Corporate Cyber Readiness

Guest Lecture Information & Communication Security | Winter 2024/2025 |
Chair of Mobile Business & Multilateral Security | Goethe University Frankfurt

February 4, 2025

Dr. Gökhan Bal | AONIC GmbH

Agenda

1. About Me
2. About AONIC
3. The Need for Cyber Readiness
4. Cyber Readiness Exercises
5. AMA

About Me

AONIC
Teamlead Cybersecurity Consulting
Dr. Gökhan Bal
goekhan.bal@aonic.de

2009: Diplom-Informatiker (Goethe Uni, FB 12)

2015: Dr. rer. pol (Goethe Uni, FB 2)

2015-2024: Deutsche Bahn (InfoSec Governance, Cybersecurity Consulting)

Since 10/2024: Teamlead Cybersecurity Consulting at AONIC GmbH

UNSER UNTERNEHMEN

Über AONIC

Als Management- und Technologieberatung beschleunigen wir den digitalen Wandel im Maschinenraum der deutschen Wirtschaft: Digitalisierung, Cybersicherheit, Wissensmanagement und KI

9
Zertifizierungen

+10
Jahre am Markt tätig

+50
Mitarbeitende

+300
Softwareeinführungen

2
Innovationspreise

0
Investoren

Kunden

DB BAHN
TDK
Rolls-Royce
GlaxoSmithKline
ThermoFisher Scientific
Aurubis
techem
Deutsche Telekom
Technische Universität Darmstadt
SAMSON
KION Group
Merck
Fresenius
Viatris
umicore
KARL MAYER – We care about your future

Partner & Zertifizierungen

Microsoft
ATLASSIAN
Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Prosci Certified Change Practitioner
ITIL 4 Foundation CPD
Project Management Institute
ISTQB International Software Testing Qualifications Board
PRINCE2
2022/2023 Innovativ durch Forschung – AONIC GmbH
ZIM Zentrales Innovationsprogramm Mittelstand
GERMAN UPA Berufsverband der Deutschen Usability und User Experience Professionals
AI Frankfurt Rhein-Main e.V.

Von der Softwareentwicklung zum IT-Consulting

2012

Gründungsteam aus der TU Darmstadt mit Schwerpunkten Cloud und Softwareentwicklung

2016

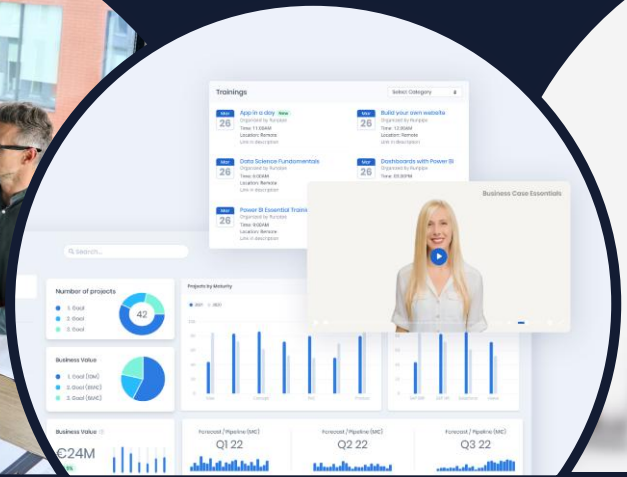
AONIC wird Microsoft Partner

2018

Neue Abteilung Consulting Services bietet Beratung im Bereich IT Infrastruktur

2020

Produktlaunch der hauseigenen Low-Code Governance Plattform Runpipe



2025

AONIC wird Atlassian Partner

Unsere Leistungen

Consulting

- IT-Strategie, IT-Prozesse, Governance
- IT-Ausschreibungen und Vendormanagement
- Portfolio- und Projektmanagement

Digitalisierung und KI

- Daten, Digitale Prozesse und Hyperautomation
- Low-Code Plattformen
- Daten und KI in der Produktion

Cybersicherheit

- Strategie, Gapanalyse und Roadmap
- Compliance (z.B. ISO 27001, IEC 62443, TISAX)
- Konzepte, Prozesse und KPIs (ISMS / CSMS)

Wissensmanagement

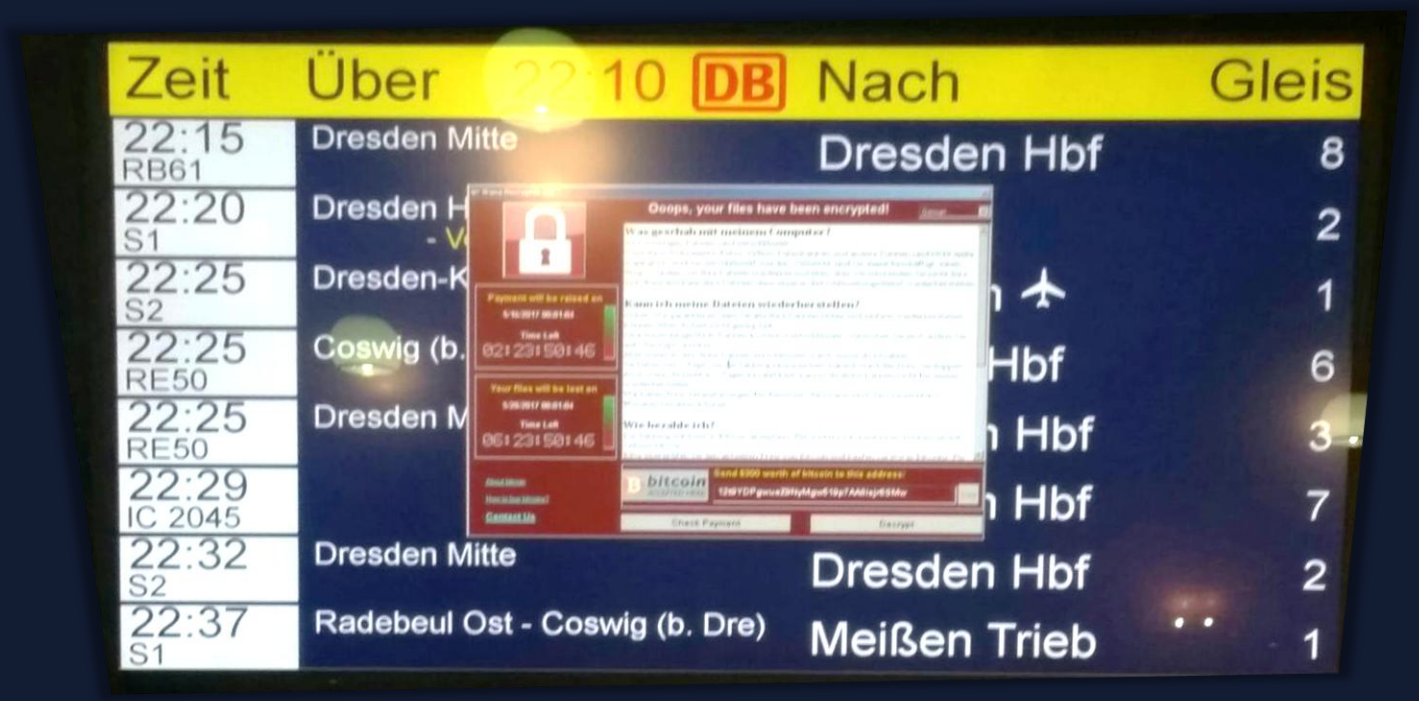
- Modernes Intranet
- Dokumentenmanagement und Wiki
- Automatisierung durch GenAI

AONIC
digital. together.

The Need for Cyber Readiness

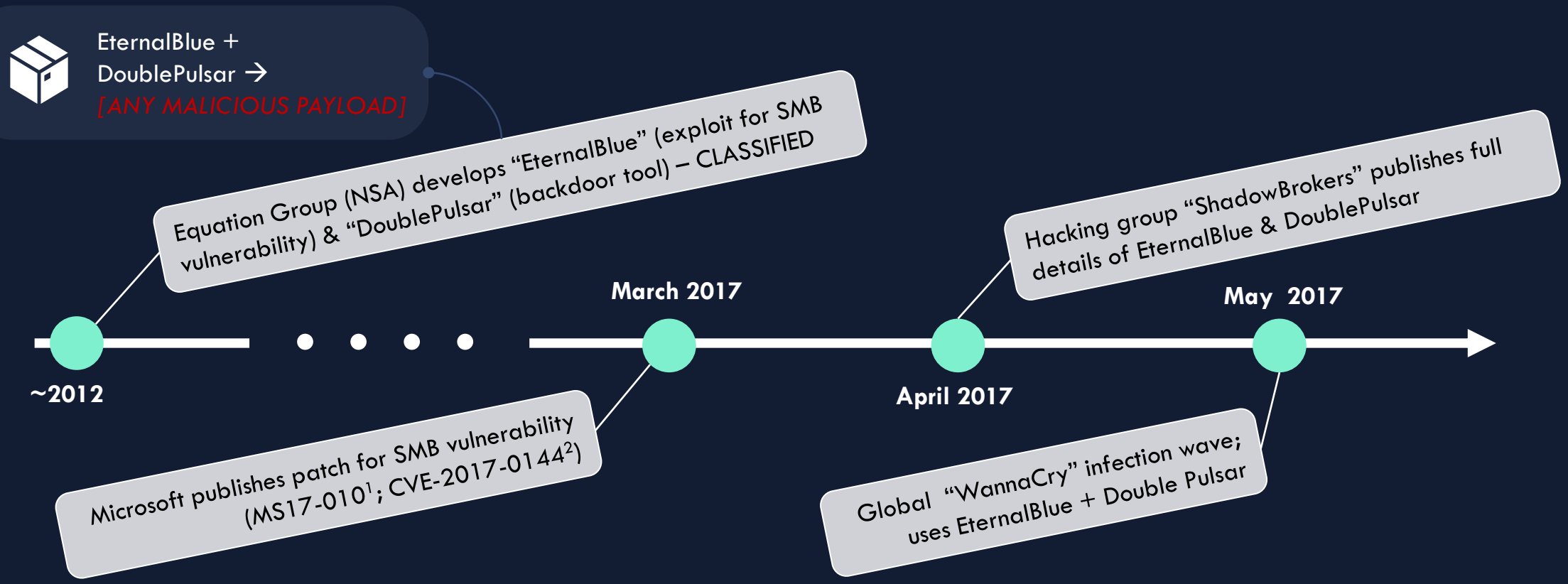
Why preventive cybersecurity is not enough

THE WANNACRY CRYPTO WORM ATTACK OF 2017



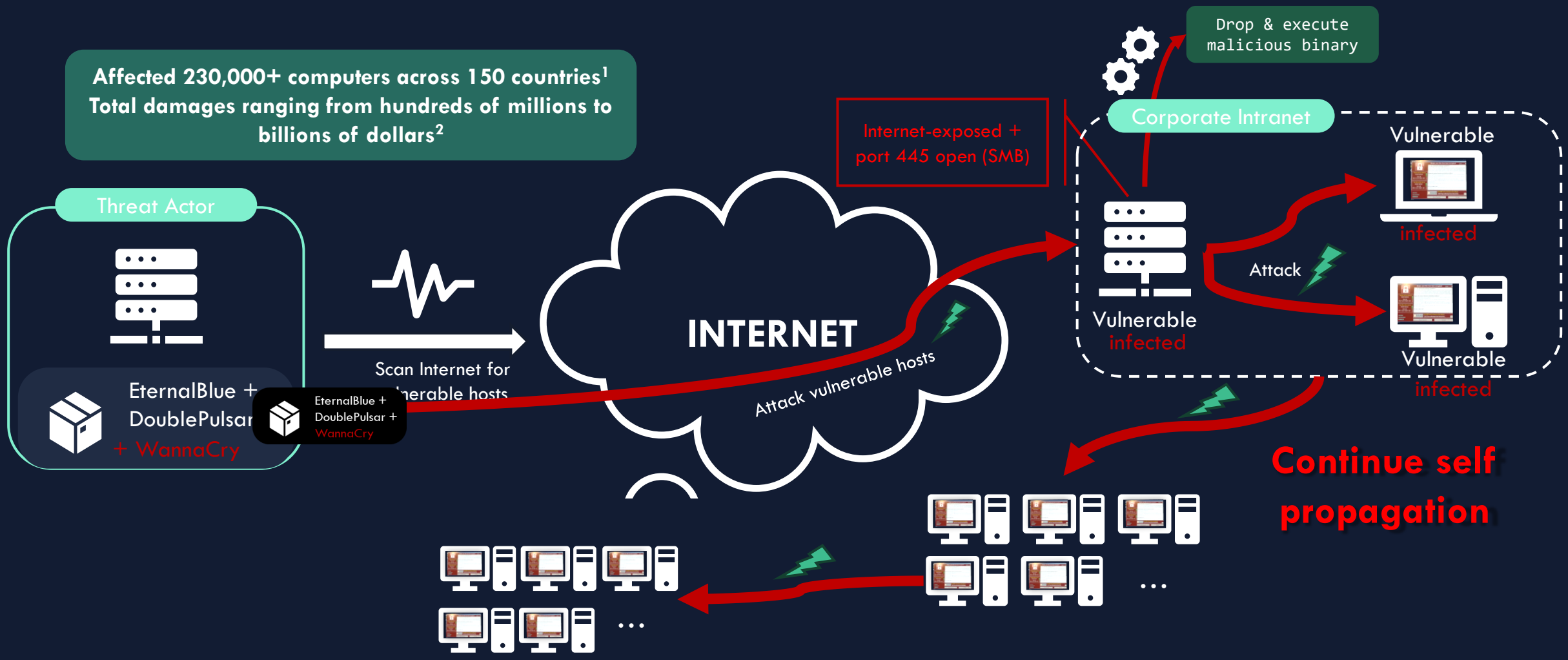
Train departure board with WannaCry ransom note

WannaCry: Background Information



[1] https://docs.microsoft.com/de-de/security-updates/SecurityBulletins/2017/ms17-010
[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

WannaCry: How it spread



[1] https://www.nist.gov/speech-testimony/bolstering-government-cybersecurity-lessons-learned-wannacry
[2] Various sources

Tense Cyber Threat Landscape

€178,6 bn.

Damage caused by cybercrime in Germany

Ransomware and phishing are the most common forms of attacks (Source: Economic Protection Study 2024, Bitkom).

+90% yearly

Between 2019 and 2023, the number of attacks with physical impacts in the industrial context (OT) has doubled on average annually (Source: 2024 OT Threat Report, Waterfall Security).

Less than 1/3

of companies in Germany have a written emergency plan (Source: BSI Situation Report 2024).

Cyber attacks: business as usual

"There are only two types of companies: Those that have been hacked and those that don't know they have been hacked."

- Robert S. Mueller, III, Former Director FBI

Cyber readiness: The capabilities of detection and response

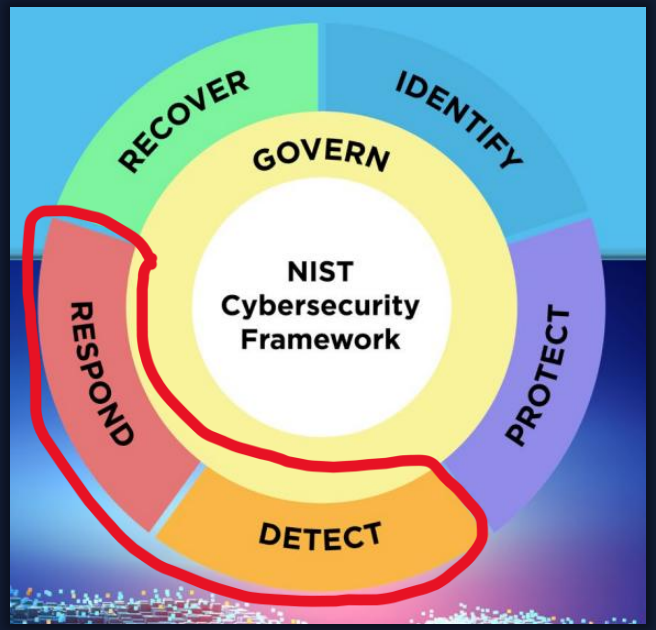


Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

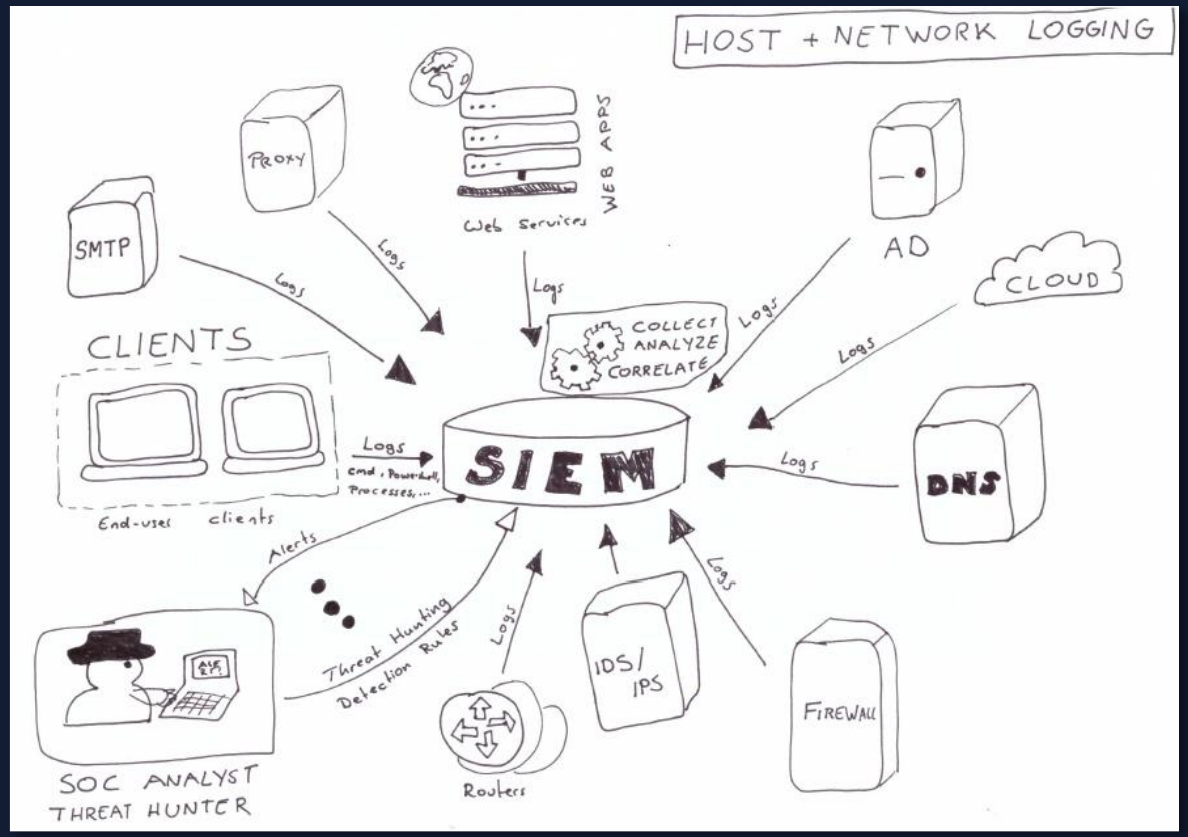
The NIST Cyber Security Framework

The SOC: An Organizations' Center for Cyber Readiness

SIEM: Key Tool for Security Monitoring

"The whole is greater than the sum of its parts." (Aristotle)

- SIEM: Security Information and Event Management (tool)
- Collects and analyses event logs from different sources
- Helps you to identify suspicious activities across your organization
- The „engine" of security operations



Generic SIEM architecture (own creation)

Security Monitoring: How to filter out the noise?

- So much information
- What to look for?
- What are typical attacker tactics and techniques?

https://attack.mitre.org/

AONIC
digital. together.

Cyber Readiness Exercises

An effective method to test and improve cyber readiness

Why Cyber Readiness?

- **Is your organization cyber ready?**
  - Fast and smart detection
  - Fast and systematic response
  - → Minimize damage
- **How to determine cyber readiness?**
  - Option 1: Wait for the next attack
  - Option 2: Test it
- **Set your goals, choose your format:**
  - SIEM alerting tests
  - Phishing simulations
  - Red team tests
  - Alarm drill
  - Tabletop exercise (TTX)

Benefits of Cyber Readiness Exercises

Testing detection capabilities

In exercises and tests, technical capabilities for detecting anomalies can be specifically and tested in a controlled environment.

Testing procedures and tools for response

Procedures and other tools designed to enable a systematic and efficient response can be tested for practical applicability. Decision-making can be practiced.

Sharpening role understanding & raising awareness

Employees can exercise their roles and responsibilities in drills, thereby sharpening their role understanding. They receive immediate feedback on their actions. It also raises their awareness of threats and tools.

Strengthening the security culture

In exercises, interactions occur between people from different areas that rarely happen in everyday work. This builds mutual trust and contributes to strengthening the security culture.

Identifying optimization potentials

Whether it's suggestions for improving the incident response process, enhancing the technical security of an application, or updating a contact list: exercises reveal diverse optimization potentials for cyber readiness.

Compliance

The regular execution of tests or exercises for handling cyber attacks is increasingly required by regulations. Cyber readiness exercises are suitable measures to meet these requirements and to achieve compliance.

Cyber Readiness Exercise

Cyber Readiness Exercise (CRX):
tabletop-based role-playing simulation of a cyber security incident involving relevant roles of various functions

AONIC

Qualities of an exercise

Relevance & realism

Chosen scenarios should relate to the real infrastructure and be coordinated with 'insiders.' Participants should perform their real roles without a script, rather than being placed in fictional roles.

Focus

The exercise should have a clear scope (e.g., a specific IT infrastructure at a location). The goal should be the extensive testing of response in this context.

Participants & engagement

Relevant roles from various levels and functions should participate. Participants should be equally challenged as much as possible. Other roles should be integrated into the exercise live as needed.

Good moderation

Good and independent moderation is essential. It ensures a focused and realistic process, responds flexibly to unforeseen situations, and is responsible for a positive experience for the participants.

Stress level

The exercise should induce the highest possible stress level in participants, as this has a significant impact on their actions in an emergency. Targeted insertion of additional scenario elements can help achieve this.

Active use of tools & resources

The use of tools and resources should be as practical as possible in exercises. Access to process documents, contact lists, or the use of incident tracking tools should be tested live during an exercise.

AONIC
digital. together.

AMA

Ask me anything about cybersecurity

Contact

Teamlead Cybersecurity Consulting

Dr. Gökhan Bal

goekhan.bal@aonic.de

Aonic GmbH, Europaplatz 5, 64293 Darmstadt

+49 6151- 4 93 26 30

info@aonic.de

www.aonic.de

de.linkedin.com/company/aonic-gmbh


Let's start. together.