infoblox®

The Power of DNS in Security

DNS Detection & Response
IT/OT Convergence

“

With DNS-based Threat Intelligence and IPAM we can map a threat to any device and user activity in **real time**.

EMEA-based tech services company

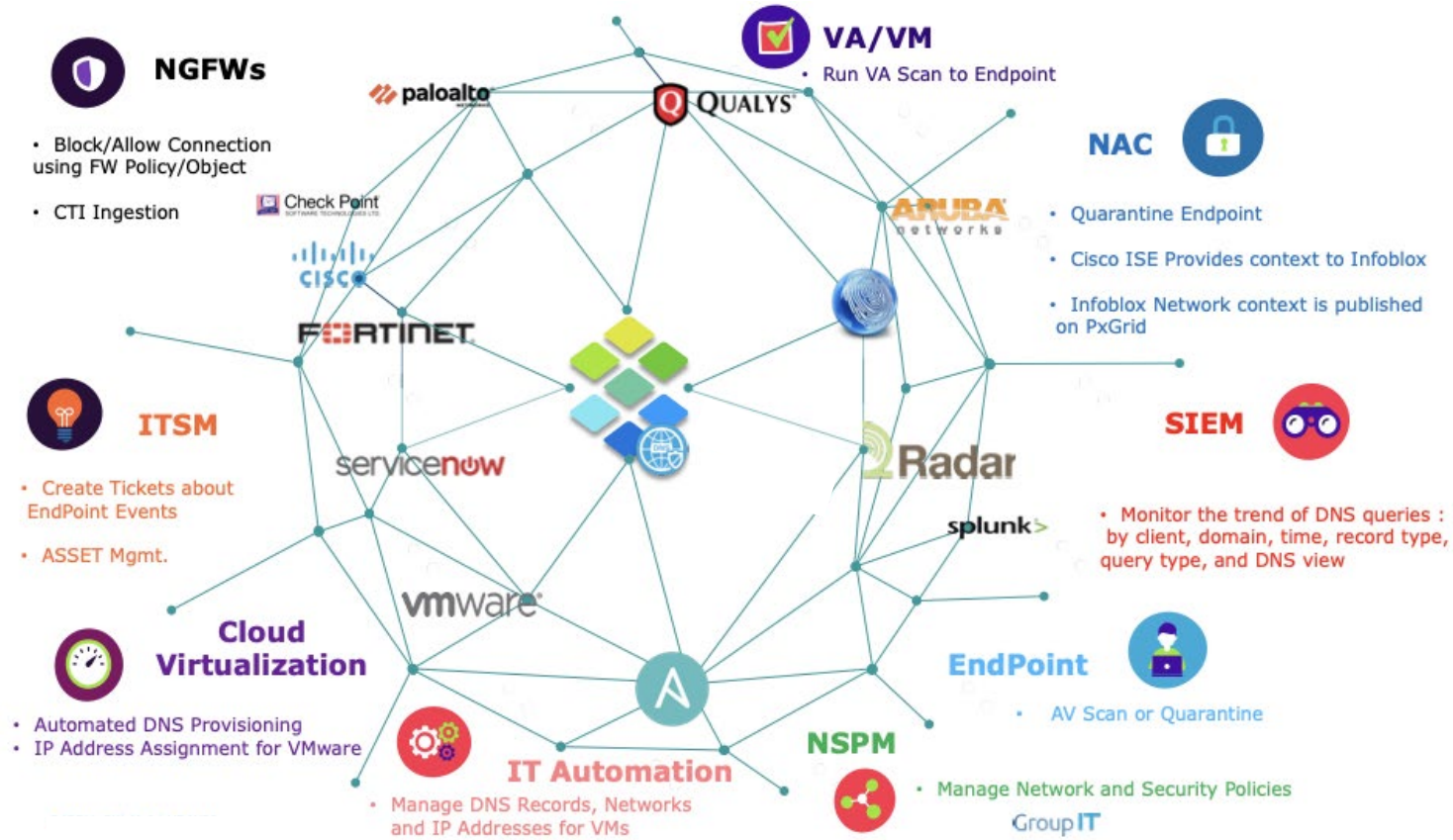
”

infoblox.

Infoblox at the heart of a SecOps Framework

- EMEA tech services company.
- **50,000** (roaming) endpoints.
- **500000** security events per day.
- Changed DNS to the 1st line of defense - on the **DNS server**!
- Correlate Threat, Device, OS, User and Location in **real time**.

API integration into Threat Intelligence, SIEM and SOAR to **Automate Response**.



infoblox.

Who is Infoblox? - Products

BloxOne - Threat Defense

NIOS DDI
BloxOne DDI

The foundation of **Core Network Services** that enables and protects all communications over an IP-based network

infoblox.

infoblox

Relevance of DNS within Security


.tk second largest country domain behind China

Humans cannot keep up with the load

Infoblox Customer TRAFFIC example

- 78% of DNS traffic came from **20** domains (0,026%)
- Remaining 22% of DNS traffic from **76,000** domains (99,97%)

TIME to investigate

- At 1 domain per minute, it would take a person 52 days to research these domains
- Today, ~100,000 new domains have already been created so far, which adds another 10 weeks.

infoblox.

Attackers know DNS is unmonitored

Firewall
Web Security
Email Security
Endpoint Security
Network Security
SSE/CASB/SWG/SASE
DLP

infoblox

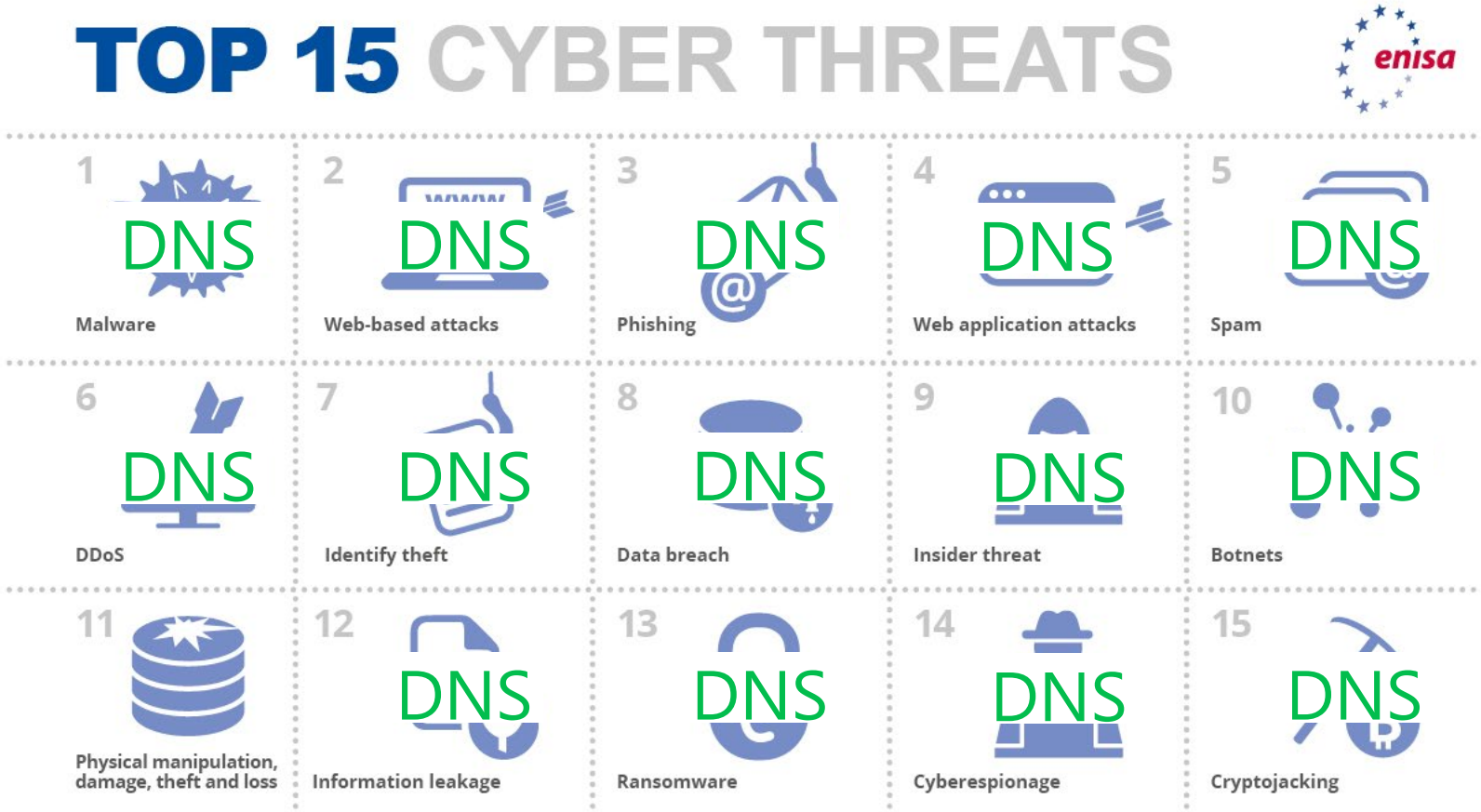
Gartner, CISA, ENISA (EU Agency for Cybersecurity)

Exponential Increase in the use of DNS in all Type of Attacks

DNS is seen as the most scalable approach to malware mitigation in a deperimeterized security world[2/3].

Gartner

How can Organizations use DNS to improve their security posture?[1]



infoblox.

Infoblox – NIST Framework Core

DNS Detection & Response (DNSDR)

Map threats to any device and user activity in near real time

BloxOne - Threat Defense

NIOS DDI BloxOne DDI

Exfiltration, etc.

infoblox®

THANK YOU!

Ben Polak
Sebastian Hein
DACH-Team @ Infoblox

Ben Polak
Accountmanager DACH
m +49 176 32 44 44 62
bpolak@infoblox.com

Sebastian Hein
Solution Architect DACH
m +49 151 17 60 47 71
shein@infoblox.com