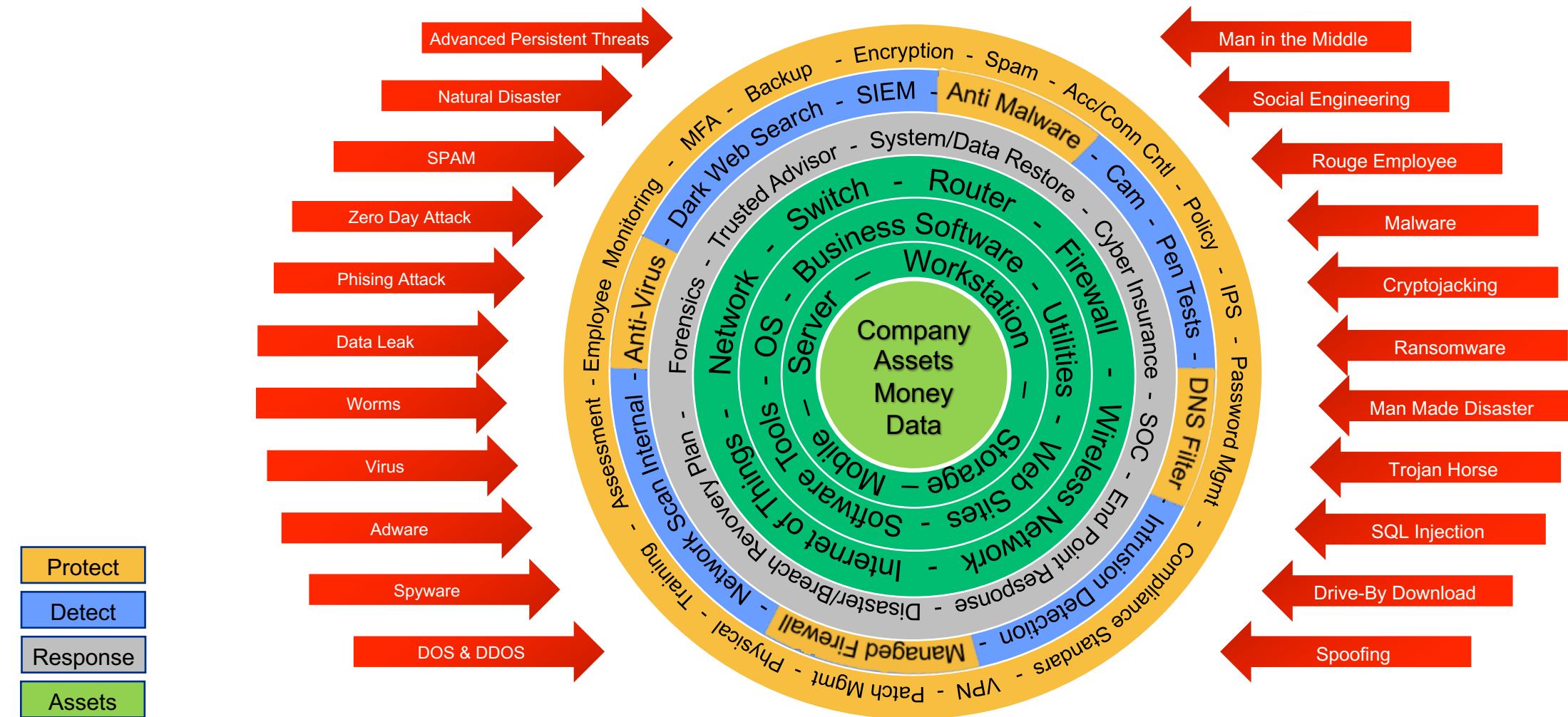
- Protection of confidential data
- Pricing data
- Protection of know-how
- Competitive position of company
- Legal requirements
- Customer satisfaction

We worry about **security** when...



...we have **something of value** and there is a **risk it could be harmed**.

Layers of IT Security



Technical IT Security

- Firewalls



- Web-Security



- Network Services



- E-Mail Security



- Malware Protection



Technical IT Security at Hartmann

- **Firewalls (Check Point)**



Hits	Source	Destination	Services & Applications	Action
686M	de-fra-gba-01 de-hei-ddi-12 de-fra-nsm-12	* Any	dns	Accept

- **Web-Security (Zscaler)**



Rule Name	Criteria	Action	Description
x-any-x_001	NETWORK SERVICES DNS SOURCE IP GROUPS ipg_xx-yyy_lan_10.0.0.0-8	Allow	DNS Traffic

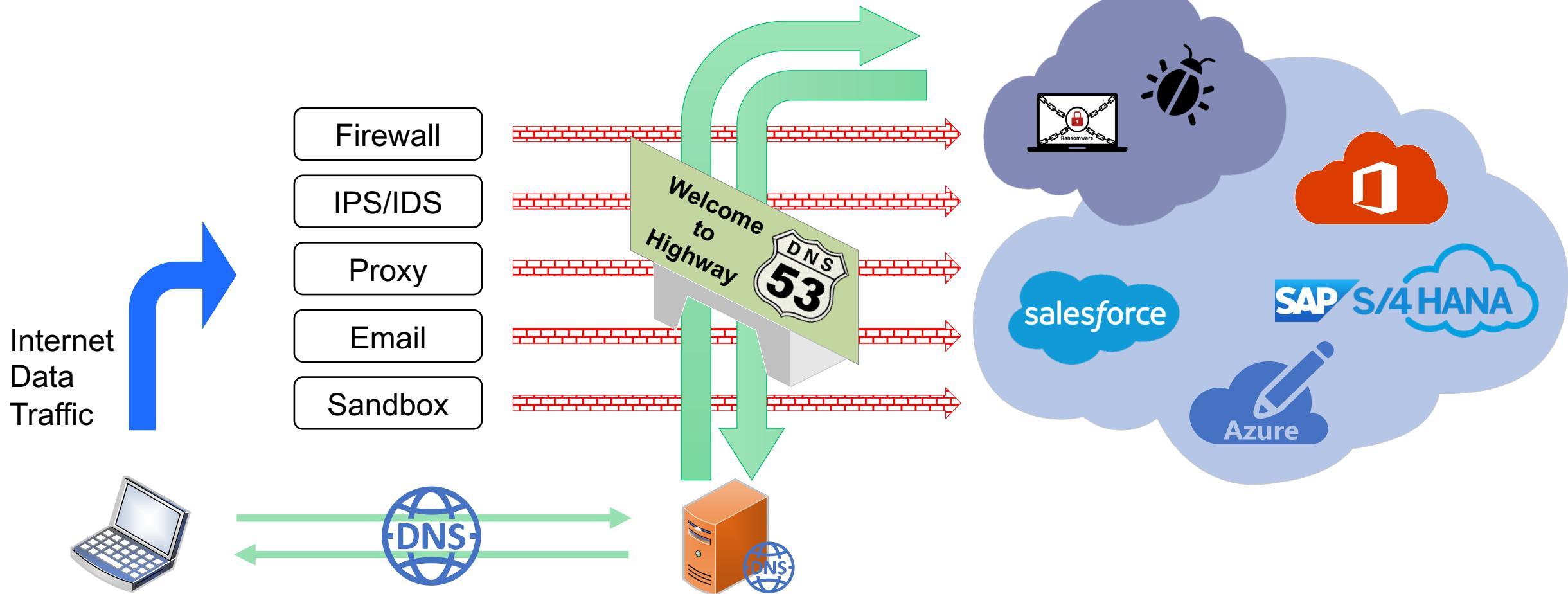
- **Network Services**

Network Service DNS

- **DNS is a critical infrastructure service**
- E-Mails, Business Applications and Websites dependent on DNS
- DNS traffic is not inspected from Firewalls, IDS and Proxies
- 79% of companies worldwide suffer from DNS attacks¹
- Risk of data loss, service downtime and image damage
 - European DSGVO imposes the „guarantee of secure storage of data“
- DNS is the gateway to any corporate network
- Average cost per DNS attack in USA ~ 780.000 €¹

¹ StealthLabs, *Cybersecurity: DNS Attacks Cost USD 924,000 on Average*,
<https://www.stealthlabs.com/news/cybersecurity-dns-attacks-cost-usd-924000-on-average/>, 20.06.2020

Is DNS a Risk?



Definition of a Risk

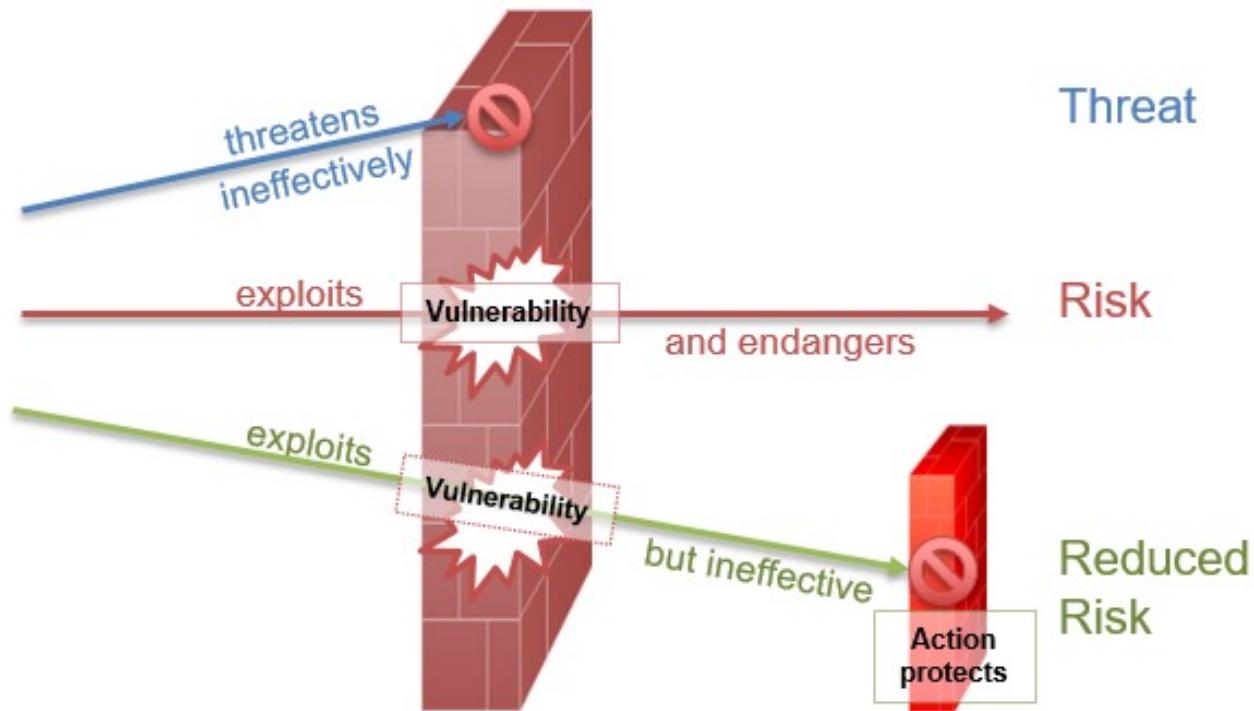


Illustration: Veranschaulichung, „Bedrohung“, „Schwachstelle“, Gefährdung“, „Risiko“ und „Maßnahme“.
Source: Based on BSI, 2011, Page 21.

DNS Security Challenges

1. Stopping APTs, Malware & Botnet communication from using DNS

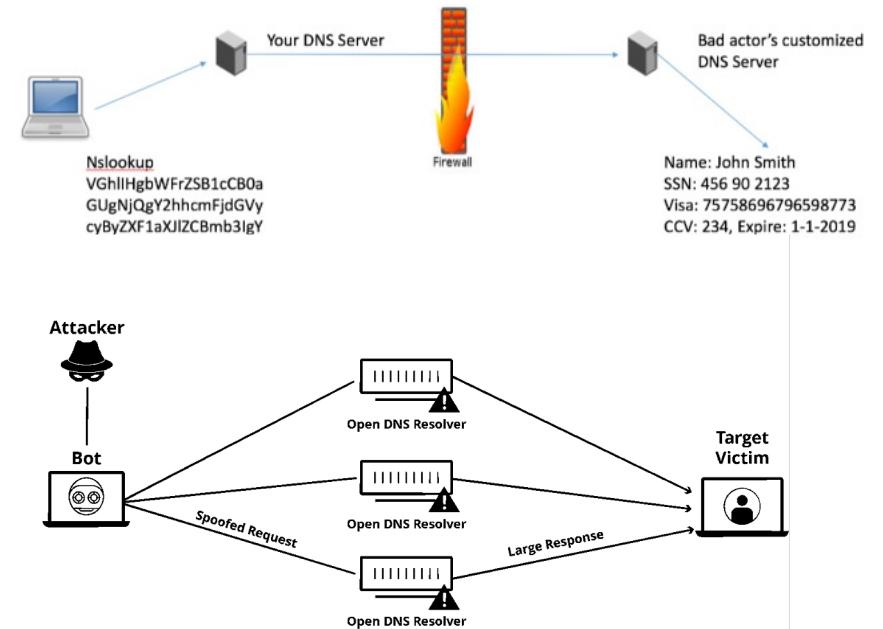
- Recursive

2. Preventing data exfiltration & DNS Tunneling

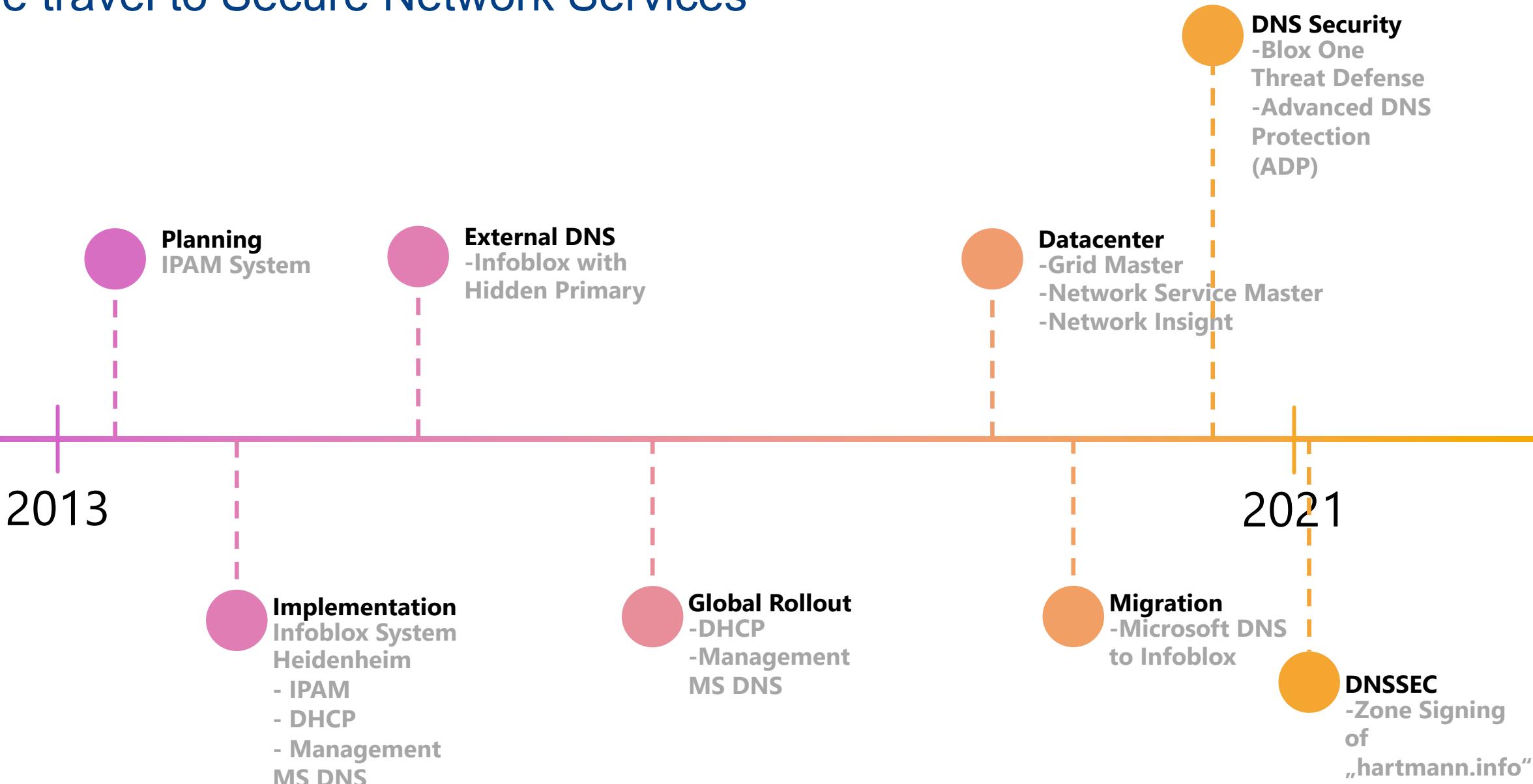
- Recursive

3. Defending against DNS DDOS & Hijacking attacks

- Authoritative + Recursive



Time travel to Secure Network Services



BloxOne Threat Defense in action

Conficker Case

- first finding directly after forwarding traffic
- One source IP tried to communicate with Malicious destinations

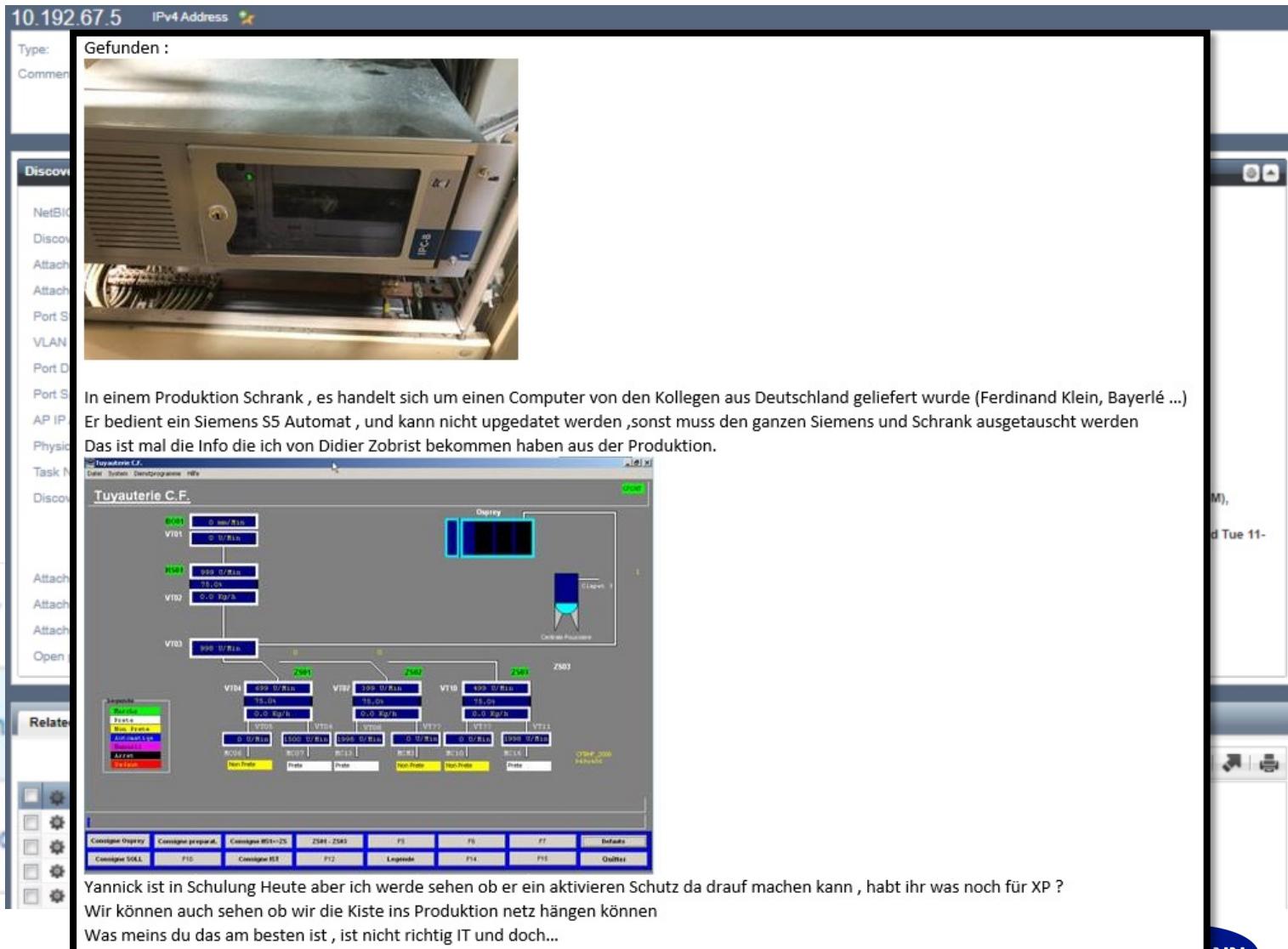
DETECTED

ACTION ▾

QUERY

01-22-2020 08:24:51 am CET Log

01-22-2020 08:24:51 am CET Log

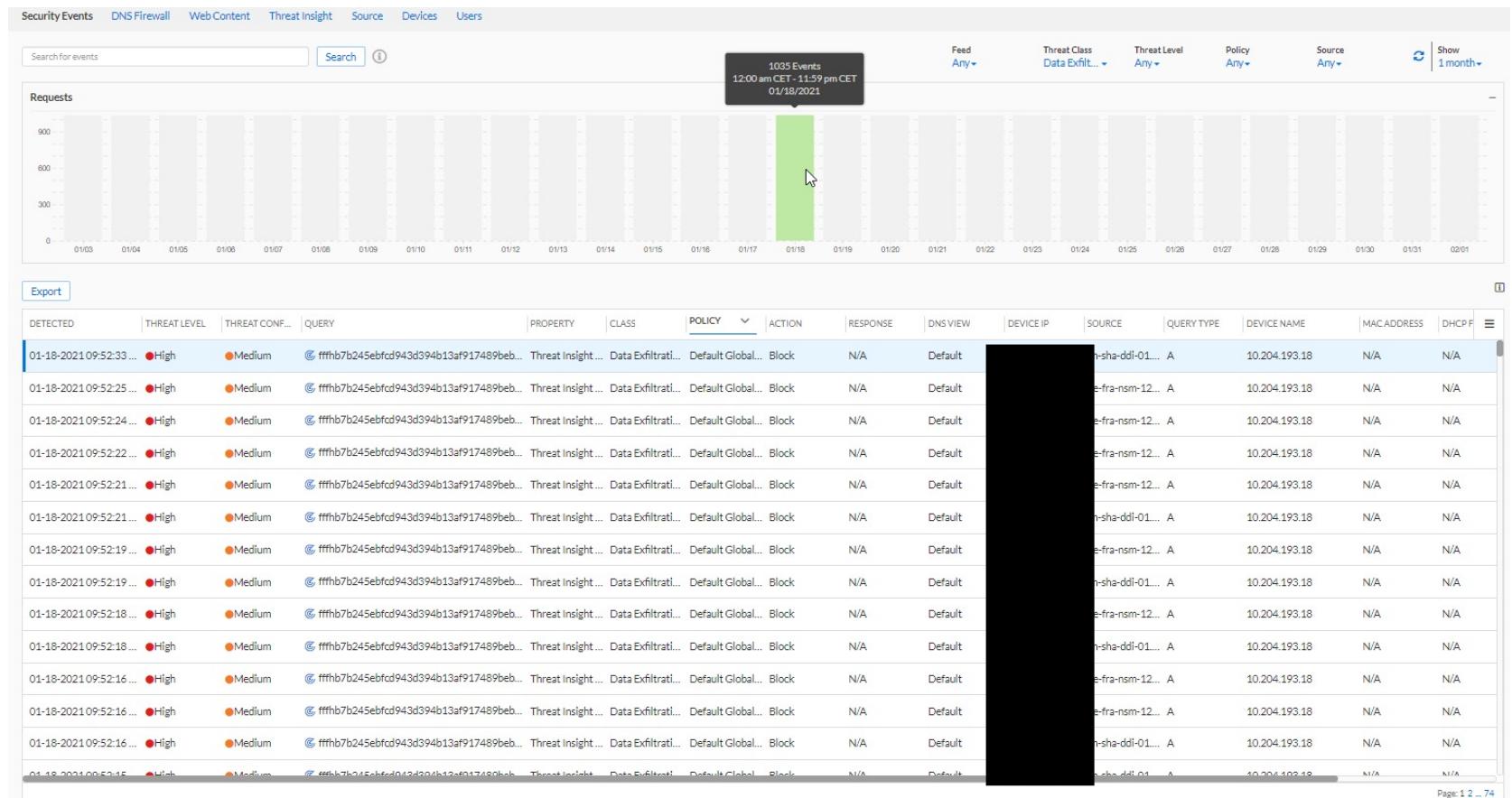


BloxOne Threat Defense in action

Data Exfiltration Case

- One source IP was sending tons of dns requests

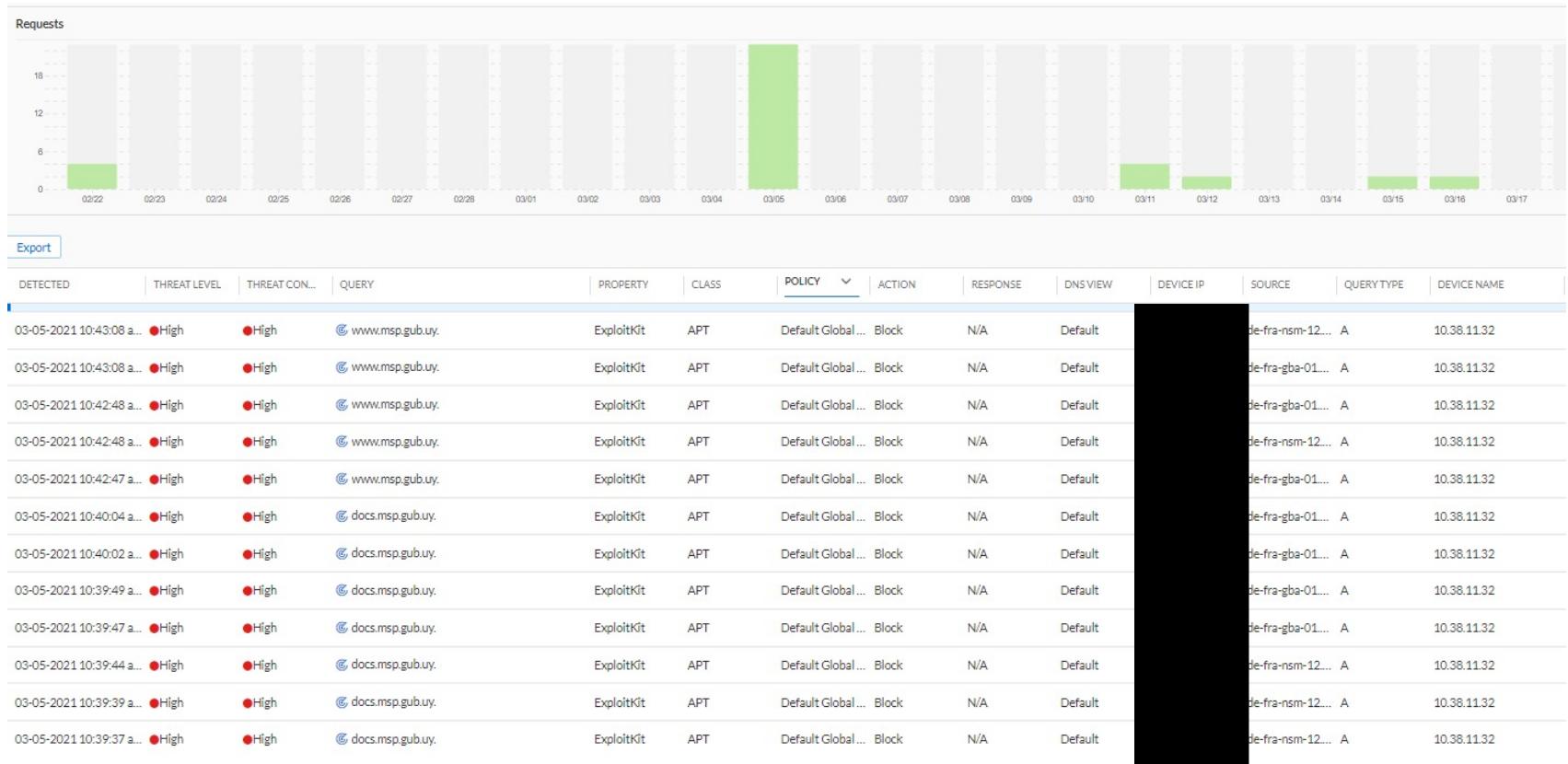
ffffb7b245ebfd943d394b13af917489bebhub9qxfvow55v65q6.f
fgj.hbpu.cwkeji.cn.



BloxOne Threat Defense in action

APT Case

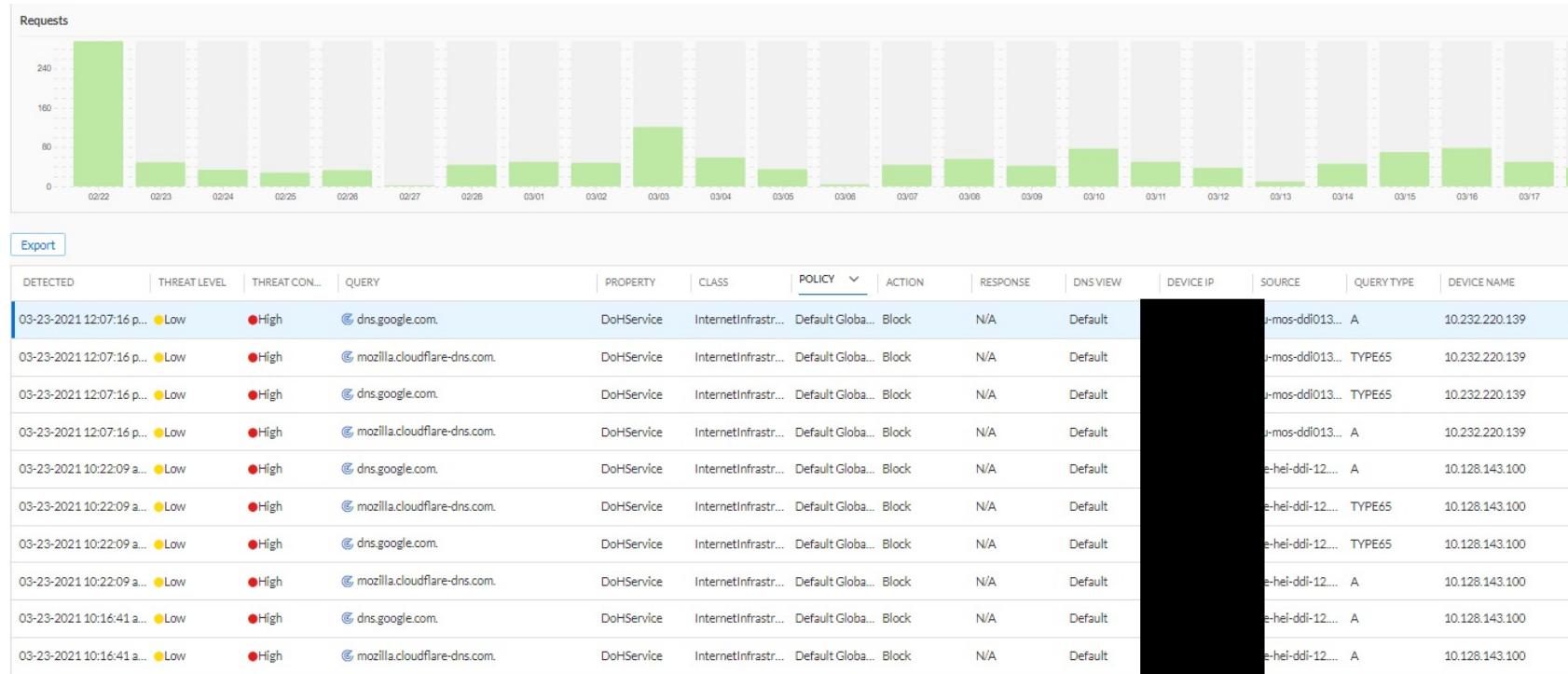
- One source IP tried to communicate to malicious destination



BloxOne Threat Defense in action

Public DoH (DNS over HTTPS)

- Some browsers (mostly Firefox) which are trying to use DoH and public DNS servers



New Technical Security

- E-Mail Security
- Firewall
- Web Security
- Malware Security
- Secure Network Services

Availability

Confidentiality

Integrity

Quote

„Trusting Infoblox was one of the best decisions of the past decade. The Grid technology is reliable and the base of bringing insight, availability and security into our network services.“

- Stefan Staub



Vielen Dank.

Haben Sie Fragen?

