# Cybersecurity Incident – Sind sie gut vorbereitet?

Christian Koch (NTT DATA)

Senior Vice President Cybersecurity – IoT/OT-Security, Innovations & Business Development

15.10.2025

# Highlights of NTT DATA Cybersecurity

## Recognition

**#2**

by revenue in Gartner® Market Share Analysis: Managed Security Services, Worldwide, 2024

**Source: Gartner® Market Share Analysis: Managed Security Services, Worldwide, 2024 – Published May 2025*

**Leader & Rising Star**

in Everest Group's Managed Detection and Response (MDR) Services PEAK Matrix® Assessment 2025

**Source: IT Managed Security Services (MSS) PEAK Matrix® Assessment 2024 – March 2025*

## Global Partnerships

**132**

Partners & solutions suite support with strong partner ecosystem

**37,400+**

Vendor certifications

**40%+**

Global Threat Intelligence – Analytics of over 40% of the global internet traffic in NTT backbone

## Community

**7,500+**

Global Cybersecurity specialists

**350+**

Local Cybersecurity specialists in DACH

ISACA

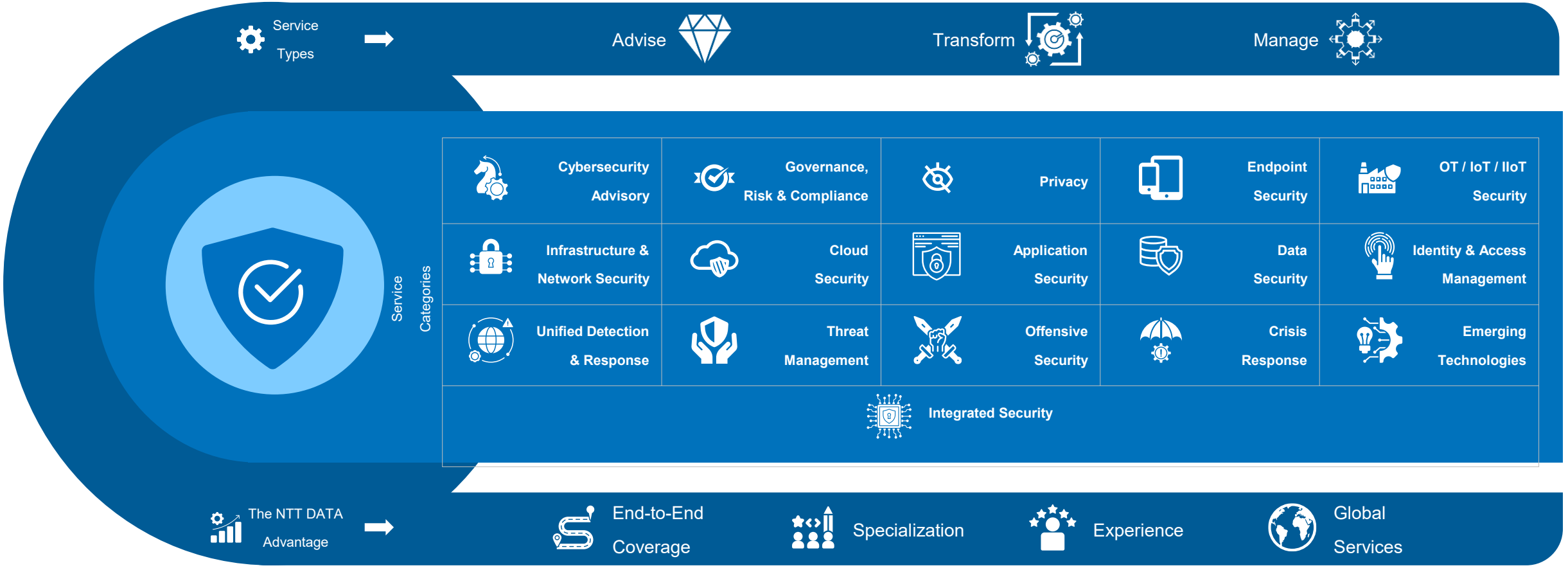
CSA cloud security alliance®



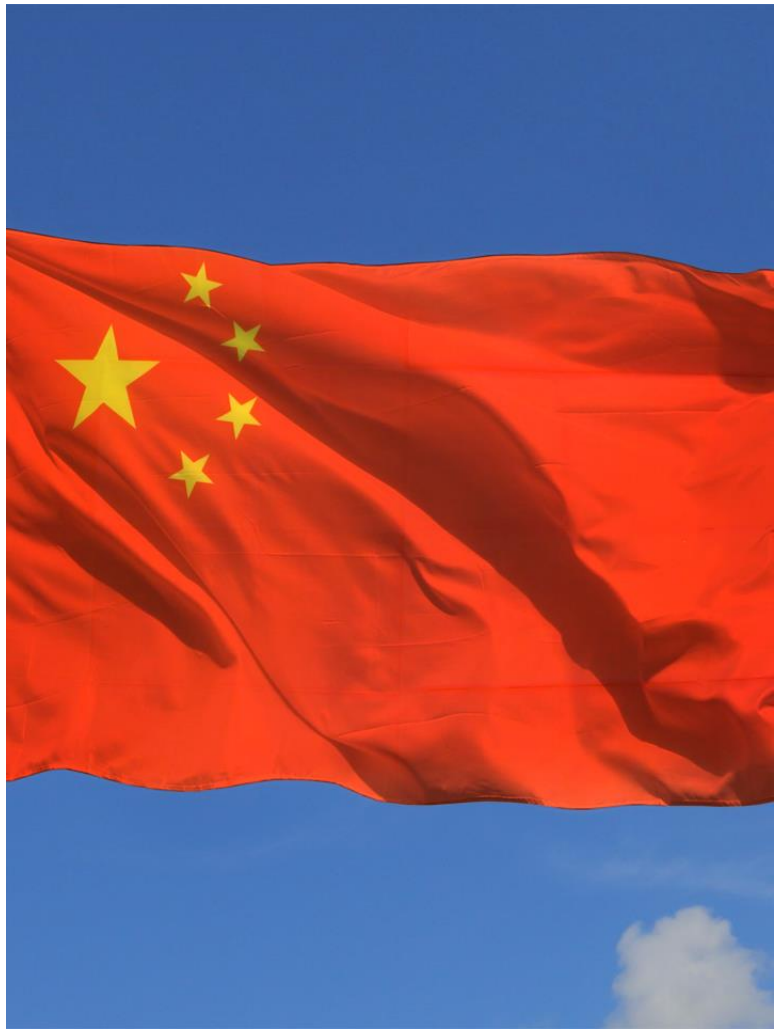


NTT DATA

# NTT DATA's Cybersecurity Services



# Die 3 größten Wirtschaftsmächte (lt. WEF)



# $10.5 trillion

Cybercrime Revenue 2025, mostly ransomware, from $8 trillion in 2023 (Source WEF)

# The Anatomy of Modern Cyber Attackers

Today's threat actors represent a sophisticated ecosystem of criminal organizations, state-sponsored groups, and opportunistic individuals.

## 65%

### Financial Motive

Most European attacks are financially motivated, targeting critical infrastructure.

## 205

### Days to Detect

Average breach detection time remains dangerously high across EU organizations.

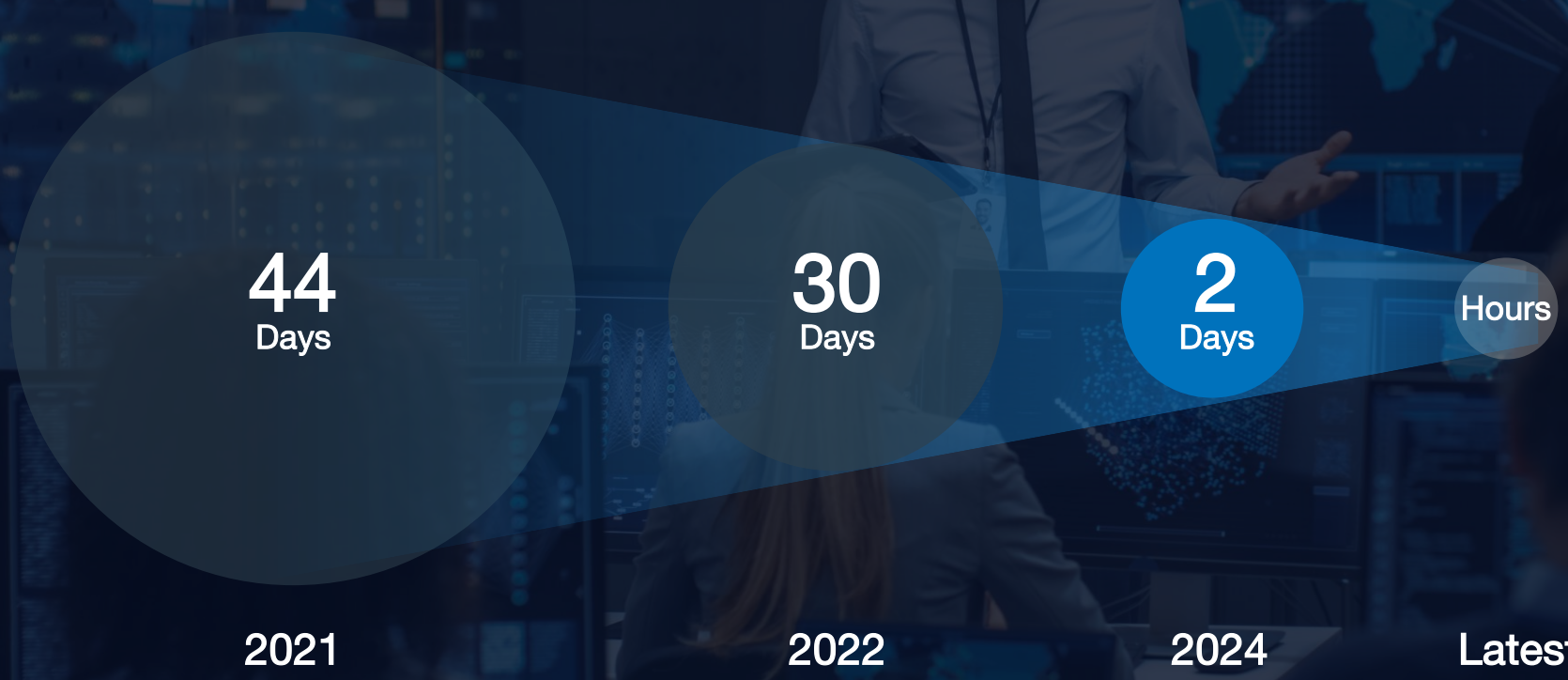
## 4X

### Increase

Growth in multi-extortion attacks targeting NIS-2 regulated entities since 2023.

# Attacks are getting faster and faster

## Average Days from “Compromise” to “Exfil”




Industry average
**4 DAYS**
to remediate

Sources:
1) Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience;
2) Under the GDPR Notification Rules, an incident that causes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.



NTT DATA

# The Motivation for Cyber-Crime

$

Extortion
via Ransomware
or DDoS

Theft of
Intellectual Property

Sabotage

# Timeline – Ransomware Entry Point

**Patient Zero**

[redacted]

4/20/2022

**0. legitimate conversation between [redacted] and Customer**

6/22/2022
5:52:25 PM

**1. E-Mail received**
user "[redacted]"
received an impersonation e-mail

[redacted]

6/22/2022
7:03:49 PM

**2. Download malicious Files in password protected Zip archive**

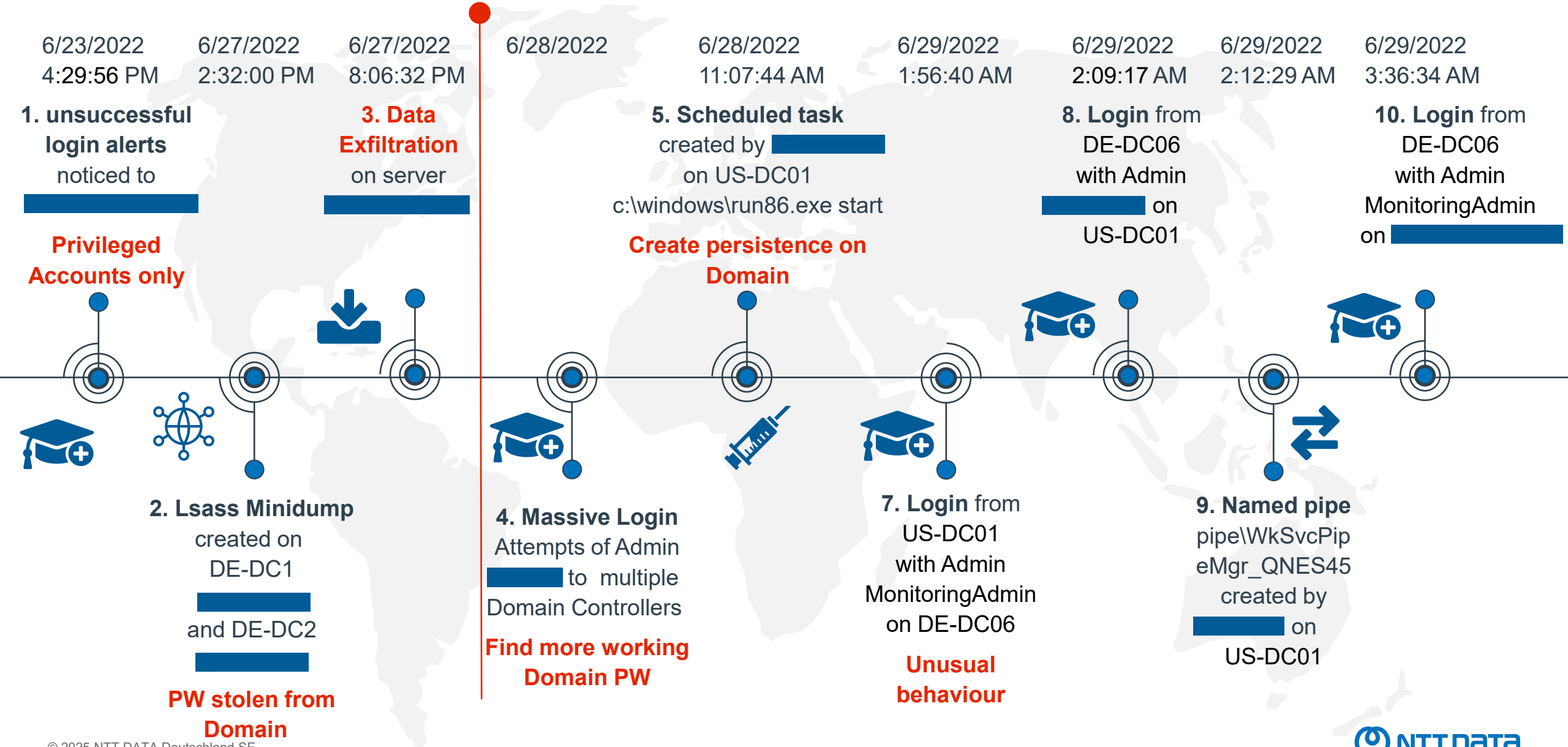
6/22/2022
8:40:40 PM

**3. Open file**
meeting_minutes.zip

6/22/2022
8:41:40 PM

**4. Infection**
Cmd.exe from Zip file executed, Qakbot (aka QBot)

# Timeline – Ransomware Lateral Movement



6/23/2022 4:29:56 PM

**1. unsuccessful login alerts** noticed to [redacted]

**Privileged Accounts only**

6/27/2022 2:32:00 PM

**2. Lsass Minidump** created on DE-DC1 [redacted] and DE-DC2 [redacted]

**PW stolen from Domain**

6/27/2022 8:06:32 PM

**3. Data Exfiltration** on server [redacted]

6/28/2022

**4. Massive Login** Attempts of Admin [redacted] to multiple Domain Controllers

**Find more working Domain PW**

6/28/2022 11:07:44 AM

**5. Scheduled task** created by [redacted] on US-DC01 c:\windows\run86.exe start

**Create persistence on Domain**

6/29/2022 1:56:40 AM

**7. Login** from US-DC01 with Admin MonitoringAdmin on DE-DC06

**Unusual behaviour**

6/29/2022 2:09:17 AM

**8. Login** from DE-DC06 with Admin [redacted] on US-DC01

6/29/2022 2:12:29 AM

**9. Named pipe** pipe\WkSvcPipeMgr_QNES45 created by [redacted] on US-DC01

6/29/2022 3:36:34 AM

**10. Login** from DE-DC06 with Admin MonitoringAdmin on [redacted]

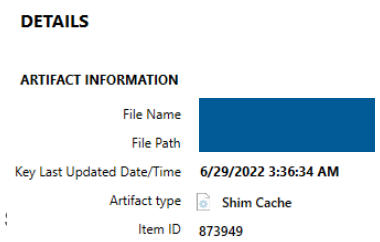
# Timeline – Ransomware Encryption

6/29/2022
3:36:34 AM

**11. Login** from DE-DC06 with Admin MonitoringAdmin on [redacted]

6/29/2022
3:36:34 AM

**12. File Execution**
MonitoringAdmin on [redacted] executes [redacted]




6/29/2022
3:37:08 AM

**13. Start encrypting files** on [redacted]


6/29/2022
7:40:08 AM

**14. SD-WAN shutdown**

6/30/2022

**15. Scheduled Tasks** [redacted] File Server in [redacted] where the encryption started on 30th of June

# Are you prepared for an incident?

# Questions in Case of a Cybersecurity Incident


**Would 6 hours of recovery time per server be sufficient in the event of a cybersecurity incident?**

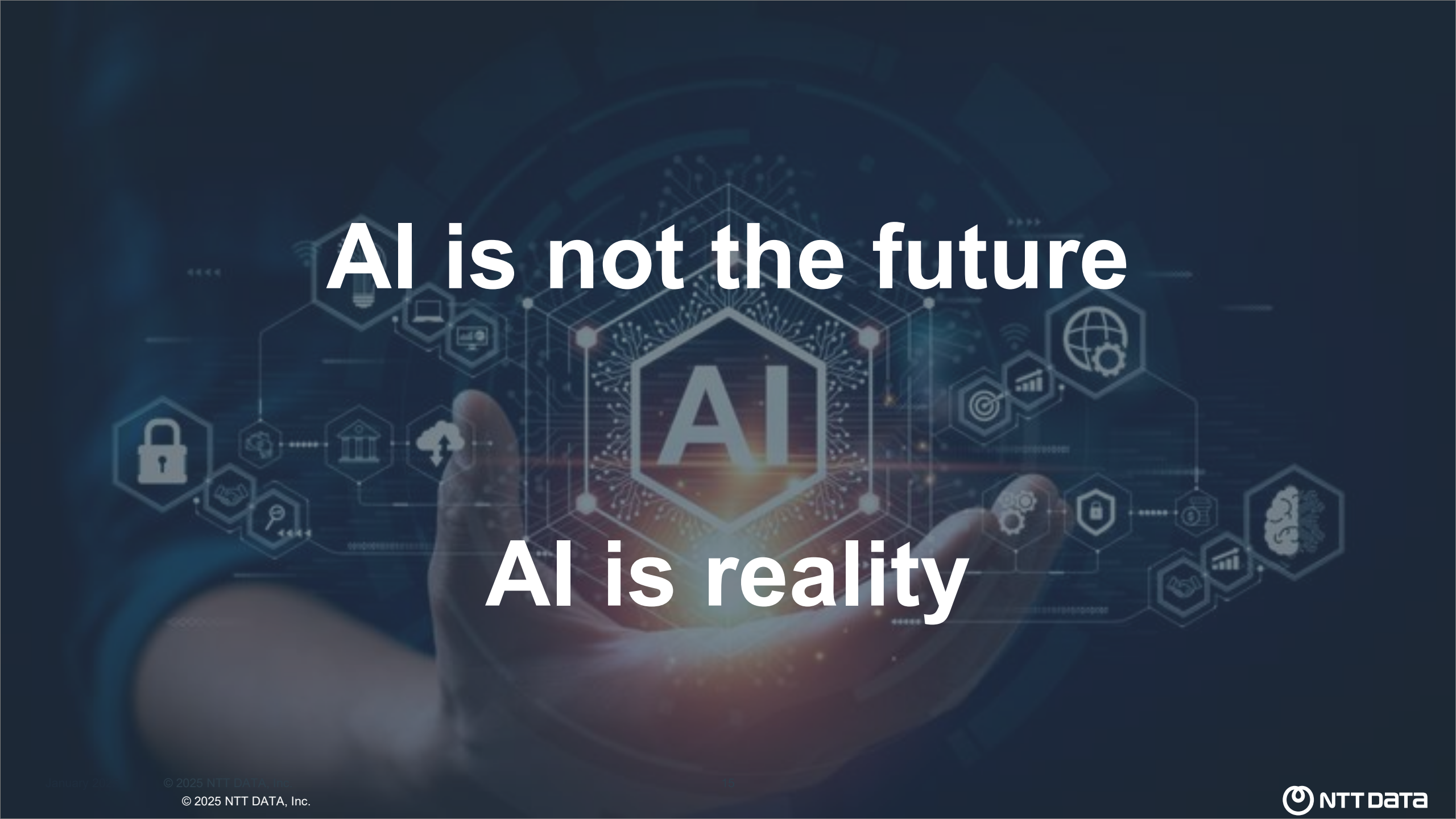
**Is your backup system still up and running?**

**Are your backups free of infection?**

**Do you have spare hardware on stock?**



NTT DATA

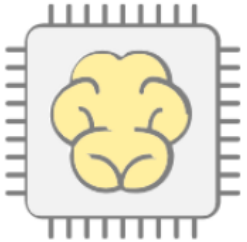




© 2025 NTT DATA, Inc.

# Increase efficiency with AI in security operations

## Assisted SOC



Automation with basic rule-based workflows to automate repetitive tasks.

Hyper-automated SOCs that combine ML, RPA, and orchestration for end-to-end automation.

AI/ML speeds up research on Indicators of Compromise (IoC), Indicators of Attack (IoA), and Tactics, Techniques, and Procedures (TTPs) and provides contextual insights.

## Manual SOC

Operated manually, limited automation through hard-coded deterministic scripts.

Human analysts solely responsible for threat life cycle.

Overwhelmed workforce.

# AI Powered SOC

## Autonomous SOC

AI independently assesses threats, makes decisions, and executes responses.

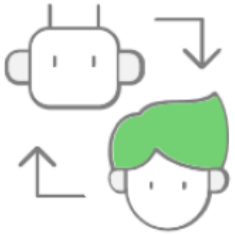
Minimal human intervention.

Human oversight for ethical considerations, focusing on strategic initiatives.

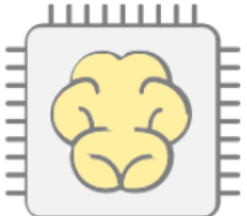
## Semi-autonomous SOC

AI drives most of the tasks on behalf of the analysts, handles predefined workflows.

Human oversight retained for critical decisions, balancing automation and expertise.



## Assisted SOC



Automation with basic rule-based workflows to automate repetitive tasks.

Hyper-automated SOCs that combine ML, RPA, and orchestration for end-to-end automation.

AI/ML speeds up research on Indicators of Compromise (IoC), Indicators of Attack (IoA), and Tactics, Techniques, and Procedures (TTPs) and

# Key learnings from more than 1000 Cybersecurity incidents

01 It will be worse than you think and expect

02 Be prepared and train different scenarios

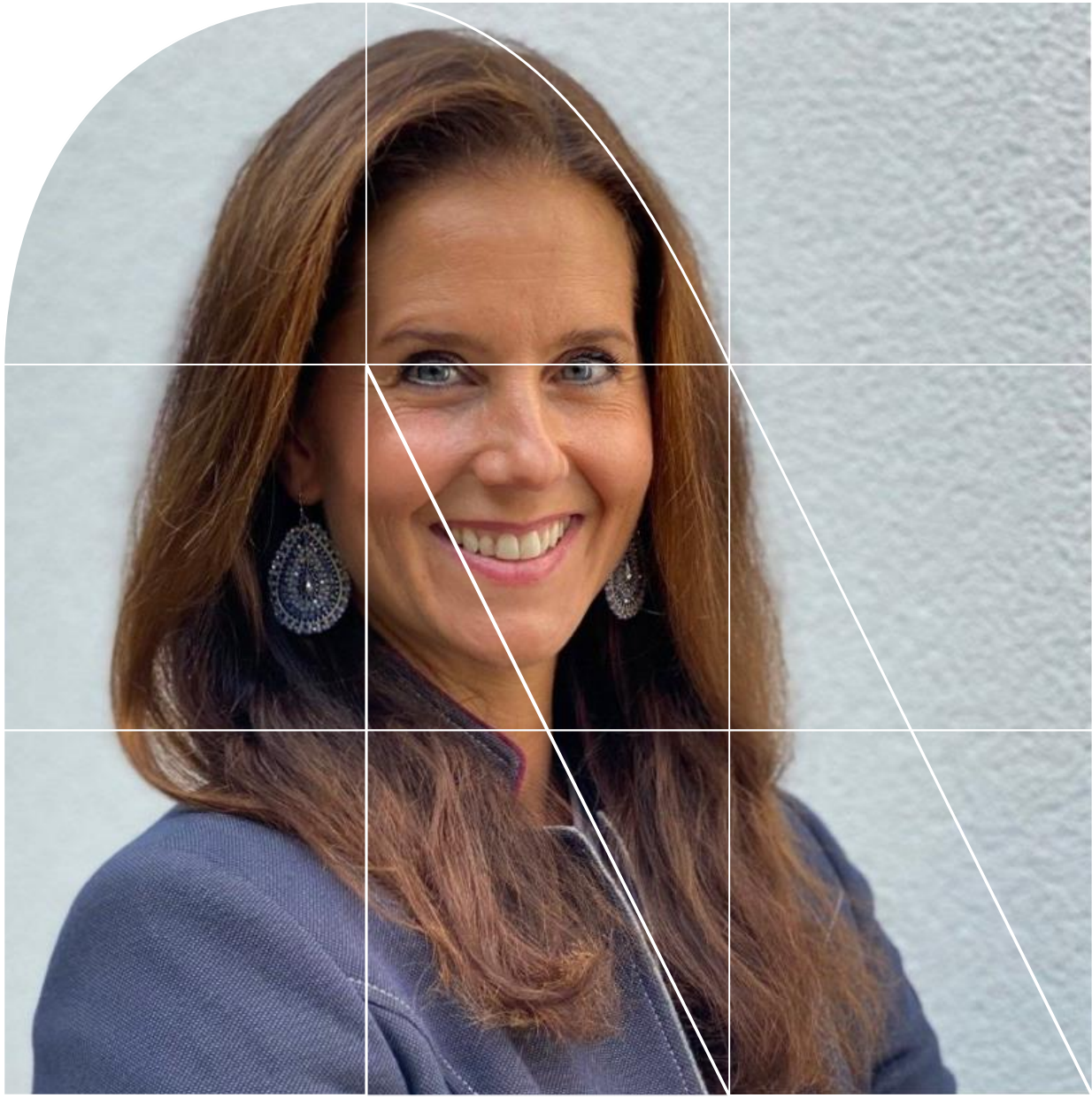
03 Educate cybersecurity and IT staff in multiple situations

04 Use technology that really helps you being more efficient

05 Start with cybersecurity automation as soon as you can

06 Only a global partner like NTT DATA can support you in a Cybercrisis

# Your Contact in Austria




## Eva Heralic

Vice President Cybersecurity AT

M: +43 660 574 37 27

Eva.Heralic@nttdata.com


NTT DATA