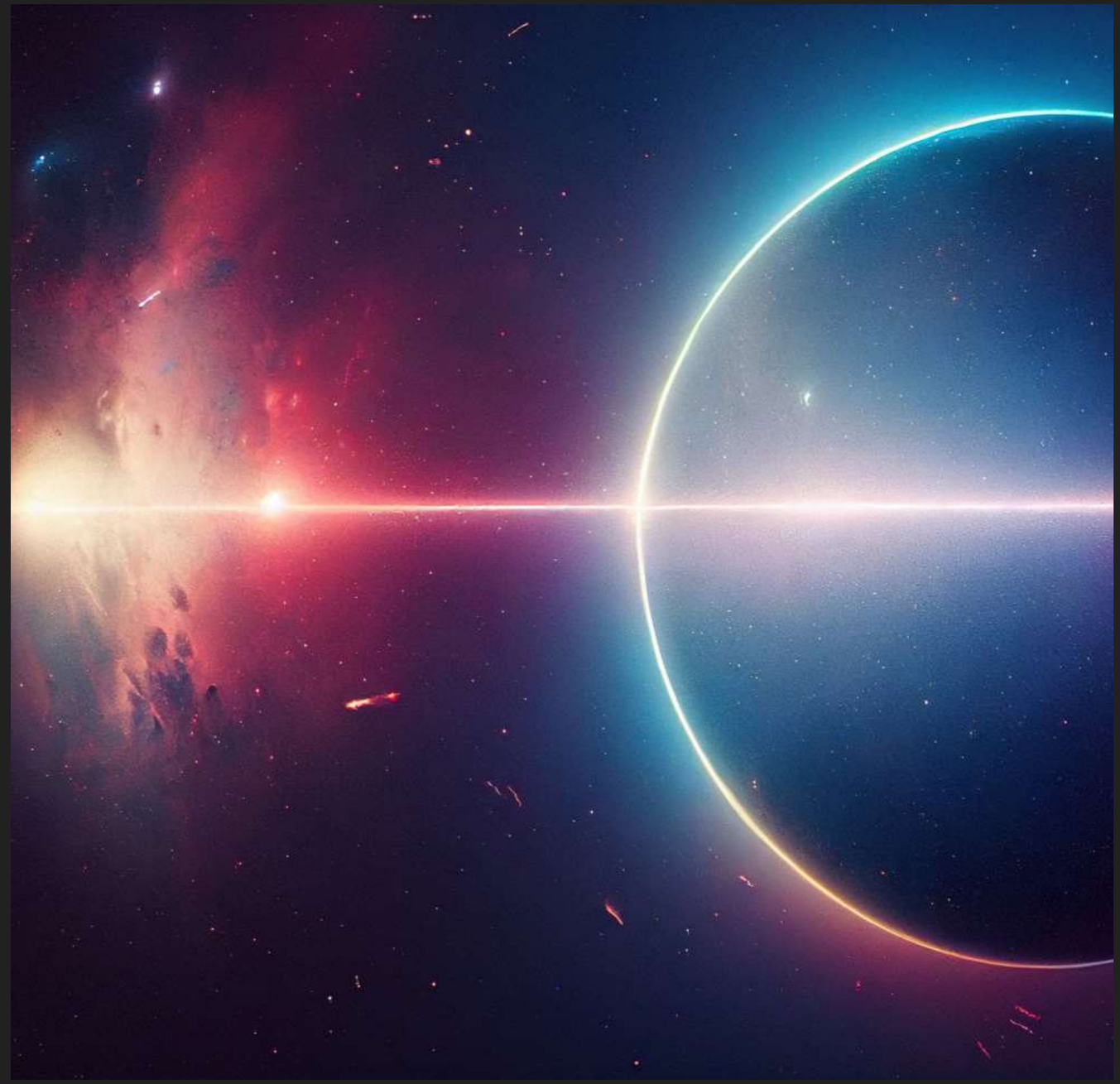
# How to Make DNS Threat Intelligence a Real Game-Changer For Your Network Security



itsa EXPO CONGRESS

**October-2023**

**Bernd WILHELM**
Customer Solution Architect

efficient iP®

# Speaker

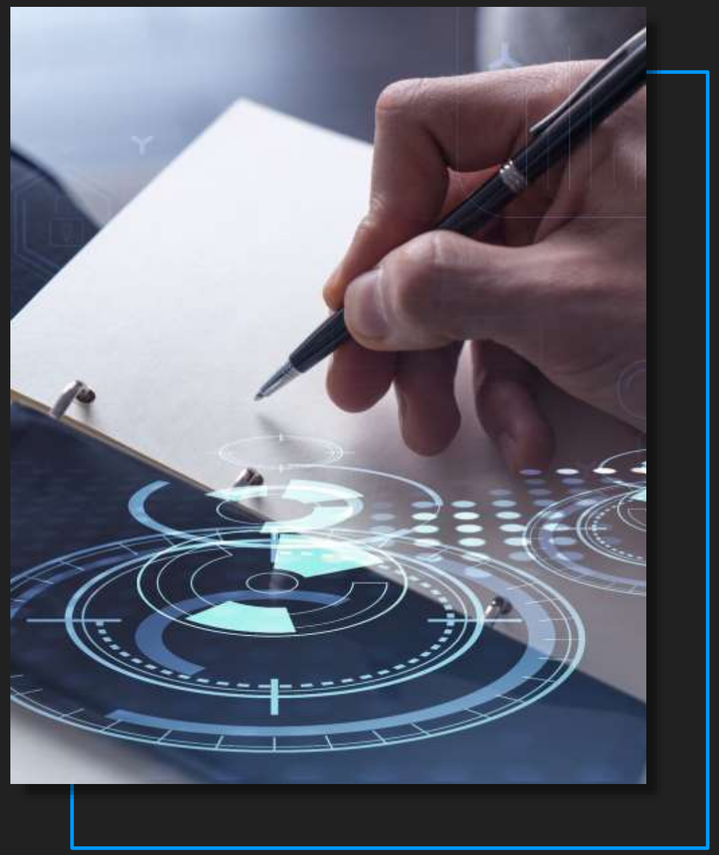
bw@efficientip.com

Bernd WILHELM

Customer Solution Architect - DACH

Bernd is currently the CSA for EfficientIP in DACH+ and has worked in the DDI and IT-Security space for 27+  years.

# Agenda



- Setting The Scene
- Why a DNS-Centric Threat Intelligence
- Why DNS Data is Essential
- How to Use it Efficiently
- Key Takeaways

# Setting The Scene

efficient iP®

# Cyber Threat Landscape Is Constantly Evolving

**+38%**

**Cyberattacks in 2022[1], 1B Malware[2], 40M Ransomware attacks per month[3], 4M+ Phishing in 2022[4]**

**$1.1M**

**Average Cost of DNS-based Attack[5]**

**66%**

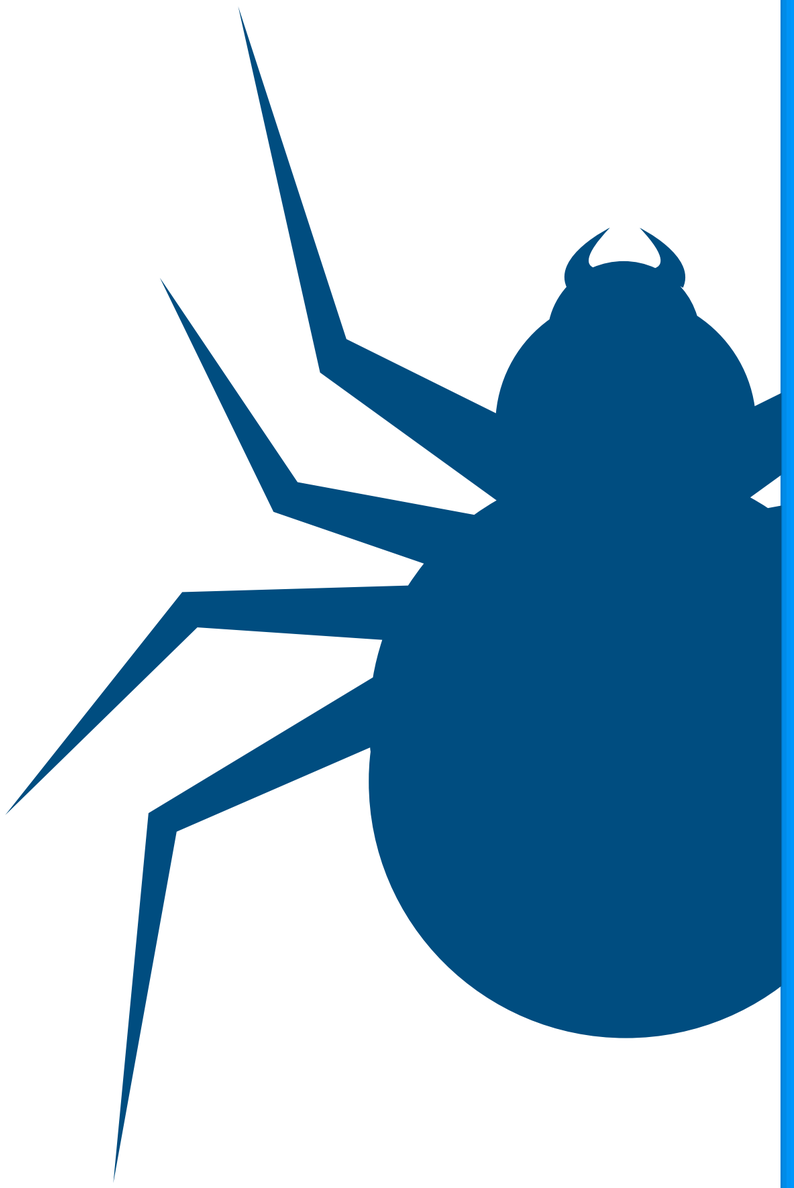
**CIOs mentioned cyber and information security as a top area of increased investment for 2023[6]**

1. *23 Cybersecurity statistics to lose sleep over in 2023 – TechTarget*
2. *AV-Test Institute*
3. *SonicWall's 2022 mid-year report*
4. *Anti Phishing Working Group*
5. *IDC 2023 Global DNS Threat Report*
6. *Emerging Technologies: Critical Insights for Threat Intelligence Demand - Gartner*

# DNS-Based Attacks Are Prominent

- DNS is an open service by essence and widely used by cyber criminals:
  **85% of malware actors are using DNS to develop their attack.**

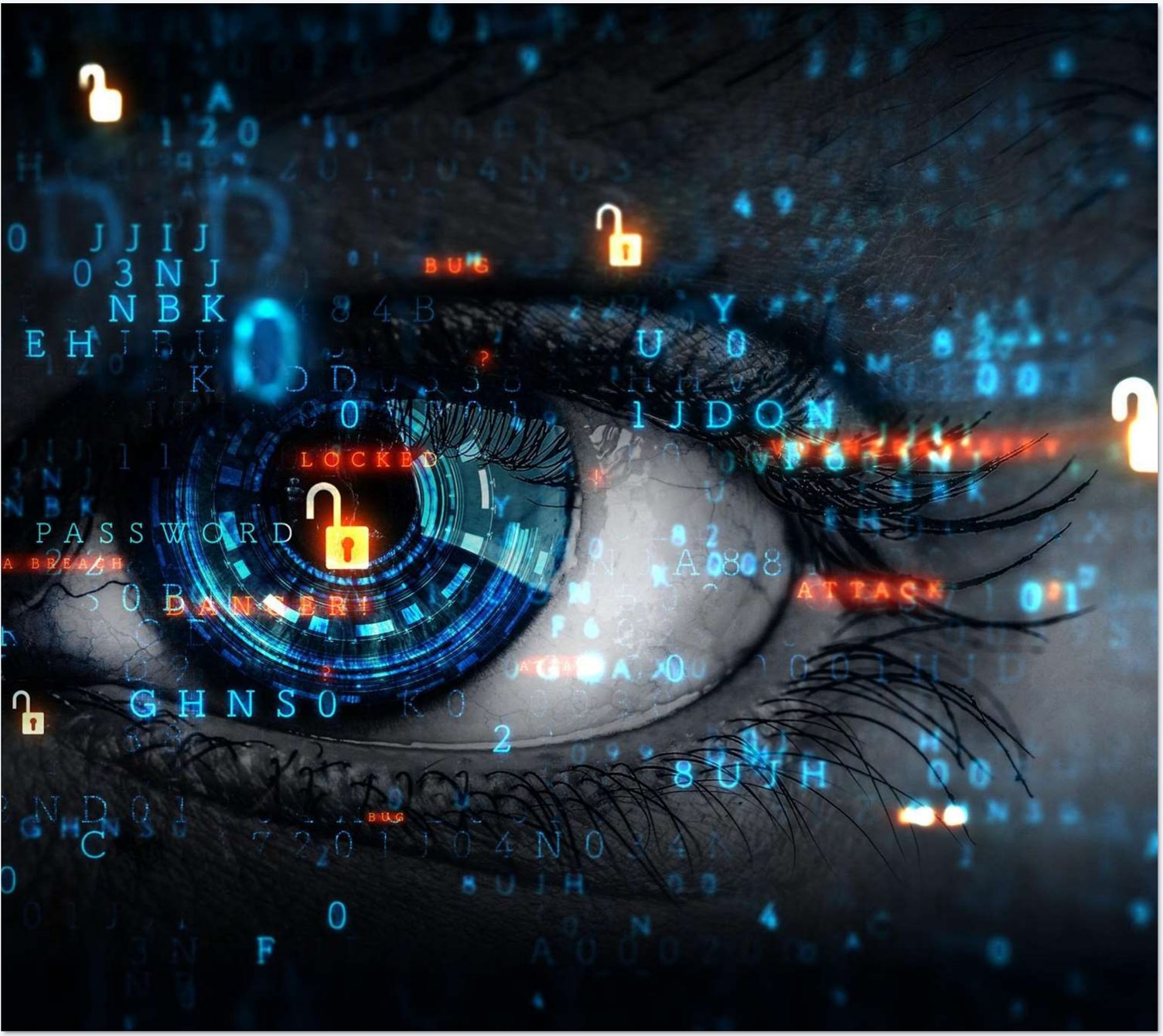
- **2023 IDC DNS Threat Report** shows that organizations have suffered significantly from DNS-based attacks

*Source: IDC 2023 Global DNS Threat Report*

# Why a DNS-Centric Threat Intelligence

efficient iP®




# Threat Intelligence Has Emerged as Critical

**60% of organizations consider it vital to company defense against cyberattacks**

# Why a DNS-Centric Threat Intelligence

- A DNS-centric Threat Intelligence will improve mitigation of attacks:

**Top 3 attack types benefiting from threat intelligence for mitigation:**

**57%** DNS-based malware

**55%** Phishing

**51%** Ransomware

- DNS data is currently underutilized

**36%** don't collect or analyze their DNS data. DNS traffic analysis can provide many benefits: early detection of threats, real-time threat intelligence, proactive threat hunting, improved incident response, and better visibility into network activity.

**79%** do not yet make use of DNS data as a source for threat intelligence.

*Source: IDC 2023 Global DNS Threat Report*

***A DNS-Centric Threat Intelligence is required to face the challenge of ever-evolving DNS threats***

# Why DNS Data Is Essential

efficient iP®

# The Value Brought by DNS Traffic Data

## Coverage

Comprehensive real-time DNS traffic data collection at a global scale across any device, network, application, and user

## Intelligence

Data analysis, curation, and classification leveraging leading-edge AI technology and pioneering algorithms to generate insightful analytics

## Reliability

Continuous data processing to ensure data is always up-to-date, relevant, and accurate

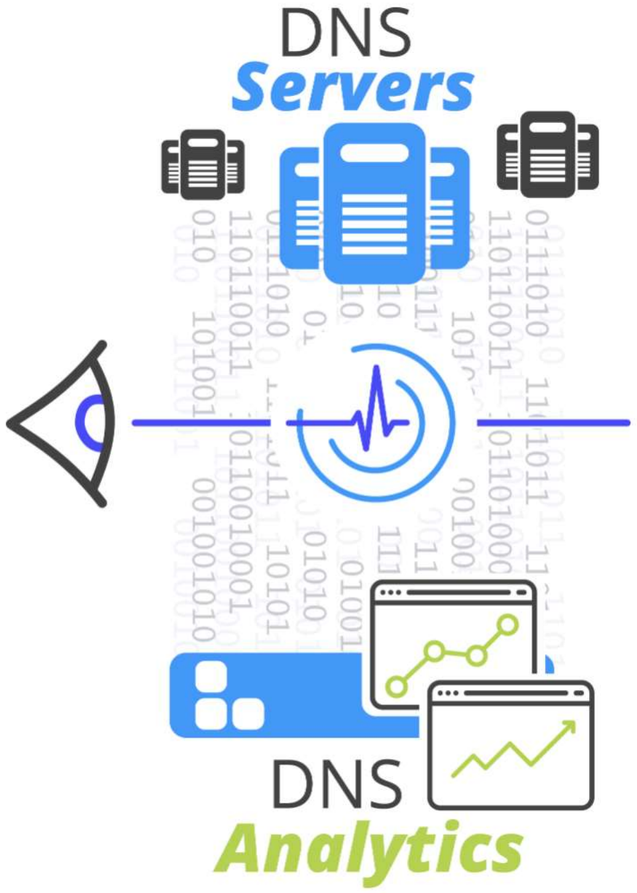
## Visibility

DNS traffic analysis and insights enable to view what is happening on networks and identify traffic anomalies

# Quick Wins To Use DNS Data Efficiently

efficient iP®

# 1. Use a DNS-Centric Threat Intelligence Feed



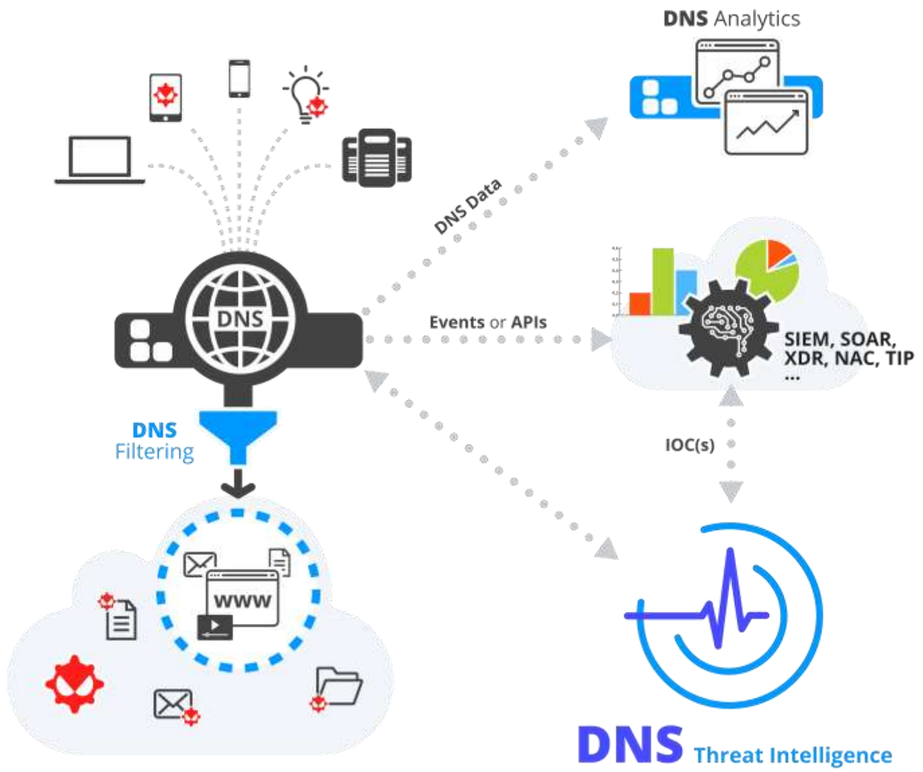

- A DNS Threat Intelligence feed is a no brainer
- Leverage comprehensive, accurate, and up-to-date list of malicious domain names to immediately block DNS queries to these domains before they are resolved for proactive defense
- Apply AI-powered algorithm to early detect threats such as Domain Generated Algorithms (DGA) and phishing

# 2. Visualize Contextual DNS Data and Analytics


- Detect threats in your networks by matching DNS Threat Intelligence feed with your DNS traffic providing contextual information to accelerate threat investigation and remediation
- Investigate Domain Names with Indicators of Compromise (IoCs) and Risk Scoring to accelerate threat detection
- Fuel DNS Threat Intelligence Feed with findings for strengthened protection

# 3. Build an End-to-End Holistic DNS Security Infrastructure

- Integrated DNS Threat Intelligence in the Security Ecosystem thanks to high-performance APIs or Events
- Automate Security Events for Accelerated and Efficient Threat Investigation and Remediation



# Key Takeaways

efficient iP®

# Key Takeaways

- A DNS-Centric Threat Intelligence is required to face the challenge of threat landscape expansion
- Use insightful and valuable DNS Data to build a DNS-Centric Threat Intelligence
- Integrate DNS-Centric Threat Intelligence with your security ecosystem to build a more holistic security infrastructure, and accelerate threat detection and remediation

**DNS Threat Intelligence** can help IT Leaders evolve into a more holistic and consolidated security infrastructure to **increase security, gain agility and resilience, and reduce complexity**.

# Questions?

**Bernd WILHELM**

Customer Solutions Architect

bernd.wilhelm@efficientip.com

efficient iP®

# EfficientIP In Brief

**DDI**
Network Automation
& Security Company

**110+**
Countries

App & infrastructure
Life-Cycle Automation

Intelligent App Traffic Steering

Adaptive DNS security

Open
Ecosystem
Integration

***Vision:***
**Make Networking Simple & Secure Everywhere**
**Deliver the Best User Experience at all Times**

HQ

***USA*** - Philadelphia

***EMEA*** – Paris

***APAC*** - Singapore

**1000+**
Customers in
All Industries

***Improve*** Efficiency

***Reduce*** Risks

***Lower*** Costs


For more information, visit

www.efficientip.com and follow @efficientip on Twitter.

efficient iP®