Navigering av Sikkerhetslandskapet

DORA, NIS-2, og Tiber-NO

CHRIS DALE

- CHO, Principal and Founder at River Security
- Principal Instructor at SANS
- Ex. CISO

- Short summary:

I show how criminals break-in, and I help throw them back out…

CERTS

GCIH	GIAC Certified Incident Handler
GPEN	GIAC Certified Penetration Tester
GSLC	GIAC Security Leadership
GIAC	GIAC Mobile Device Security Analyst
GDAT	GIAC Defending Advanced Adversaries
GCTI	GIAC Cyber Threat Intelligence
GCFA	GIAC Certified Forensic Analyst
GXIH	GIAC Experienced Incident Handler
GXPT	GIAC Experience Penetration Tester
GSP	GIAC Security Professional

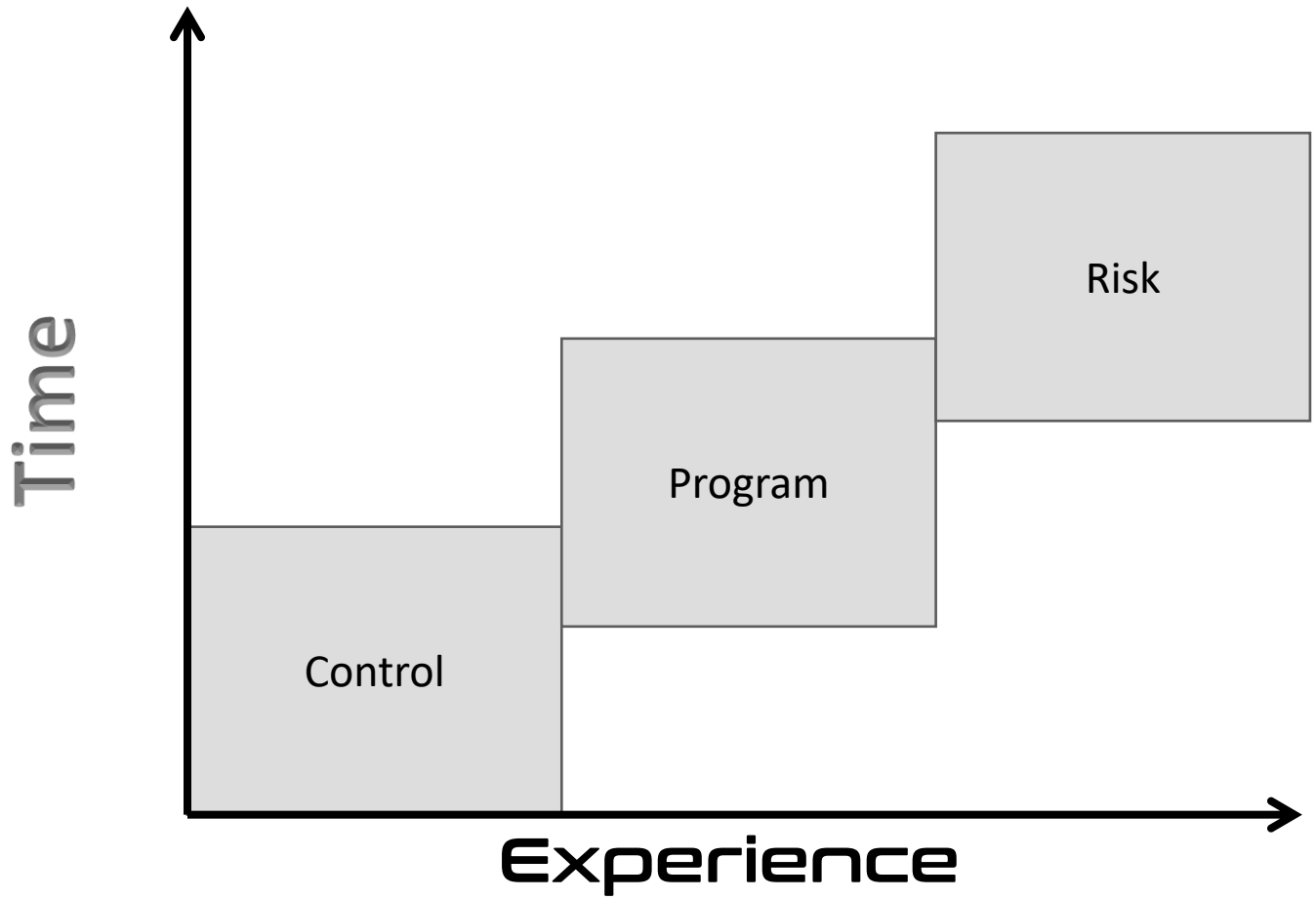
Why This Talk

habet soup of buzzword and topics.
wanted to better understand these frameworks myself
Help others learn too
fensive Services and Incident Response closely align with the uirements

enda:
Cyber Security Frameworks
NIS2
DORA
Tiber-EU

Security Frameworks

- Control Frameworks
  - NIST 800-53
  - CIS 18 Controls
  - ISO 27002
- Program Frameworks
  - ISO 27001
  - NIST CSF
- Risk Frameworks
  - NIST 800-39, 800-37, 800-30
  - ISO 27005



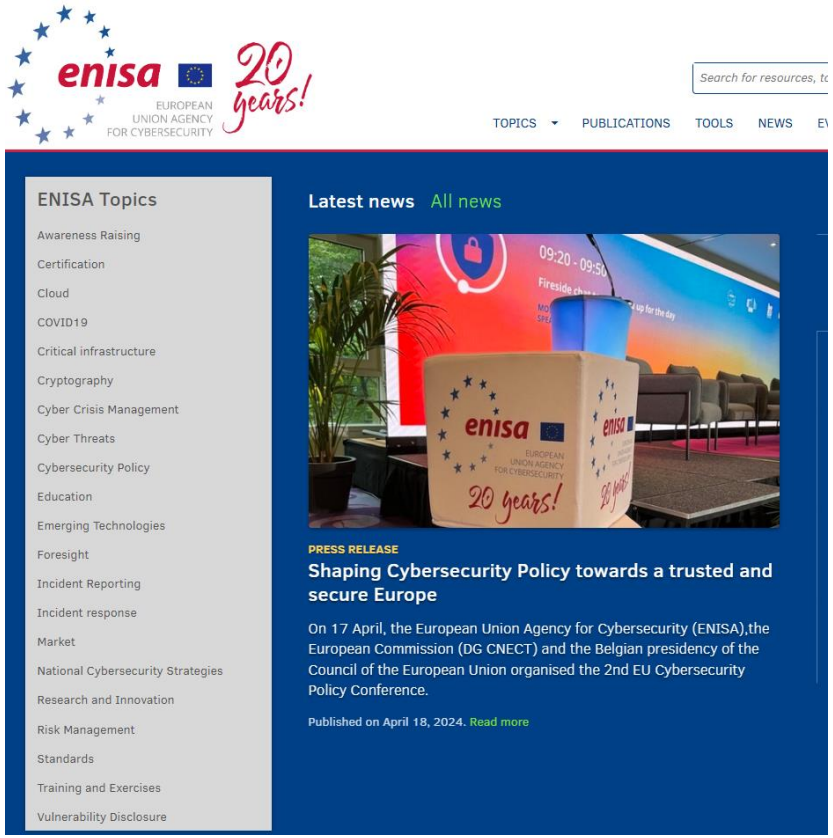
Shout Out to Sounil Yu

Era	1980 Identify	1990 Protect	2000 Detect	2010 Respond	2020 Recover
Core Challenges	What did we buy and how does it support the biz?	Viruses, Server-side Attacks, Insecure Configs	Too many logs and alerts, Client-side attacks	Assume Breach, Raging Fires, Too Many Privileges	Ransomware, MBR Wiper, DDoS, Firmware Bricking
Solutions	Asset Mgt, Systems Mgt Tools	Anti-Virus, Firewalls, Secure Configs	IDS, SIEM	Incident Responders & IR Tools (EDR, SOAR)	Distributed, Immutable, Ephemeral (DIE!!!) Systems
IT / Security Tension	SECURITY (CISO) / STABILITY (CIO)				A / B / C
Security Team Composition & Focus	None	Hobby Shop / Vulnerability Mgt	Sec Ops Center / Threat Mgt	Dedicated Biz Unit / Risk Mgt	Choose Your Own Destiny


The need for
frameworks
NIS-2

Key Threats in EU

- Ransomware
  - Lockbit and the throves of actors
- Supply Chain
  - Solarwinds, SSH Xz Compression library
- War in Ukraine / Russia
  - Signals, connectivity, destruction
- Industrial and State Espoinage
  - NXP looted for 2 years
  - Swizz aviation compromised for multitude of years
- Foreign interference
  - EU elections, influence operations, PsyOps
- ICT supply chain risks
  - 5G and dependencies on third countries
- Emerging Threats
  - Vulnerabilites, Known Exploitable Vulnerabilities, Deep Fake Attacks, Social Engineering



NIS2 – 3 Pillars

National Capabilities

- CSIRT
- Strategy
- Cyber Crisis Management Framework
- Cyber Authorities

EU Collaboration

- Strategic
- Technical
- Risk management
- Supply chain risk assessment coordination

Supervision of Critical Sectors

- Security measures
  - Risk based approach
- Incident reporting
  - Inform Authorities

NIS2 Sectors Included

- Energy, including electricity, oil, and gas
- Transport, covering air, rail, water, and road transport
- Banking
- Financial Market Infrastructures
- Health sector, including healthcare providers
- Drinking water, encompassing both supply and distribution
- Waste water, including sewage and treatment facilities
- Digital infrastructure, such as DNS services, data centers, and trust services
- Public administration
- Space

NIS2 Critical Sectors

- Energy
- Transp
  transpo
- Bankin
- Financi
- Health
- Drinkin
  distribu
- Waste
  facilities
- Digital infra
  centers, and trust services
- Public administration
- Space

Including

Third Party

IT Suppliers

NIS2 – 10 Minimum Requirements

Policies and procedures on cybersecurity risk management	You need to **assess** risk and define security policies for information systems
Incident Handling	Have **plans** for dealing with incidents, and be ready to do **reporting** when something has happened
Business Continuity	Ensure **plans** are made for managing business operations during and after a security incident.
Supply Chain Security	Understand which **provides** you have and do risk management accordingly.
Basic cyber hygiene practices and training	Put your staffing through **updates on your policies, procedures and best practice**.
Policies and procedures for use of crypto, where appropriate encryption	Data in **transit** and **at-rest** should be considered encrypted. Start with plans and procedures so enforcement and governance can begin.
Use of MFA and continuous authentication	**Get it done!** Replace passwords with tokens. Use password managers.

Source: https://nis2directive.eu/nis2-requirements/

NIS2: Incident Handling

- Disclosure requirements in three different levels
- Requires reporting of **significant** (and large) incidents to CSIRT

Within 24 hours
- Early warning
- Incident is *suspected*

Within 72 Hours
- Initial assessment
- Share key details

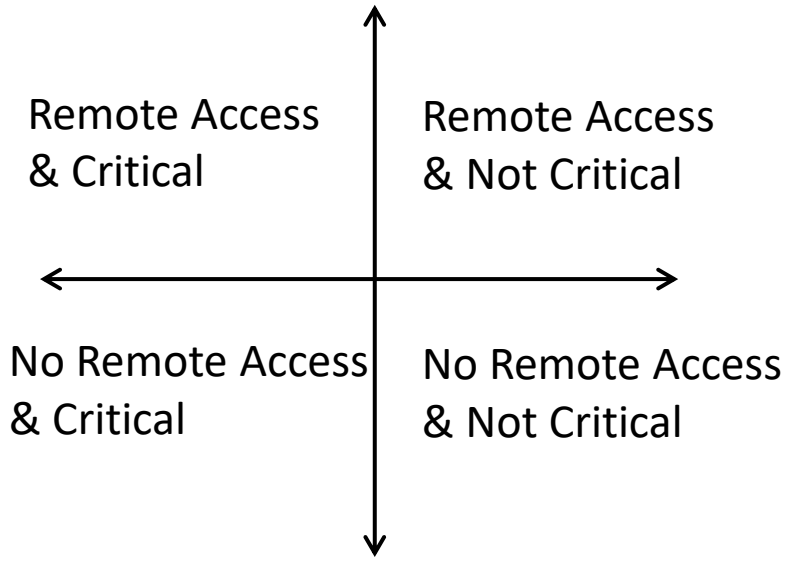
Within 1 Month
- Provide “final” report
- Describe cause and mitigations

NIS2: Supply Chain

- NIS2 requires us to ensure security in our supply chains
- On of the biggest challenges in this is to:
  - Know what suppliers you have
  - Understand how this supplier is significant for you

Discovering Your Supply Chain

- Ask procurement
  - What are you paying for?
  - Highest cost third party, perhaps most important third part
- Consider asking your SoMe / Press team
  - Let them “follow” important providers
- Utilize Offensive SOC, E-ASM and other technology
- Have a plan to consider what happens if something happens to that third party
  - They get hacked / data breach
  - Loss of service



npmjs.com/package/http

Pro Teams Pricing Documentation

npm Search packages Search Sign Up Sign In

http

0.0.1-security • Public • Published 4 years ago

Readme Code Beta 0 Dependencies 2,195 Dependents 2 Versions

Security holding package

This package name is not currently in use, but was formerly occupied by another package. To avoid malicious use, npm is hanging on to the package name, but loosely, and we'll probably give it to you if you want it.

You may adopt this package by contacting support@npmjs.com and requesting the name.

Keywords

none

Install

```
> npm i http
```

Repository
github.com/npm/security-holder

Homepage
github.com/npm/security-holder#readme

Weekly Downloads
220,801

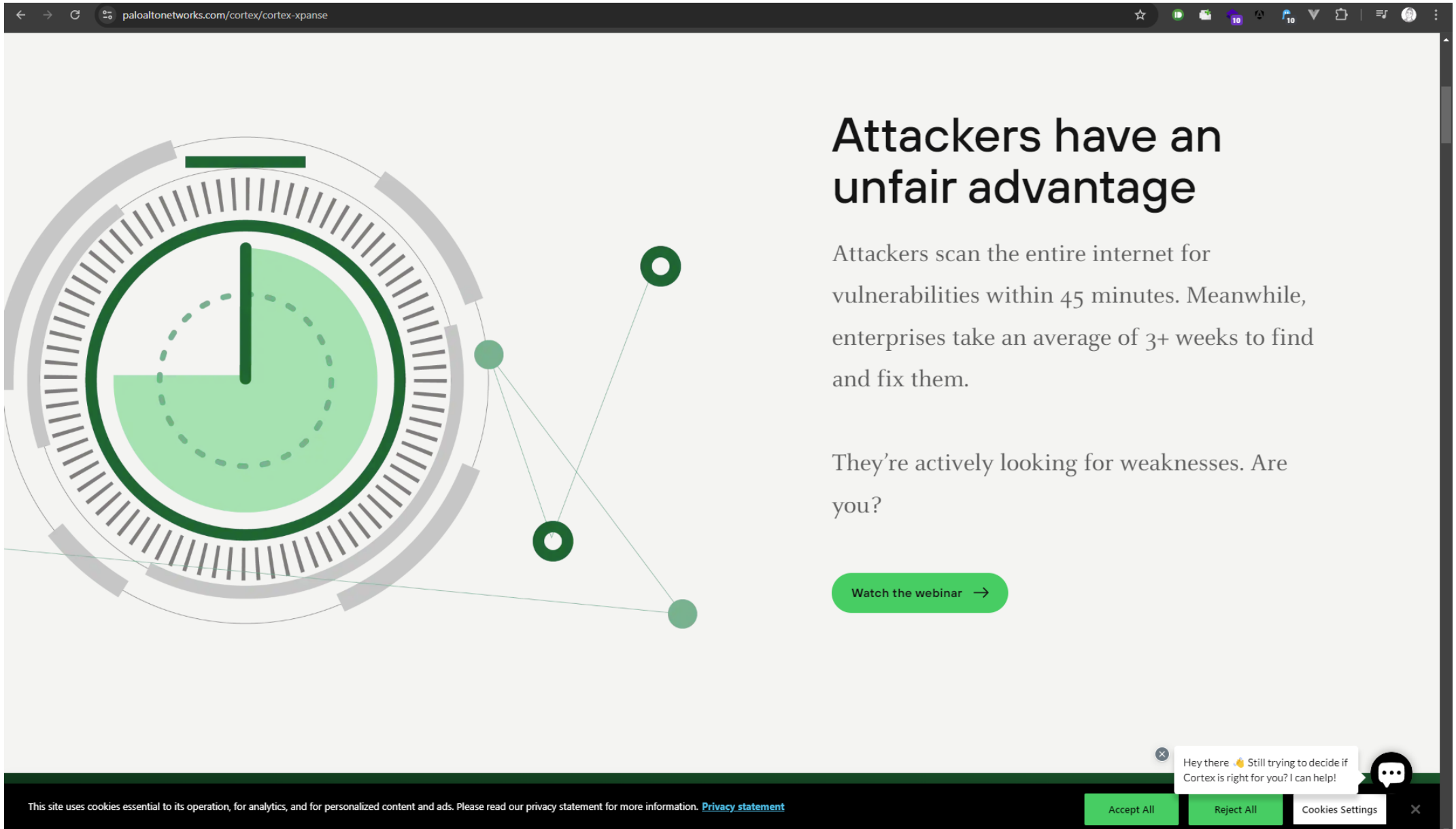
Version
0.0.1-security

License
none

Unpacked Size
464 B

Total Files
2

24 Hours to Patch




Confluence

February 21, 2024 at 3:00 AM EST

PDF Version

Report indicates adversaries seek to disrupt global elections and exploit generative AI technology

AUSTIN, Texas--(BUSINESS WIRE)--Feb. 21, 2024-- CrowdStrike (Nasdaq: CRWD) today announced the findings of the 2024 CrowdStrike Global Threat Report, highlighting a surge in adversaries leveraging stolen identity credentials to exploit gaps in cloud environments and maximize the stealth, speed and impact of cyberattacks. The report also details the biggest threats on the horizon for 2024, including the disruption of global elections and the exploitation of generative AI to lower the barrier of entry and launch more sophisticated attacks.

In the 10th annual edition of the cybersecurity leader's seminal report, CrowdStrike highlights activity from some of the 230+ prolific threat groups that it tracks today. Key findings in the 2024 report include:

- **Dramatic Increase in Attack Velocity:** The speed of cyberattacks continues to accelerate at an alarming rate. The report indicates that the average breakout time is down to only 62 minutes from 84 in the previous year (with the fastest recorded attack coming in at 2 minutes and 7 seconds). Once initial access was obtained, it took only 31 seconds for an adversary to drop initial discovery tools in an attempt to compromise victims.
- **Stealthy Attacks Spike as Adversaries Compromise Credentials:** The report notes a sharp increase in interactive intrusions and hands-on-keyboard activity (60%) as adversaries increasingly exploit stolen credentials to gain initial access at targeted organizations.
- **Adversaries Follow as Business Moves to the Cloud:** Adversaries turned their sights to the cloud through valid credentials – creating a challenge for defenders looking to differentiate between normal and malicious user behavior. The report shows cloud intrusions increased by 75% overall with cloud-conscious cases amplifying by 110% Year-over-Year.
- **The Exploitation of Generative AI on the Horizon:** In 2023, CrowdStrike observed nation-state actors and hacktivists experimenting with and seeking to abuse generative AI to democratize attacks and lower the barrier of entry for more sophisticated operations. The report highlights

1-10-60 Rule

1

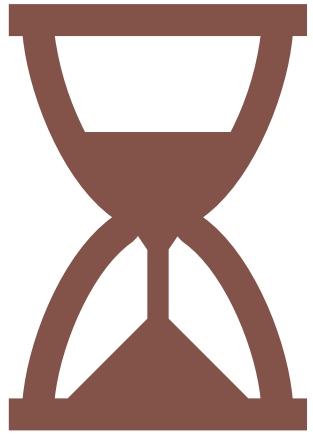
1 Minute

- Detect
- Triage

10

10 minutes

- Investigate
- Understand



60 Minutes

- Remediate
- Contain

DORA

Digital Operational Resiliency Act

The Digital Operational Resiliency Act
Deadline: 2025.01.17 for Financial Entities operating in EU.

Monitoring/enforcement starts 2025.

5 Pillars of DORA

These items are all much more detailed and complex

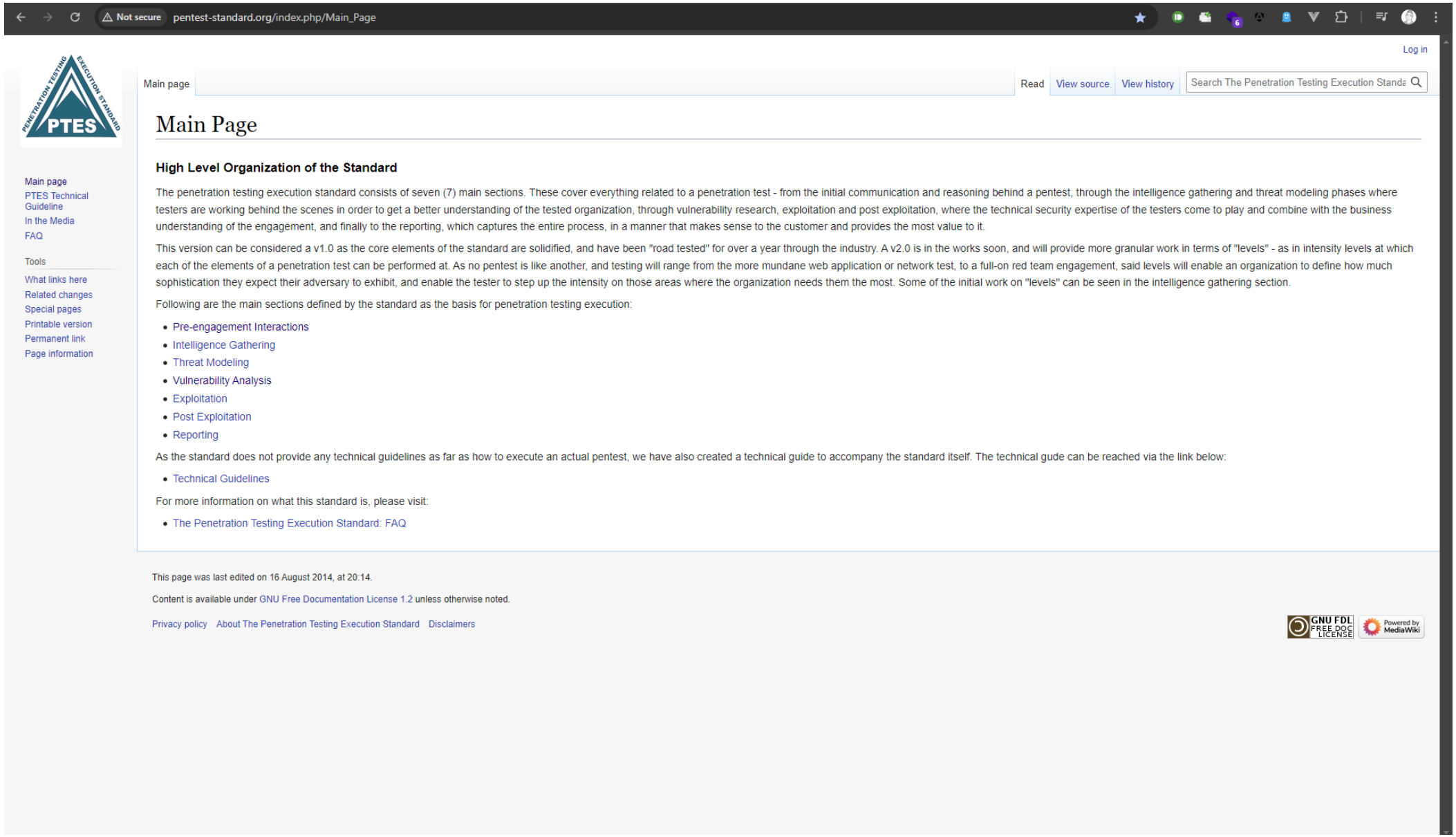
IT Risk Management	You need a framework to **assess** and **manage** risk; you will get audited! There is a focus on accountability and ability to identify important and critical functions. **Know yourself!**
Third Party Risk Management	You have to **identify** and **assess** third parties and monitor critical **third parties.** You also need exit strategies.
Digital Operational Resilience Testing	You must do “basic” and “advanced” **penetration testing** . Vulnerability scanning is not enough. Yearly “basic” pentesting, and every 3rd year “advanced” pentesting.
IT Incident Reporting	Have **plans** for incidents and **report major IT incidents** to authorities. You need to report **early and often**… You need to classify and log all IT incidents and determine which ones are “major”. Exist templates exist!
Information Sharing	**Act** on Threat Intelligence sharing - ensure threat intelligence is exchanged.

Source: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Digital Operational Resilience Testing

- Penetration Testing is a requirement
  - “Basic” testing once a year
  - “Advanced” testing once every three year
- Vulnerability scanning and assessment is still necessary
- The methodologies for penetration testing should be up to date with the latest cybersecurity developments.

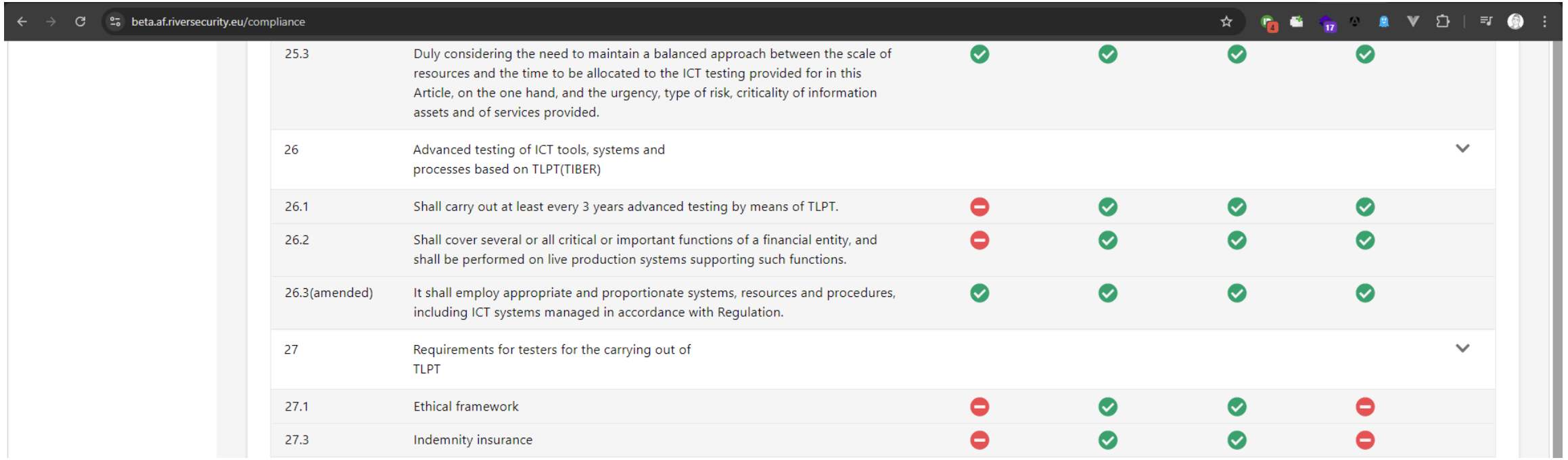
Pentest Execution Standard



Basic vs. Advanced Testing

DORA & Tiber

- TLPT – Threat Lead Penetration Testing
  - TIBER – Threat Intel Based Ethical Red teaming…
  - Aim is to make organizations resilient



25.3	Duly considering the need to maintain a balanced approach between the scale of resources and the time to be allocated to the ICT testing provided for in this Article, on the one hand, and the urgency, type of risk, criticality of information assets and of services provided.	✓	✓	✓	✓
26	Advanced testing of ICT tools, systems and processes based on TLPT(TIBER)				
26.1	Shall carry out at least every 3 years advanced testing by means of TLPT.	⊖	✓	✓	✓
26.2	Shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions.	⊖	✓	✓	✓
26.3(amended)	It shall employ appropriate and proportionate systems, resources and procedures, including ICT systems managed in accordance with Regulation.	✓	✓	✓	✓
27	Requirements for testers for the carrying out of TLPT				
27.1	Ethical framework	⊖	✓	✓	⊖
27.3	Indemnity insurance	⊖	✓	✓	⊖

Challenges with Pentesting – Speed and Agility

Key To Success

- APT – Advanced **Persistent** Threat
- Know the target better than the target know themselves
- Waiting game, patience, and you get in

Tiber-EU/NO In A Nutshell

- Simulated cyberattacks on critical financial infrastructures to assess and improve their defense mechanisms against real cyber threats.

TIBER-NO
Red Team Test Plan Guidance

Version 0.1

1 Introduction

This is practical guidance produced by TCT-NO to support and guide how to produce the Red Team Test Plan (RTTP) in TIBER-NO tests. The figure below shows the Red Team test phase in the TIBER-EU process.

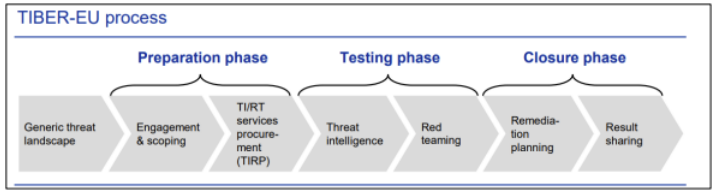
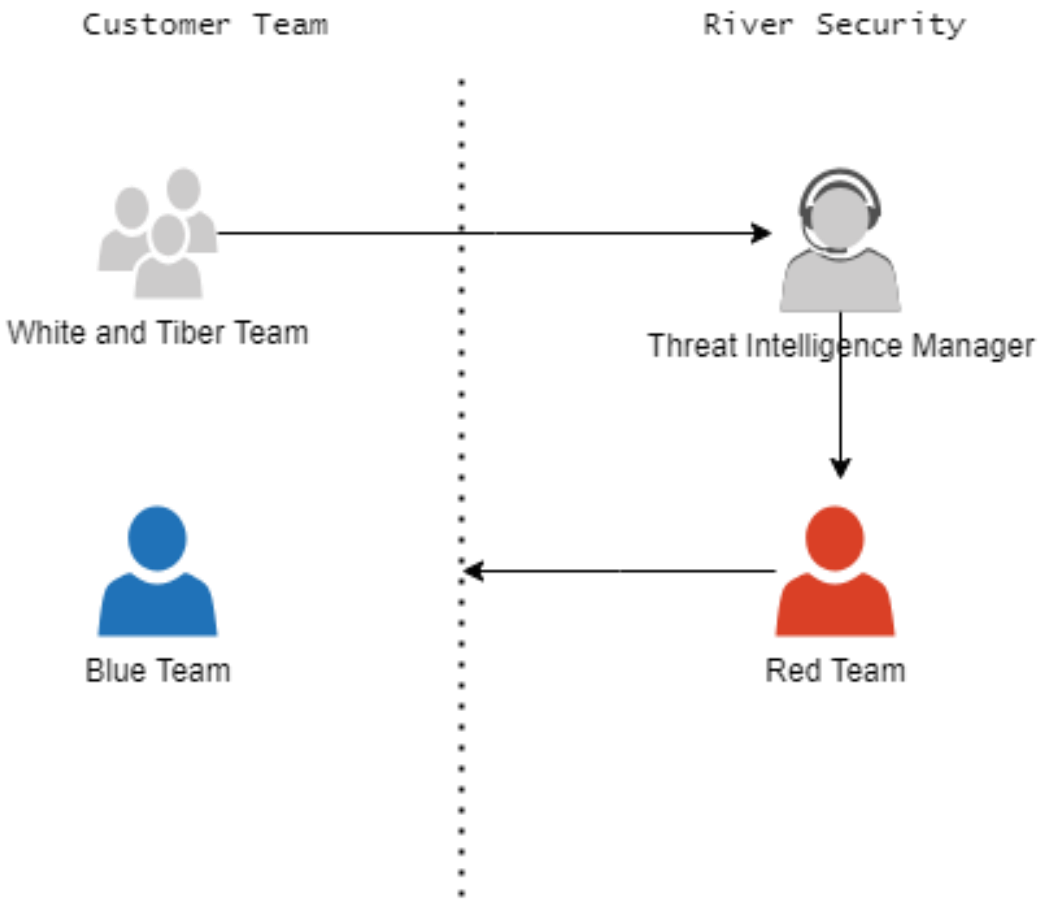
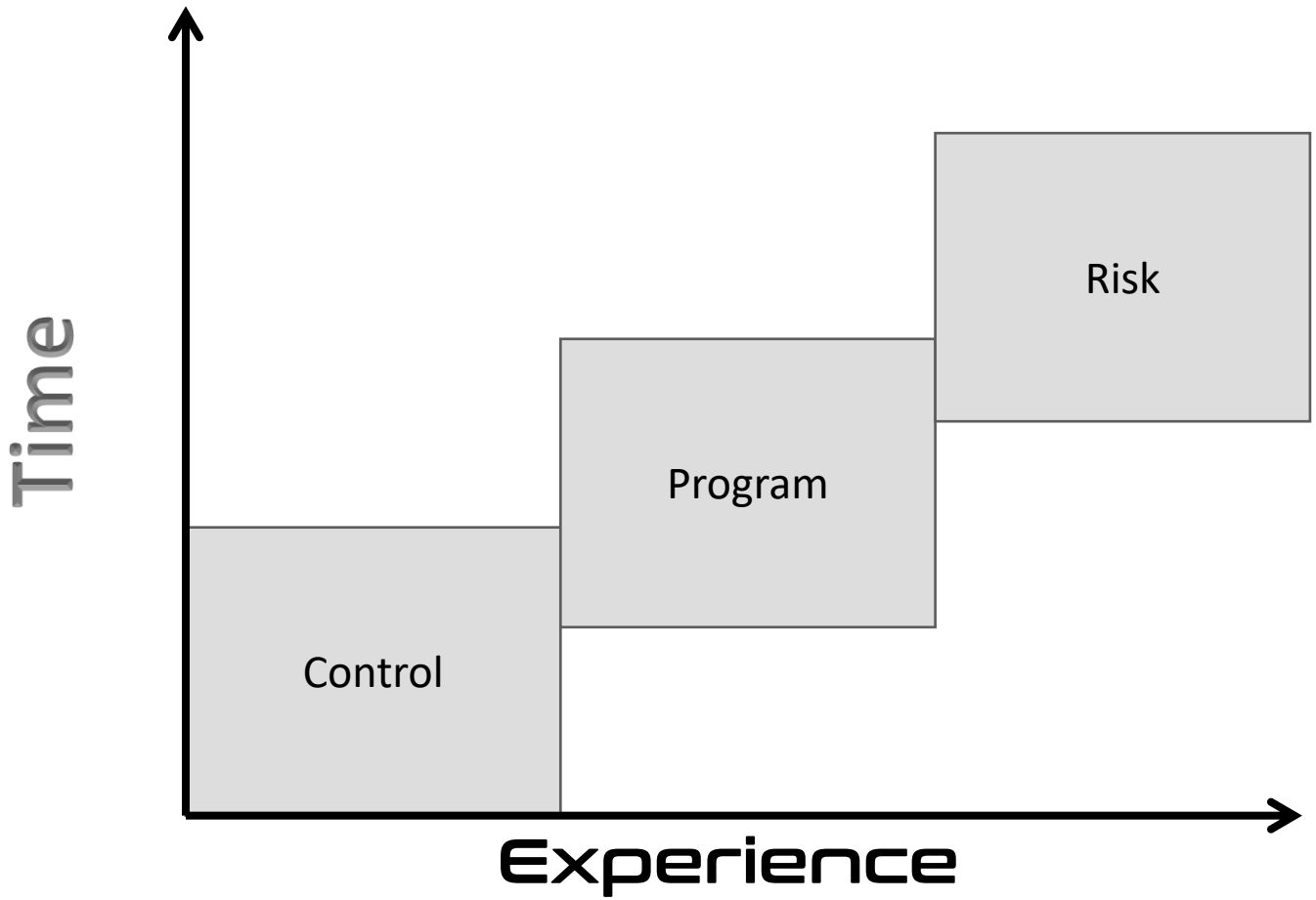


Fig: TIBER-EU process



Security Frameworks

- Control Frameworks
  - TIBER
- Program Frameworks
  - NIS2
- Risk Frameworks
  - DORA



RIVER SECURITY

https://into.bio/chrisdale & https://into.bio/rivsec

Download slides here!

Twitter – https://twitter.com/ChrisADale

LinkedIn – https://www.linkedin.com/in/chrisad/

Fighting Cyber Crime – https://riversecurity.eu