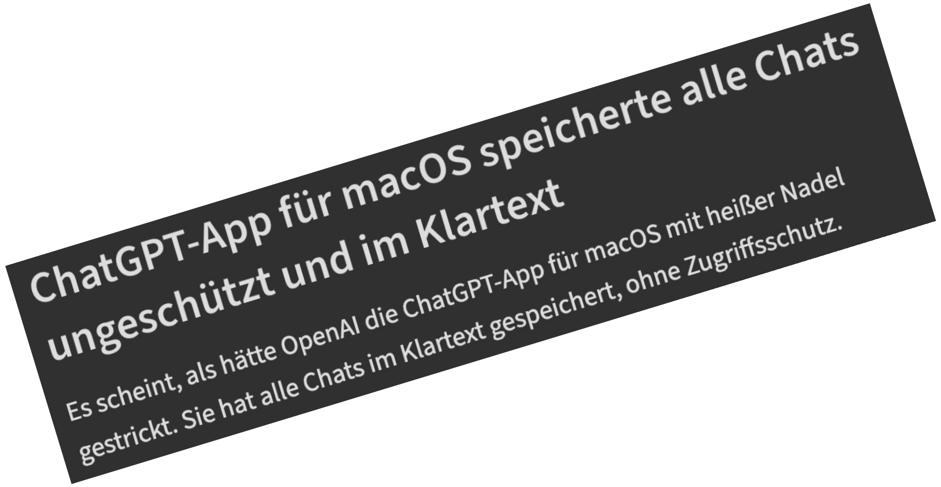
Hochschule
München
University of
Applied Sciences

Fakultät für Informatik und Mathematik

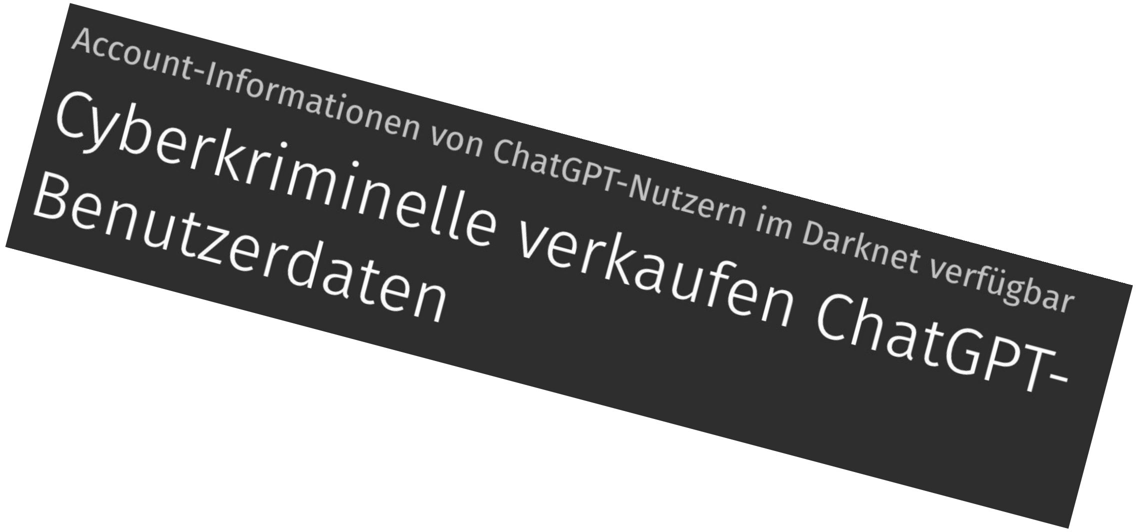
KI – Chance und Gefahren für die Informationssicherheit

2024-11-27 / Prof. Dr.-Ing. Thomas Schreck



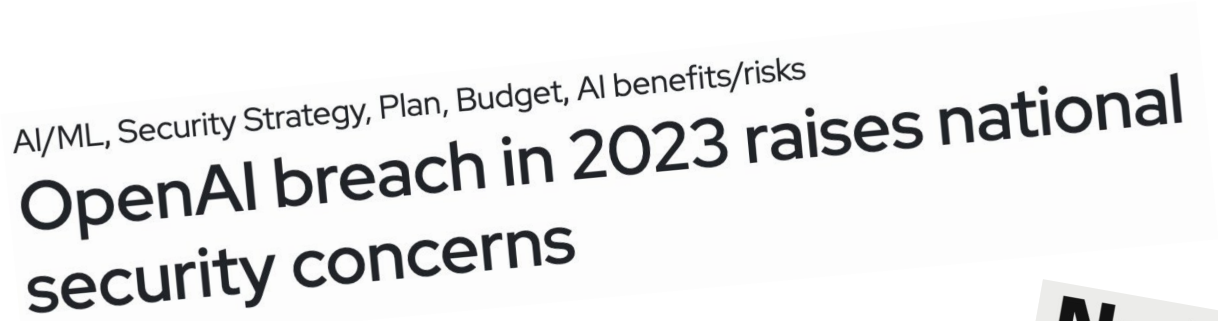
ChatGPT-App für macOS speicherte alle Chats ungeschützt und im Klartext

Es scheint, als hätte OpenAI die ChatGPT-App für macOS mit heißer Nadel gestrickt. Sie hat alle Chats im Klartext gespeichert, ohne Zugriffsschutz.



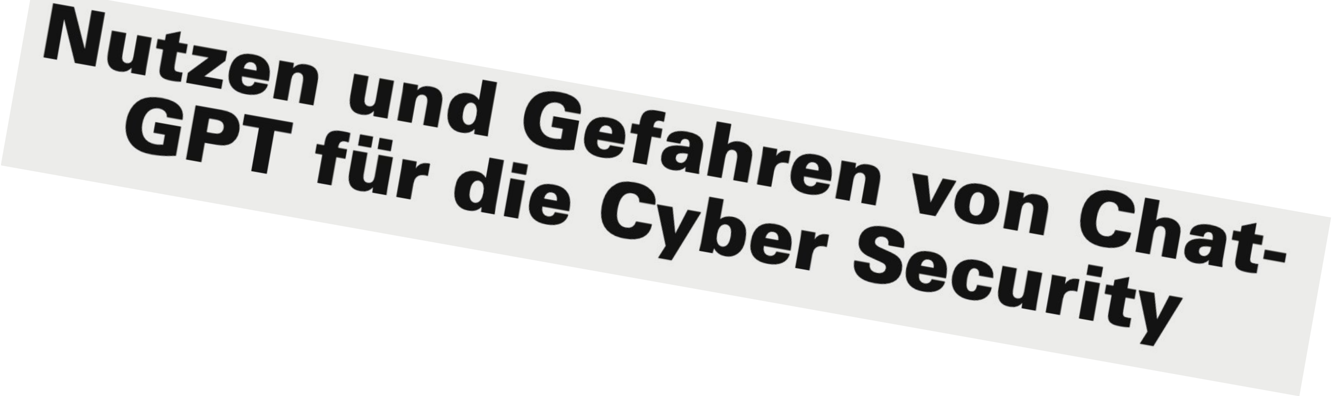
Account-Informationen von ChatGPT-Nutzern im Darknet verfügbar

Cyberkriminelle verkaufen ChatGPT-Benutzerdaten

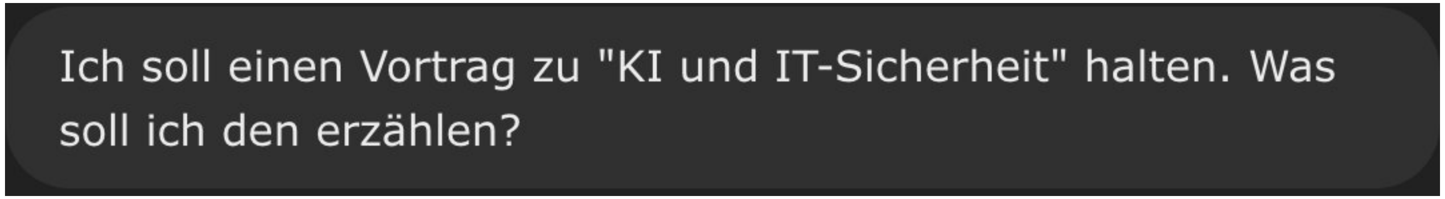


AI/ML, Security Strategy, Plan, Budget, AI benefits/risks

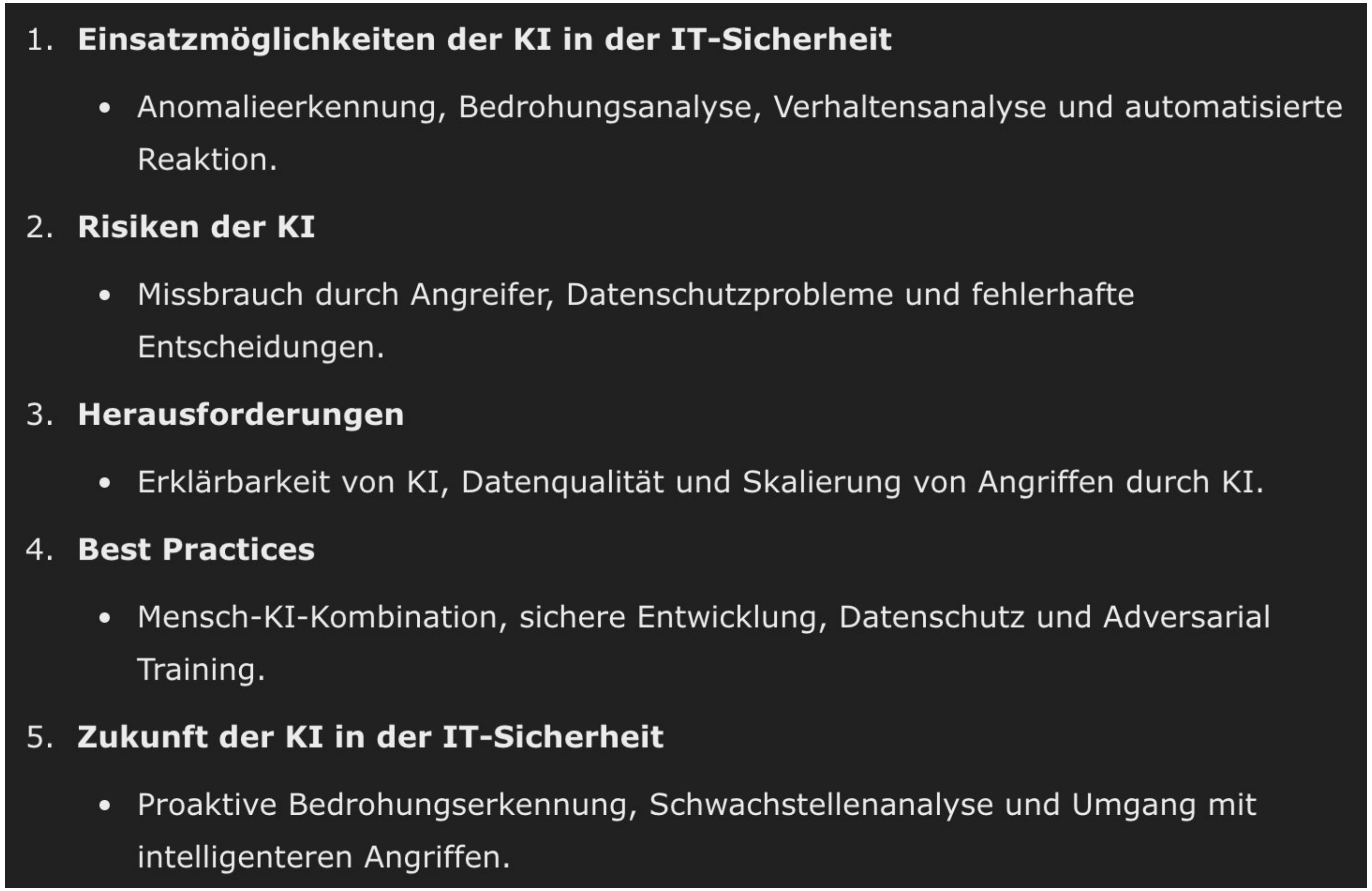
OpenAI breach in 2023 raises national security concerns



Nutzen und Gefahren von Chat-GPT für die Cyber Security

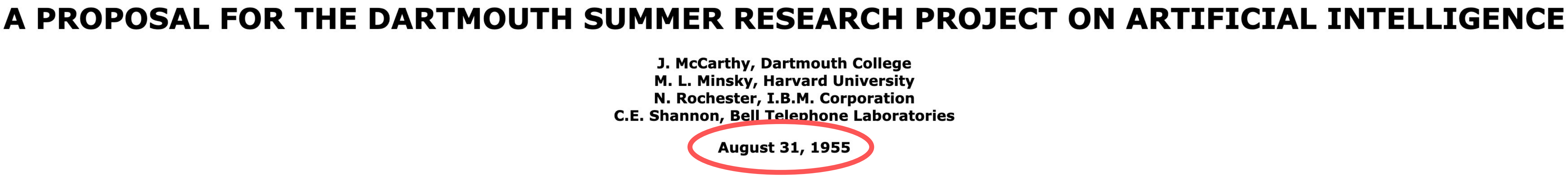


Ich soll einen Vortrag zu "KI und IT-Sicherheit" halten. Was soll ich den erzählen?



1. **Einsatzmöglichkeiten der KI in der IT-Sicherheit**
   - Anomalieerkennung, Bedrohungsanalyse, Verhaltensanalyse und automatisierte Reaktion.
2. **Risiken der KI**
   - Missbrauch durch Angreifer, Datenschutzprobleme und fehlerhafte Entscheidungen.
3. **Herausforderungen**
   - Erklärbarkeit von KI, Datenqualität und Skalierung von Angriffen durch KI.
4. **Best Practices**
   - Mensch-KI-Kombination, sichere Entwicklung, Datenschutz und Adversarial Training.
5. **Zukunft der KI in der IT-Sicherheit**
   - Proaktive Bedrohungserkennung, Schwachstellenanalyse und Umgang mit intelligenteren Angriffen.

Künstliche Intelligenz



A PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE

J. McCarthy, Dartmouth College
M. L. Minsky, Harvard University
N. Rochester, I.B.M. Corporation
C.E. Shannon, Bell Telephone Laboratories

August 31, 1955

… woher kommt der Hype jetzt?

LLM ⊂ AI

AI is a Cloud Service

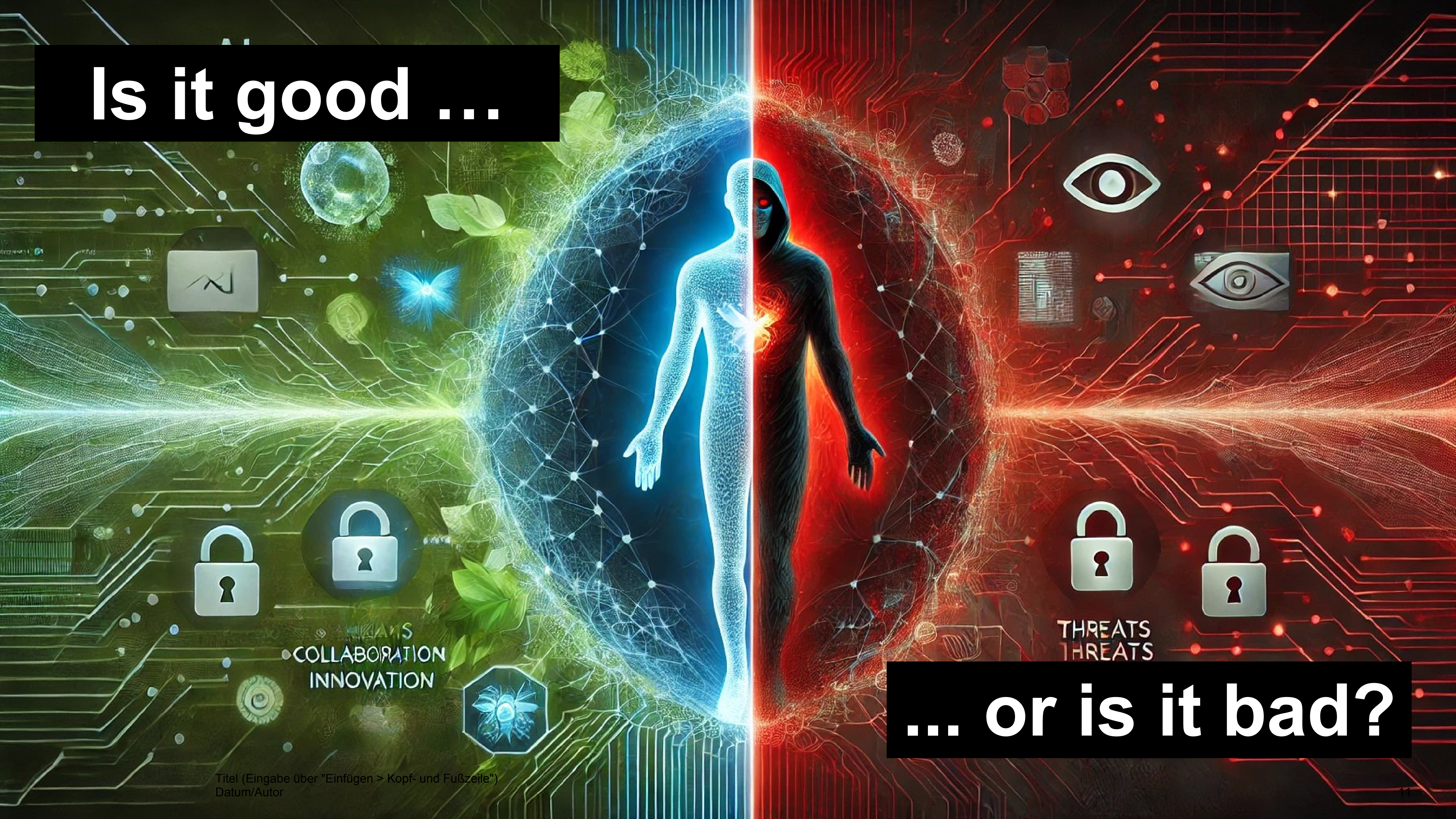
Looking at AI from IT-Security

Trust in AI

Criminals use AI

AI and Cyberdefense

Is it good …



... or is it bad?

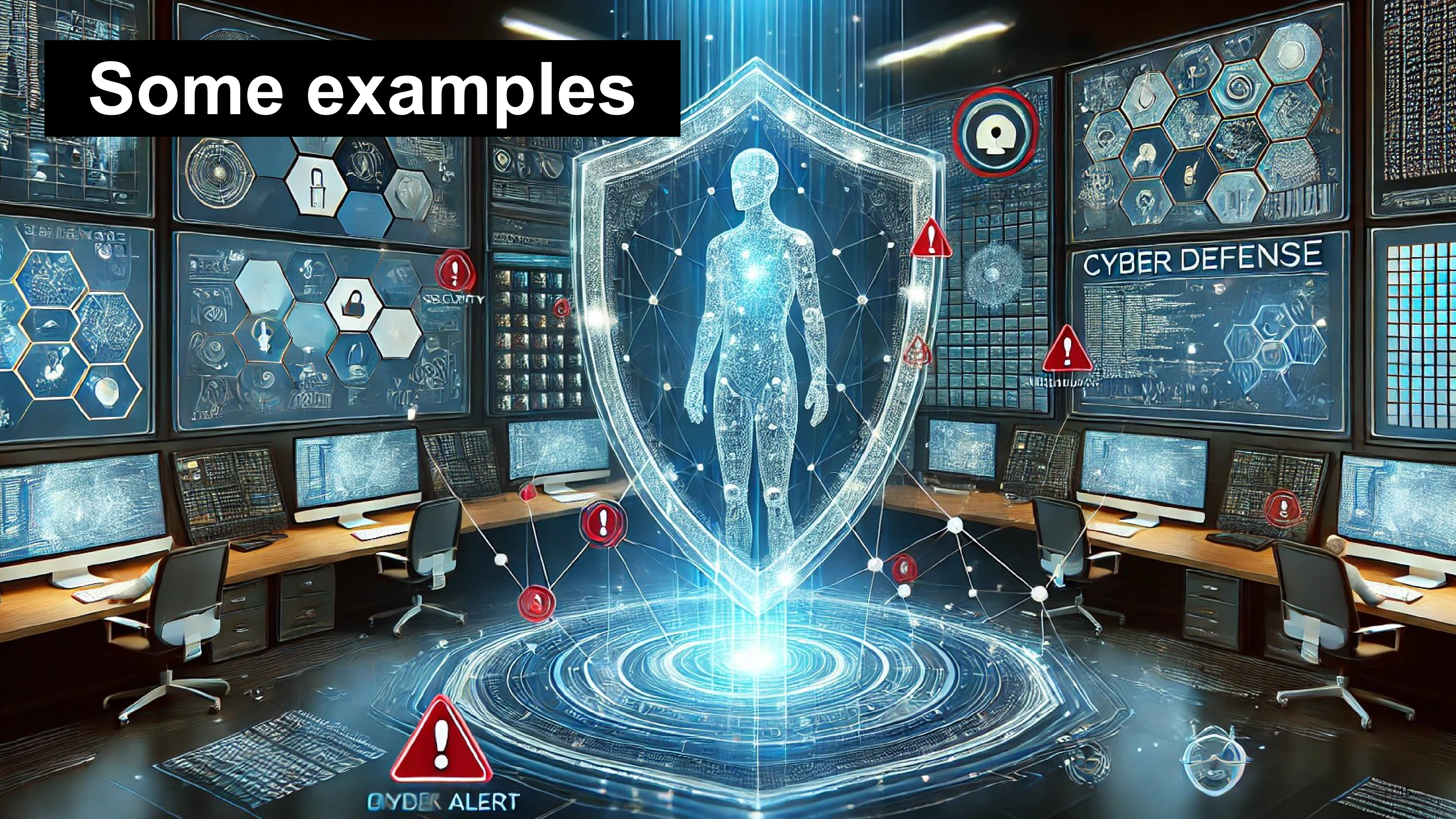
New technologies …

… interrupt

Focus on the opportunities …

... and manage the risk.

Some examples

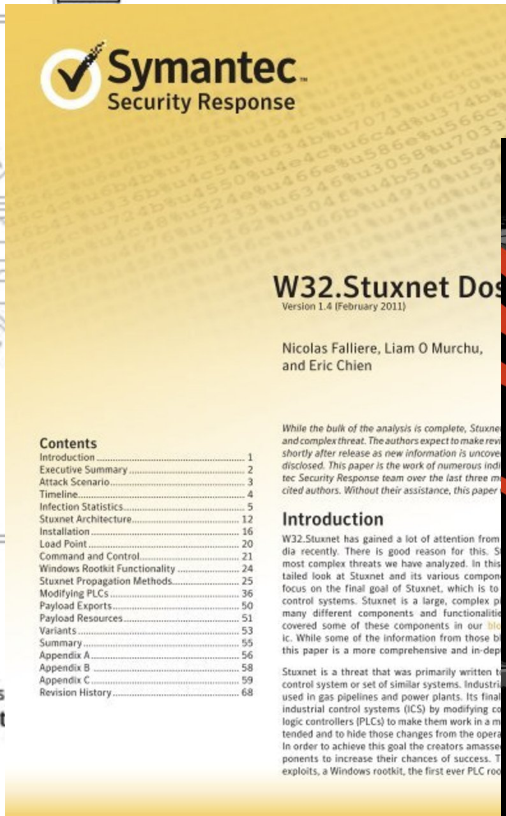


Understanding

DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2024

Bundesamt für Sicherheit in der Informationstechnik

Deuts
Digit



Symantec.
Security Response

W32.Stuxnet Dos
Version 1.4 (February 2011)

Nicolas Falliere, Liam O Murchu,
and Eric Chien

While the bulk of the analysis is complete, Stuxne
and complex threat. The authors expect to make rev
shortly after release as new information is uncove
disclosed. This paper is the work of numerous indi
tec Security Response team over the last three m
cited authors. Without their assistance, this paper

Introduction

W32.Stuxnet has gained a lot of attention from
dia recently. There is good reason for this. S
most complex threats we have analyzed. In this
tailed look at Stuxnet and its various compon
focus on the final goal of Stuxnet, which is to
control systems. Stuxnet is a large, complex p
many different components and functionaliti
covered some of these components in our blo
ic. While some of the information from those b
this paper is a more comprehensive and in-dep

Stuxnet is a threat that was primarily written t
control system or set of similar systems. Industri
used in gas pipelines and power plants. Its final
industrial control systems (ICS) by modifying co
logic controllers (PLCs) to make them work in a m
tended and to hide those changes from the opera
In order to achieve this goal the creators amasse
ponents to increase their chances of success. T
exploits, a Windows rootkit, the first ever PLC roo

CROWDSTRIKE

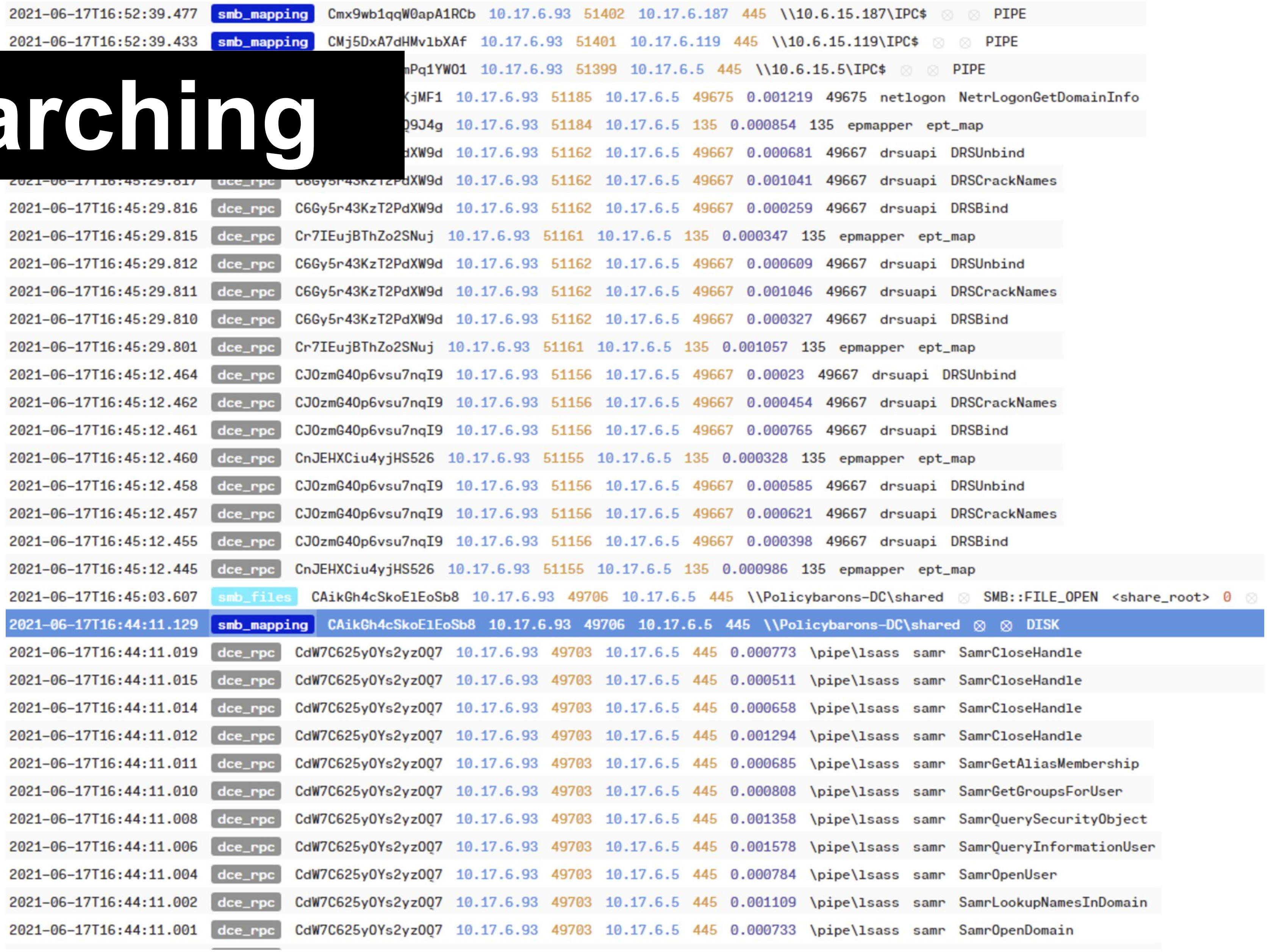
THREAT HUNT REPORT 2024

NSA joins CISA and partners in releasing:

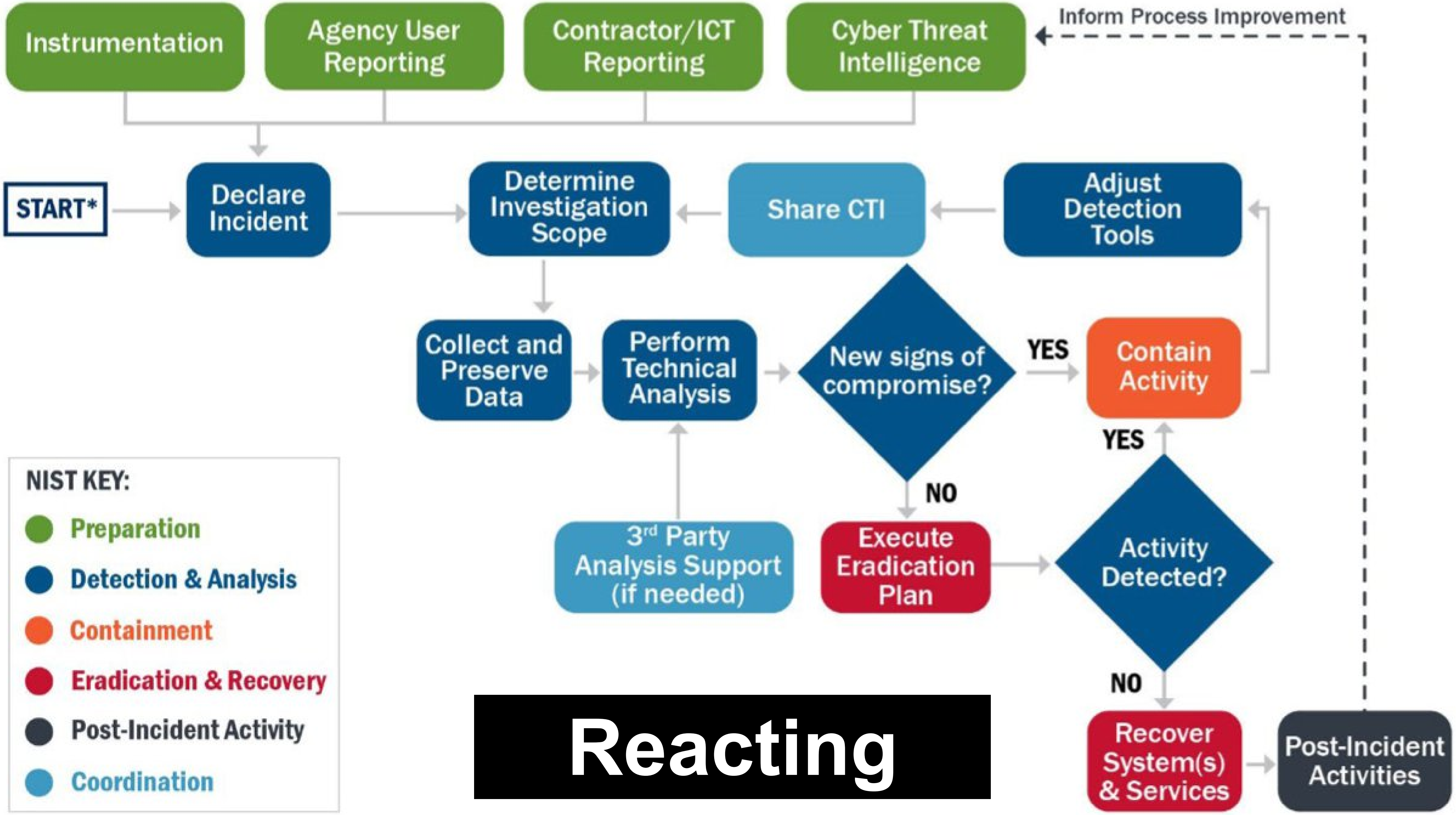
2023 TOP ROUTINELY EXPLOITED VULNERABILITIES

CYBERSECURITY ADVISORY

Searching



```
2021-06-17T16:52:39.477  smb_mapping  Cmx9wb1qqW0apA1RCb  10.17.6.93  51402  10.17.6.187  445  \\10.6.15.187\IPC$  ⊗  ⊗  PIPE
2021-06-17T16:52:39.433  smb_mapping  CMj5DxA7dHMvlbXAf  10.17.6.93  51401  10.17.6.119  445  \\10.6.15.119\IPC$  ⊗  ⊗  PIPE
mPq1YW01  10.17.6.93  51399  10.17.6.5  445  \\10.6.15.5\IPC$  ⊗  ⊗  PIPE
jMF1  10.17.6.93  51185  10.17.6.5  49675  0.001219  49675  netlogon  NetrLogonGetDomainInfo
Q9J4g  10.17.6.93  51184  10.17.6.5  135  0.000854  135  epmapper  ept_map
dXW9d  10.17.6.93  51162  10.17.6.5  49667  0.000681  49667  drsuapi  DRSUnbind
2021-06-17T16:45:29.817  dce_rpc  C6Gy5r43KzT2PdXW9d  10.17.6.93  51162  10.17.6.5  49667  0.001041  49667  drsuapi  DRSCrackNames
2021-06-17T16:45:29.816  dce_rpc  C6Gy5r43KzT2PdXW9d  10.17.6.93  51162  10.17.6.5  49667  0.000259  49667  drsuapi  DRSBind
2021-06-17T16:45:29.815  dce_rpc  Cr7IEujBThZo2SNuj  10.17.6.93  51161  10.17.6.5  135  0.000347  135  epmapper  ept_map
2021-06-17T16:45:29.812  dce_rpc  C6Gy5r43KzT2PdXW9d  10.17.6.93  51162  10.17.6.5  49667  0.000609  49667  drsuapi  DRSUnbind
2021-06-17T16:45:29.811  dce_rpc  C6Gy5r43KzT2PdXW9d  10.17.6.93  51162  10.17.6.5  49667  0.001046  49667  drsuapi  DRSCrackNames
2021-06-17T16:45:29.810  dce_rpc  C6Gy5r43KzT2PdXW9d  10.17.6.93  51162  10.17.6.5  49667  0.000327  49667  drsuapi  DRSBind
2021-06-17T16:45:29.801  dce_rpc  Cr7IEujBThZo2SNuj  10.17.6.93  51161  10.17.6.5  135  0.001057  135  epmapper  ept_map
2021-06-17T16:45:12.464  dce_rpc  CJOzmG40p6vsu7nqI9  10.17.6.93  51156  10.17.6.5  49667  0.00023  49667  drsuapi  DRSUnbind
2021-06-17T16:45:12.462  dce_rpc  CJOzmG40p6vsu7nqI9  10.17.6.93  51156  10.17.6.5  49667  0.000454  49667  drsuapi  DRSCrackNames
2021-06-17T16:45:12.461  dce_rpc  CJOzmG40p6vsu7nqI9  10.17.6.93  51156  10.17.6.5  49667  0.000765  49667  drsuapi  DRSBind
2021-06-17T16:45:12.460  dce_rpc  CnJEHXCiu4yjHS526  10.17.6.93  51155  10.17.6.5  135  0.000328  135  epmapper  ept_map
2021-06-17T16:45:12.458  dce_rpc  CJOzmG40p6vsu7nqI9  10.17.6.93  51156  10.17.6.5  49667  0.000585  49667  drsuapi  DRSUnbind
2021-06-17T16:45:12.457  dce_rpc  CJOzmG40p6vsu7nqI9  10.17.6.93  51156  10.17.6.5  49667  0.000621  49667  drsuapi  DRSCrackNames
2021-06-17T16:45:12.455  dce_rpc  CJOzmG40p6vsu7nqI9  10.17.6.93  51156  10.17.6.5  49667  0.000398  49667  drsuapi  DRSBind
2021-06-17T16:45:12.445  dce_rpc  CnJEHXCiu4yjHS526  10.17.6.93  51155  10.17.6.5  135  0.000986  135  epmapper  ept_map
2021-06-17T16:45:03.607  smb_files  CAikGh4cSkoE1EoSb8  10.17.6.93  49706  10.17.6.5  445  \\Policybarons-DC\shared  ⊗  SMB::FILE_OPEN  <share_root>  0  ⊗
2021-06-17T16:44:11.129  smb_mapping  CAikGh4cSkoE1EoSb8  10.17.6.93  49706  10.17.6.5  445  \\Policybarons-DC\shared  ⊗  ⊗  DISK
2021-06-17T16:44:11.019  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.000773  \pipe\lsass  samr  SamrCloseHandle
2021-06-17T16:44:11.015  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.000511  \pipe\lsass  samr  SamrCloseHandle
2021-06-17T16:44:11.014  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.000658  \pipe\lsass  samr  SamrCloseHandle
2021-06-17T16:44:11.012  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.001294  \pipe\lsass  samr  SamrCloseHandle
2021-06-17T16:44:11.011  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.000685  \pipe\lsass  samr  SamrGetAliasMembership
2021-06-17T16:44:11.010  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.000808  \pipe\lsass  samr  SamrGetGroupsForUser
2021-06-17T16:44:11.008  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.001358  \pipe\lsass  samr  SamrQuerySecurityObject
2021-06-17T16:44:11.006  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.001578  \pipe\lsass  samr  SamrQueryInformationUser
2021-06-17T16:44:11.004  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.000784  \pipe\lsass  samr  SamrOpenUser
2021-06-17T16:44:11.002  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.001109  \pipe\lsass  samr  SamrLookupNamesInDomain
2021-06-17T16:44:11.001  dce_rpc  CdW7C625yOYs2yzOQ7  10.17.6.93  49703  10.17.6.5  445  0.000733  \pipe\lsass  samr  SamrOpenDomain
```



Instrumentation

Agency User Reporting

Contractor/ICT Reporting

Cyber Threat Intelligence

Inform Process Improvement

START*

Declare Incident

Determine Investigation Scope

Share CTI

Adjust Detection Tools

Collect and Preserve Data

Perform Technical Analysis

New signs of compromise?

YES

Contain Activity

NO

YES

3rd Party Analysis Support (if needed)

Execute Eradication Plan

Activity Detected?

NO

Recover System(s) & Services

Post-Incident Activities

NIST KEY:

- ● Preparation
- ● Detection & Analysis
- ● Containment
- ● Eradication & Recovery
- ● Post-Incident Activity
- ● Coordination

Reacting

Takeaways

- KI sind Algorithmen, die in groß angelegten Infrastrukturen eingesetzt werden.
- Aus sicherheitstechnischer Sicht handelt es sich um einen Datenprozessor.
- Nutzen Sie einfach die bereits vorhandenen risikobasierten Ansätze.
- KI ist eine Technologie, die sowohl von **guten** als auch von **schlechten Akteuren** genutzt werden kann.

- Ein Thema ist jedoch wichtig: **Vertrauen in KI**

Kontakt

Prof. Dr.-Ing. Thomas Schreck
Hochschule München University of Applied Sciences

Email: thomas.schreck@hm.edu
Website: https://seclab.cs.hm.edu

Open Source Projekte der HM IT:

https://github.com/hm-edu