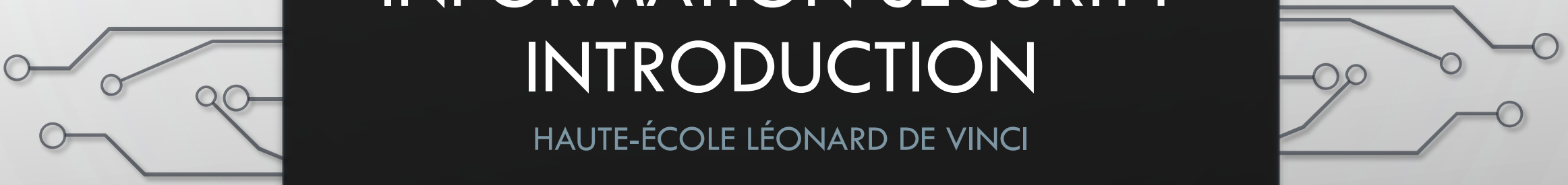


INFORMATION SECURITY INTRODUCTION

HAUTE-ÉCOLE LÉONARD DE VINCI

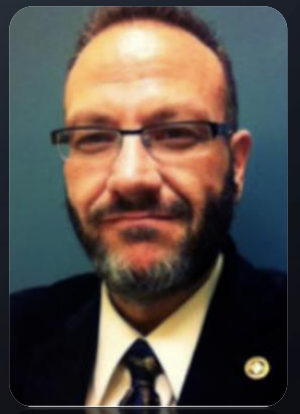
CHAPTER 1 - GENERALITIES

Cyber security is not something you learn in a Masters Degree.

It is something you learn from years of experience across the broad spectrum of IT.

This cannot be bypassed.

- Randall Frietzche



CHAPTER 1

- 1.1 Cybersecurity Objectives
- 1.2 Threat Landscape
- 1.3 Malicious Code
- 1.4 Threat Intelligence Tools
- 1.5 To Learn and Have Fun

1.1 CYBERSECURITY OBJECTIVES

- Why does cybersecurity exists ?
- What are cybersecurity objectives ?
- What does it protects ?

1.1 CYBERSECURITY OBJECTIVES

1.1 CYBERSECURITY OBJECTIVES

The three key objectives of cybersecurity are:

Confidentiality

Integrity

Availability

The CIA Triad

1.1 CONFIDENTIALITY

Confidentiality ensures that unauthorized individuals are not able to gain access to sensitive information.

1.1 INTEGRITY

Integrity ensures that there are no unauthorized modifications to information or systems, either intentionally or unintentionally.

1.1 AVAILABILITY

Availability ensures that information and systems are ready to meet the needs of legitimate users at the time those users request them.

1.1 CYBERSECURITY OBJECTIVES

Cybersecurity professionals develop and implement *security controls* to meet these objectives.

Examples:

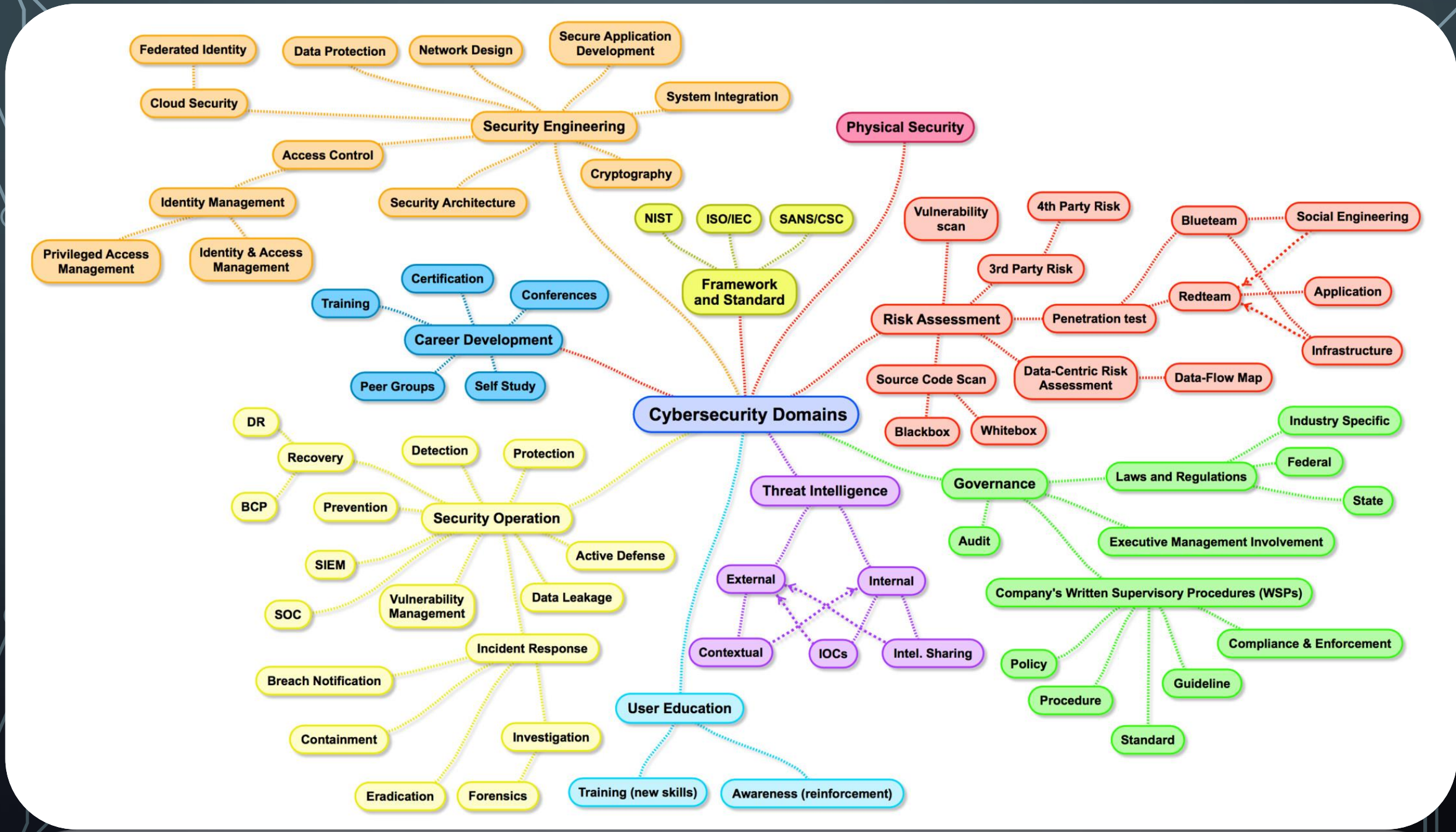
Confidentiality: firewalls, encryption, access control lists, ...

Integrity: hashing, digital signature, read-only, ...

Availability: clustering, load-balancing, backups, ...

CYBERSECURITY CONTAINS MULTIPLE DOMAINS.

IT'S BIG !


Cybersecurity Domains
Security Engineering
Federated Identity
Data Protection
Network Design
Secure Application Development
Cloud Security
System Integration
Access Control
Cryptography
Identity Management
Security Architecture
Privileged Access Management
Identity & Access Management
Physical Security
NIST
ISO/IEC
SANS/CSC
Framework and Standard
Certification
Training
Conferences
Career Development
Peer Groups
Self Study
Vulnerability scan
4th Party Risk
3rd Party Risk
Risk Assessment
Penetration test
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
DR
Recovery
Detection
Protection
BCP
Prevention
Security Operation
SIEM
Active Defense
SOC
Vulnerability Management
Data Leakage
Incident Response
Breach Notification
Containment
Investigation
Eradication
Forensics
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Governance
Industry Specific
Federal
Laws and Regulations
State
Audit
Executive Management Involvement
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
Policy
Guideline
Procedure
Standard

1.2 THREAT LANDSCAPE

1.2 THREAT LANDSCAPE

We just introduced the CIA triad, used to describe the three main goals of cybersecurity.

Another model exist that explains the three key threats to cybersecurity.

Each of these three threats, maps directly to one of the CIA Triad.

The DAD Triad

1.2 THREAT LANDSCAPE

The three key threats to cybersecurity are:

Disclosure

Alteration

Denial

1.2 DISCLOSURE

Disclosure is the exposure if sensitive information to unauthorized individuals, otherwise known as *data loss*. It's a violation of the principle of confidentiality.

1.2 ALTERATION

Alteration is the unauthorized modification of information and is a violation of the principle of integrity.

1.2 DENIAL

Denial is the unintended disruption of an authorized user's legitimate access to information. Denial events violates the principle of availability.

1.2 THREAT LANDSCAPE

The DAD triad can be mapped to vulnerabilites or threats.

Examples:

Disclosure: misconfiguration, loss of device, weak encryption, ...

Alteration: power surge, human error, code injection, ...

Denial: DDoS, failure of critical server, accidental activity, ...

100%

OF WHAT IS ON INTERNET WILL BE ATTACKED

1.2 THREAT LANDSCAPE

Exploring Cybersecurity Threats. There are different characteristics that differentiate their types

Understanding the adversary is crucial to defend against them!

1.2 THREAT LANDSCAPE

Internal vs. External: We mainly think of threat actors who exists outside our organizations. However the most dangerous threats come from within: the insider threat.

Sophistication/Capability: Threat actors vary greatly in their level of sophistication and capability. From unsophiscated script kiddie to advanced persistent threat (APT).

Resource/Funding: Like sophistication, they also vary in the resources available to them. Highly organized attackers often have virtually limitless resources.

Intent/Motivation: Attackers vary in their motivation and intent. The script kiddie may be simply out for the fun of it, whereas Nation-states seek to achieve political objectives.

1.2 THREAT LANDSCAPE

A shortway to defines motivation of an actor is the hats hackers wear.

The origin of this approach goes back to the Western films where "good guys" wore white hats and the "bad guys" wore black hats to help distinguish them in the film.

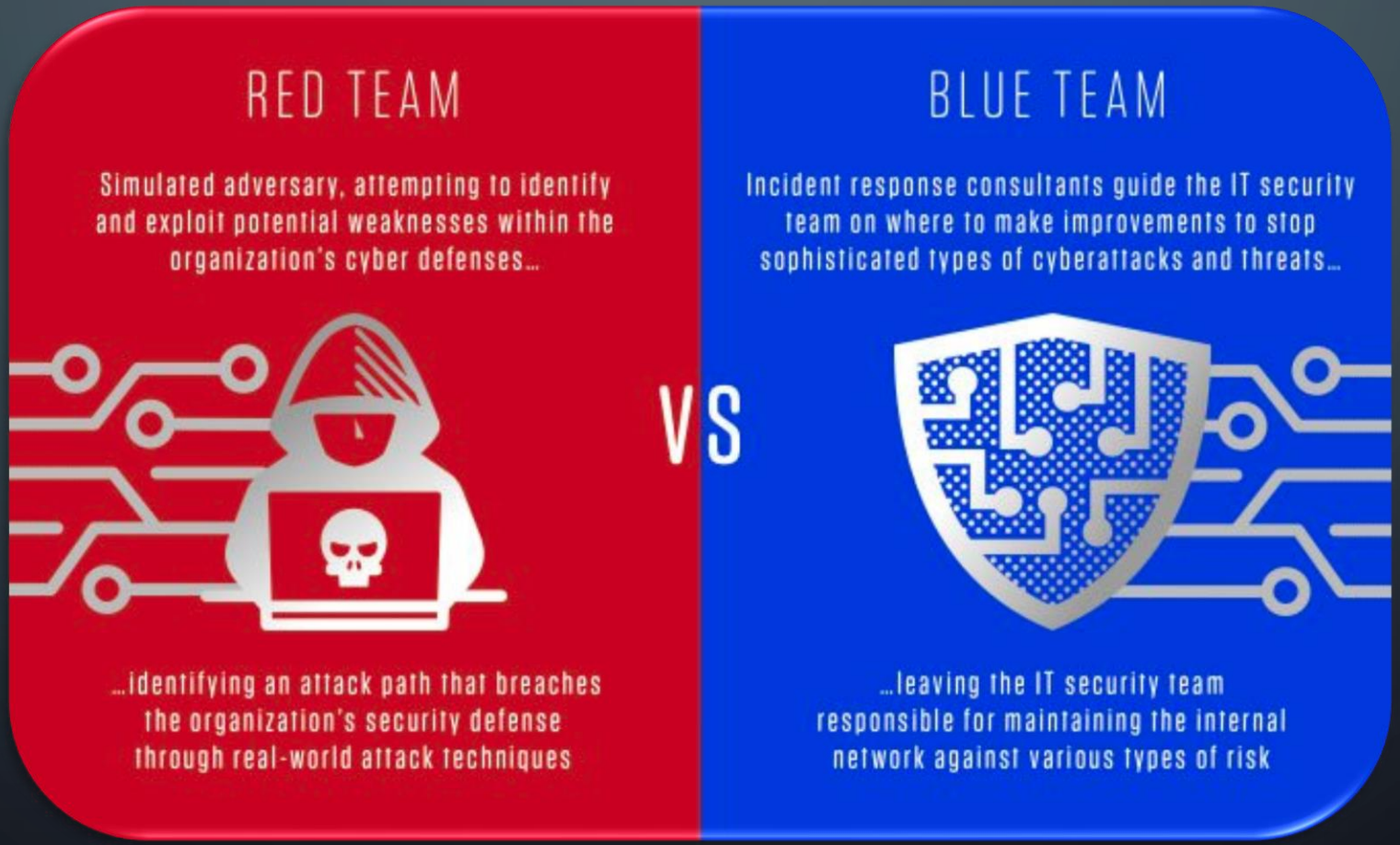
Cybersecurity professional have adopted this approach to describe different type of hackers.

Nevertheless a more precise categorization exists...

1.2 THREAT LANDSCAPE

Script Kiddies	Hacktivists	Criminal Syndicate	APT	Insiders	Competitors
• Use hacking technics but have limited skills. They rely almost entirely on automated tools they download on internet. • Motivation is generaly improving their skill.	• Use hacking technics to accomplish some activist goal. • They believe they are motivated by the greater good, even if their activity violates the law.	• Link to traditional organized crime. Gangs, Mafia • The motive is illegal financial gain	• State actors • Every technologically advanced country • Virtually limitless resources • Motive can be economic or political	• Use of legitimate, authorized access to information and systems to perform an attack against the organization. • Motive can be activism, financial, revenge	• Engaging in corporate espionage to steal sensitive information. • Motivation is theft of customer info, proprietary software, confidential product development plans

1.2 THREAT LANDSCAPE



1.3 MALICIOUS CODE

1.3 MALICIOUS CODE

In this subchapter we will explore the various types of malware, as well as the distinguishing elements, behaviors, traits of each malware type.

The term *malware* describes a wide range of software that are intentionally designed to cause harm to systems, devices, network or users. They can also gather information or provide unauthorized access.

We will also discuss how we can fight them.

1.3 MALICIOUS CODE

Ransomware

Trojans

Worms

Rootkits

Backdoors

Bots

Botnets

Keyloggers

Logic Bomb

Viruses

Spyware

1.3 RANSOMWARE

Ransomware is a malware that takes over a computer and then demands a ransom. There are many types of ransomware, the most famous is the crypto malware, which encrypts files and then holds them hostage until a ransom is paid.

The best defense against a ransomware are:

- an *effective* backup system that stores files in a separate location that will not be impacted by the ransomware.
- antimalware can provide some level of protection.

Famous ransomware: WannaCry, Petya, NotPetya, TeslaCrypt

1.3 TROJANS

Trojans are a type of malware that is typically disguised as legitimate software and providing attackers with a path into system or device.

Remote Access Trojan (RATs) provide attackers with remote access to systems.

Legitimate remote access tools can be used as RATs which can make identification difficult.

Security teams often combat Trojans and RATs using a combination of:

- User security awareness, to encourage users to not download untrusted software
- Deploy antimalware tools

Famous trojans: Zeus, StormWorm

1.3 WORMS

Worms are malware that does not require any user interaction, they self-install. They spread themselves through automated means. They can spread via email attachment, network file shares, exploiting vulnerabilities or other method as well. Which makes them quite dangerous.

Worms countermeasures are:

- Software patches
- Antimalware are helpful
- Firewall can play a role
- User awareness to not open suspicious email attachment

Famous worm: Stuxnet, MyDoom, Conficker...

1.3 ROOTKITS

Rootkits are malware specifically designed to allow attackers to access system through a backdoor. It can includes capability to conceal from detection, modify filesystem drivers, infecting startup code in the Master Boot Record (MBR) of a disk allowing attack against full-disk encryption.

Rootkits can be *extremely* challenging to remove. The best countermeasures are:

- Integrity checking
- Backup and restore process
- Good security practices (patch, secure configuration, privilege management)
- Secure boot
- Antimalware for specific rootkit

Famous rootkits: Sony BMG, Greek wiretaping

1.3 BACKDOORS

Backdoors are methods or tools that provide access that bypass normal authentication and authorization procedures. It can be both hardware or software based.

Manufacturer-installed backdoors are a concern since they may not be disclosed and can be used by attackers if discovered.

Detecting backdoors can sometimes be done by controlling unexpected open ports and services but more complex backdoors that requires a different URL under a web service or that uses traffic encryption cannot.

- Code review (if possible)
- Firewall
- For extreme case: Diverse Double Compiling

Famous backdoors: Back Orifice, WordPress, Joomla, Juniper

1.3 BOTS & BOTNETS

Bots are remotely controlled systems that have a malware infection. They are used by attackers who control them for various action: additional compromise, DoS attacks or spam relays.

Largest botnet to date: 30 million computers named "Bredolab".

Botnet can work as a client-server or Peer-to-peer control model.

IRC used to be famously known to manage client-server botnets but modern botnets rely on HTTPS traffic to help hide Command and Control traffic.

Peer-to-peer networks connects bots to each other making it harder to to take down a single central server.

Many botnets are able to use (fast flux) DNS to better hide.

Famous botnets: Bredolab, Mariposa, Confiker, ...

1.3 BOTS & BOTNETS

Detecting botnets is often accomplished by analysis network traffic using:

- Network monitoring tool IDS and IPS
- Analysing DNS traffic
- Detecting the underlying malware using an antimalware tool
- Endpoint Detect and Response (EDR)

1.3 KEYLOGGER

Keyloggers are programs that capture keystroke, mouse movement or touchscreen.
Keyloggers works in a multitude of way: data capture from the kernel, APIs, script or hardware.

The goal remains the same: acquiring user input to be used by an attacker.

It's difficult to prevent from keylogger.
Normal security best practices remains the only viable option:

- Patching
- Antimalware
- Multifactor authentication can help limit but cannot defeat

For hardware keylogger, only physical inspection of the material can help prevent.

No specificaly famous keylogger.
There are lots of them for free on internet.

1.3 LOGIC BOMB

Logic bombs are malware that are not an independant program. They are a function or piece of code placed inside other programs that will activate upon a certain condition.

They are relatively rare compared to other types of malware. They mainly are a consideration in software development and system management.

As logic bombs are mainly related to software development.
The best approach to avoid them is to use one of the code review model:

- Pair programming
- Over-the-shoulder
- Pass-around code review
- Tool-assisted review
- Formal code review

Famous logic bomb: Medco Health (2003), Fannie Mae (2008), ...

1.3 VIRUSES

A virus is a malicious program that self-copy and self-replicate. Viruses typically have both a *trigger* and a *payload*.

The *trigger* defines the condition for the virus to execute.

The *payload* is what the virus does, delivers or the action it performs.

Viruses come in many varieties:

- Memory-resident (Fileless): remain in memory while the system is running
- Non-memory-resident: execute, spread and then shutdown
- Boot sector: reside inside the boot sector of a drive or media
- Macro: use macros or code inside software

1.3 VIRUSES

Against viruses, nothing works better than:

- Antimalware
- Patching (OS, browser, plug-ins, software in general)
- Network IPS with reputation-based protection / Proxy can prevent access to malicious sites

1.3 SPYWARE

Spyware is malware that is designed to obtain information about an individual, organization or system.

Many spyware track browsing habits, installed software.

Spyware range from innocent to targeting sensitive data. Identity theft, fraud, advertising, …

Spyware are notably used by agencies to spy on politicaly exposed persons, journalists, etc.

Spyware is most frequently combated using:

- Antimalware
- User awarness

Famous spyware: Pegasus, Hermit, …

1.3 MALICIOUS CODE

Real life is not black or white. It's grey.

It has become rare to find a threat that match perfectly one of the definitions we have discussed. In the absolute majority of case today's threat always are a combination of the above.

For example:

The Pegasus spyware: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

The Belgacom hack: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

BUT...

The biggest risk is the user.

Companies spend millions of dollars on firewalls, encryption and secure access devices, and it is money wasted. None of these measures address the weakest link in the security chain.

- Kevin Mitnick

1.4 BREACH IMPACT

1.4 BREACH IMPACT

The impact of a security incident can be wide and depend of the nature of the incident and the type of organization affected.

We can organize the potential impact of a security incident with the following categories.

FINANCIAL

REPUTATIONAL

STRATEGIC

OPERATIONAL

COMPLIANCE

1.4 FINANCIAL RISK

Financial risk, is as the name implies, the risk of monetary damage as a result of a breach.

The impact can be:

- direct, such as rebuilding a datacenter it is physically destroyed
- indirect if a new product is leaked to competitor and beat you to market resulting in potential significant loss

1.4 REPUTATIONAL RISK

Reputational risk occurs when the negative publicity surrounding a security breach causes the loss of goodwill among customers, employees, suppliers, etc.

It is difficult to quantify reputational damage as the impact could be immediate or/and have an impact on future decisions about doing business with your organization.

1.4 STRATEGIC RISK

Strategic risk is the risk that an organization will become less effective in meeting its major goals and objectives as a result of a breach.

1.4 OPERATIONAL RISK

Operational risk is the risk to the organization's ability to carry out its day-to-day activities.

Operational risks may slow down, delay or stop business processes.

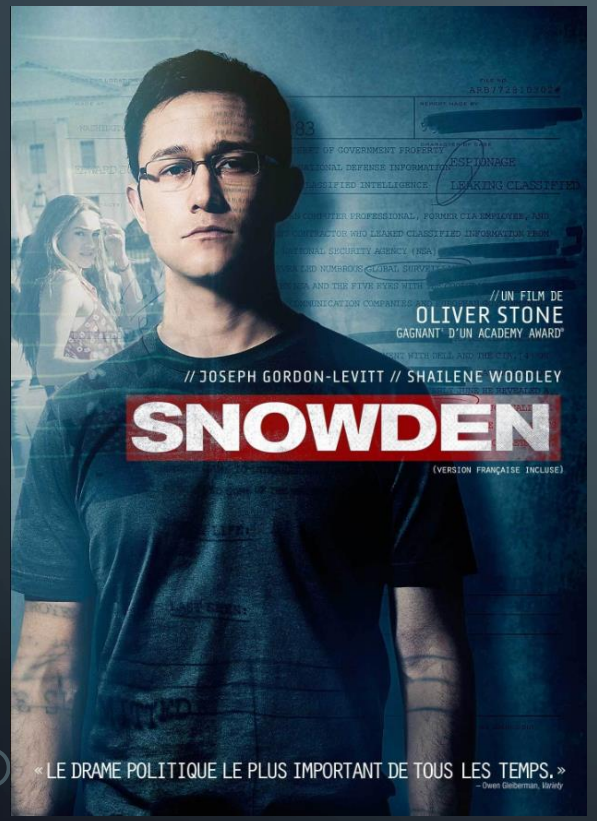
1.4 COMPLIANCE RISK

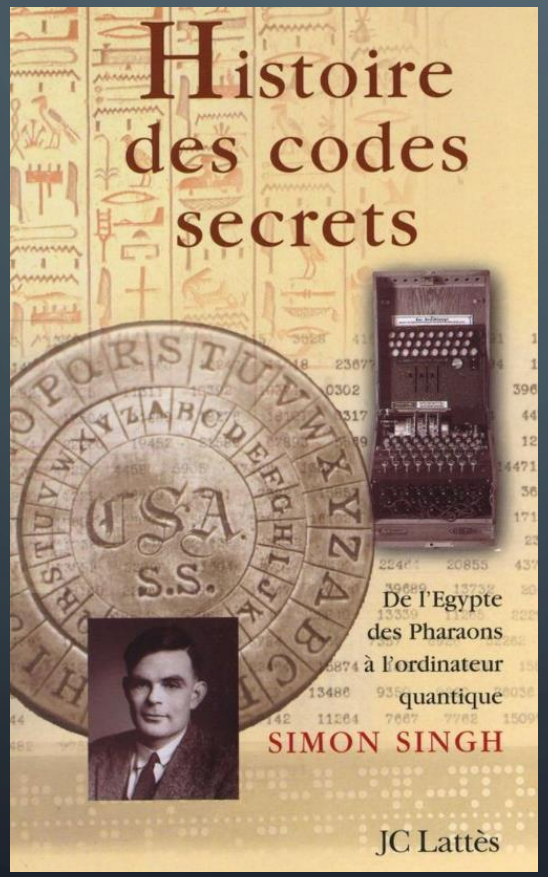
Compliance risk occurs when a security breach causes an organization to not encounter the legal or regulatory requirements.

Ex: GDPR in Europe or HIPAA in the USA

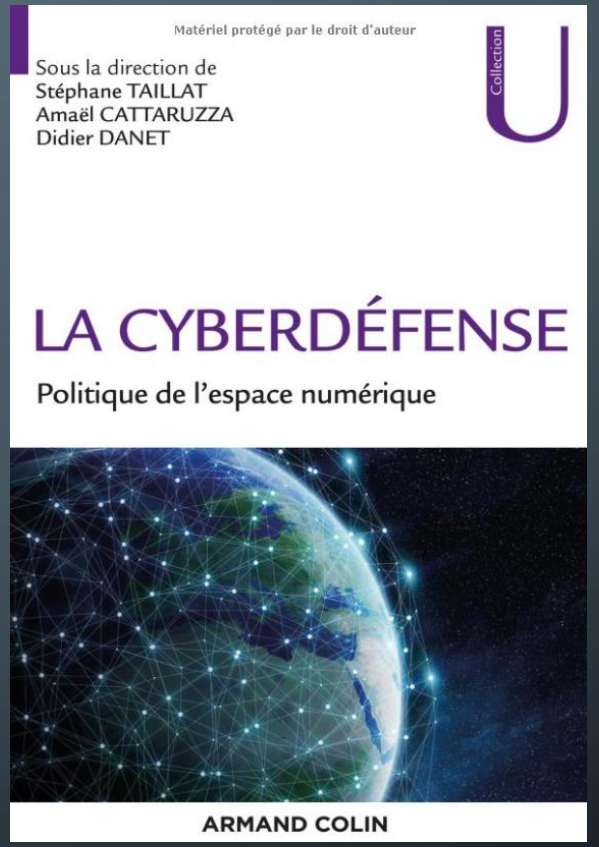
1.5 BOOKS, MOVIES AND TO HAVE FUN

1.5 BOOKS & MOVIES





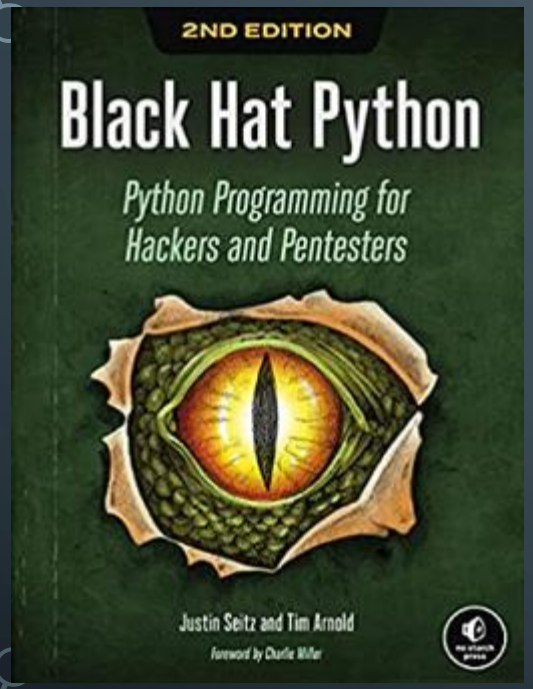
ISBN-13: 978-2070301874



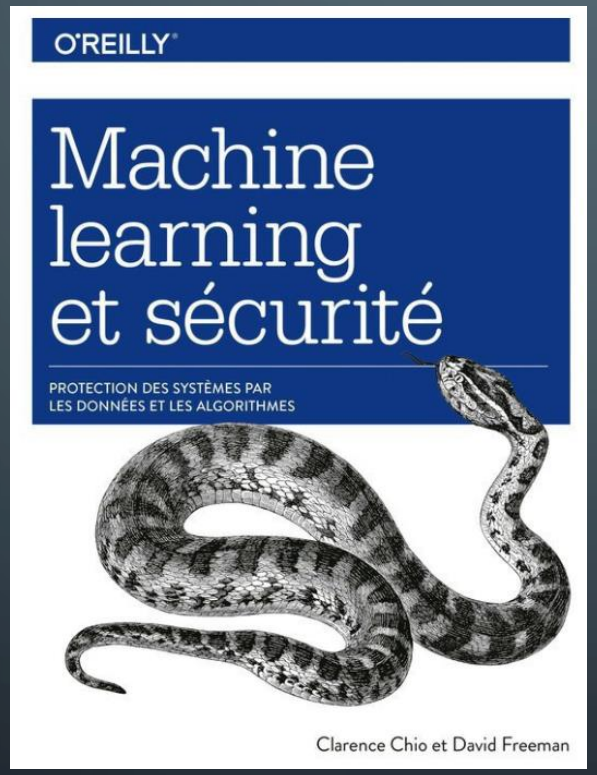
ISBN-13: 978-2200621292

ISBN-13: 979-1093240428

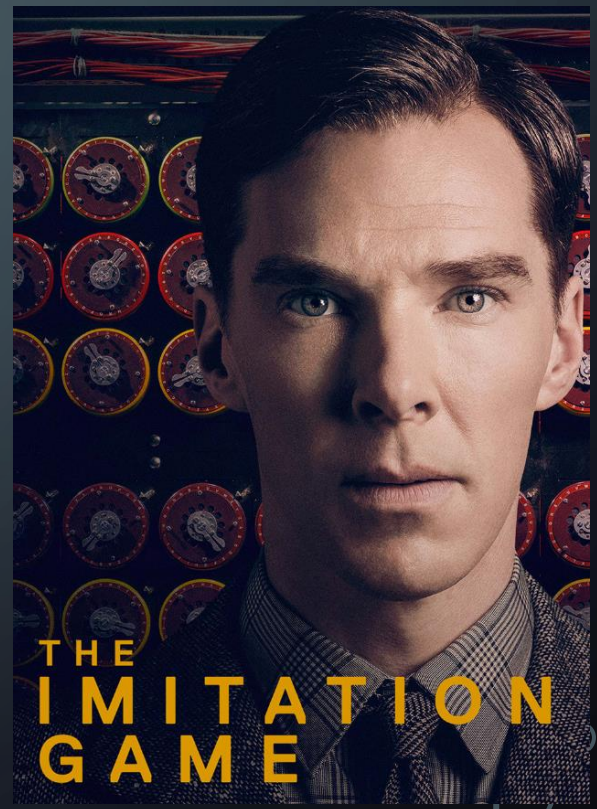
1.5 BOOKS & MOVIES



ISBN-13: 978-1718501126



ISBN-13: 978-2412043561



1.5 TO HAVE FUN

- root-me.org
- Overthewire.org
- Hackthebox.com
- Tryhackme.com
- Metasploitable
- Damn Vulnerable Web Application

https://discord.gg/be-cyber

- Create your own vulnerable application together. The BEST WAY to learn both side!