CYBER SECURITY WORLD

By Mehdi Nacer KERKAR

09/06/2021

WHO AM I

Mehdi Nacer KERKAR

Information Security Student from USDB University

Actually Cyber Security Consultant at Ernest & Young, with principal role of guiding companies on there IT/Cyber transformations leading by a Cyber roadmap (Cybersecurity assessment VAPT, Security Risk Analysis, and management).

You can find me on LinkedIn

/in/mehdi-nacer-kerkar/

WHY ARE WE TALKING ABOUT CYBERSECURITY?

FEW NUMBERS

2021 Cybersecurity Trends

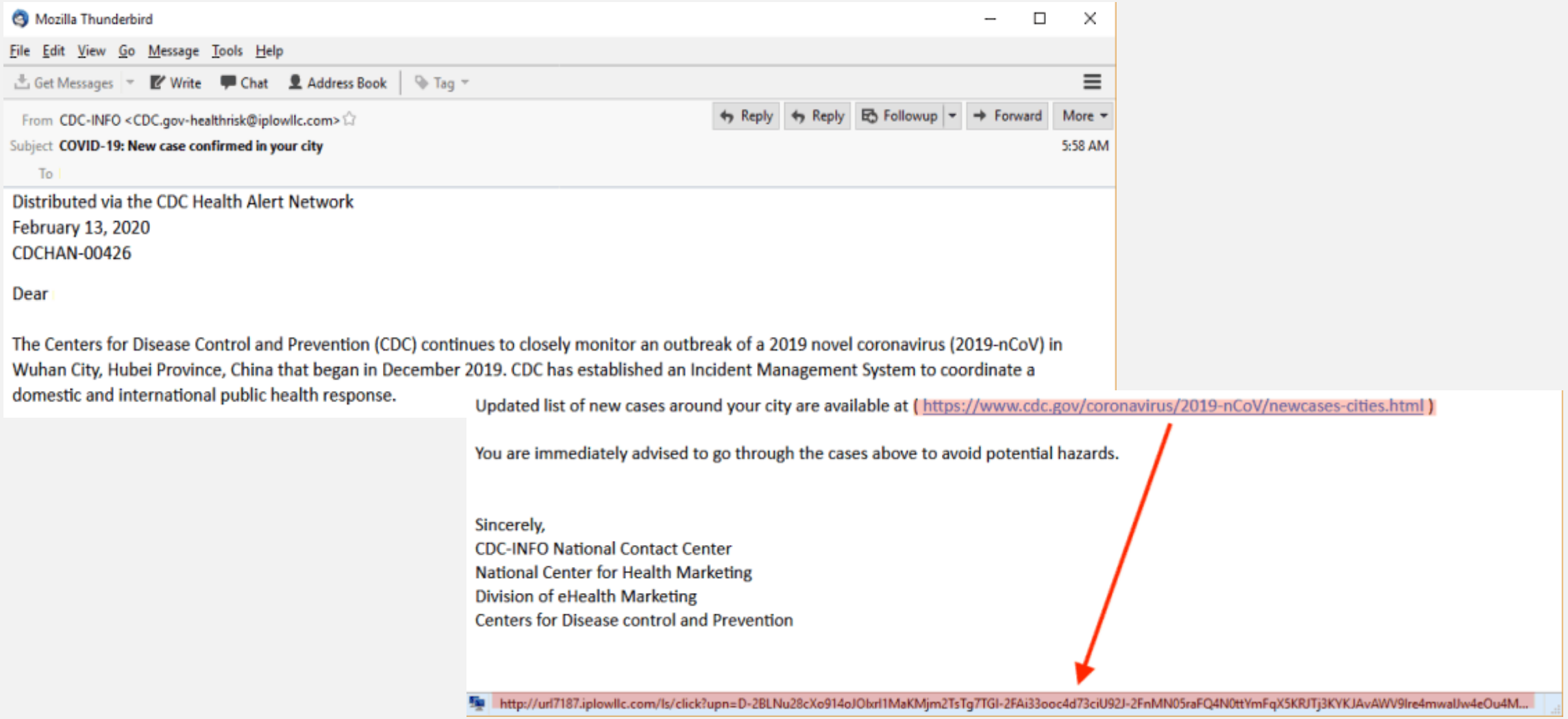
- 95% of cybersecurity breaches are caused by human error. (Cybint)
- The worldwide information security market is forecast to reach $170.4 billion in 2022. (Gartner)
- 88% of organizations worldwide experienced spear phishing attempts in 2019. (Proofpoint)
- 68% of business leaders feel their cybersecurity risks are increasing. (Accenture)
- On average, only 5% of companies' folders are properly protected. (Varonis)

FEW NUMBERS

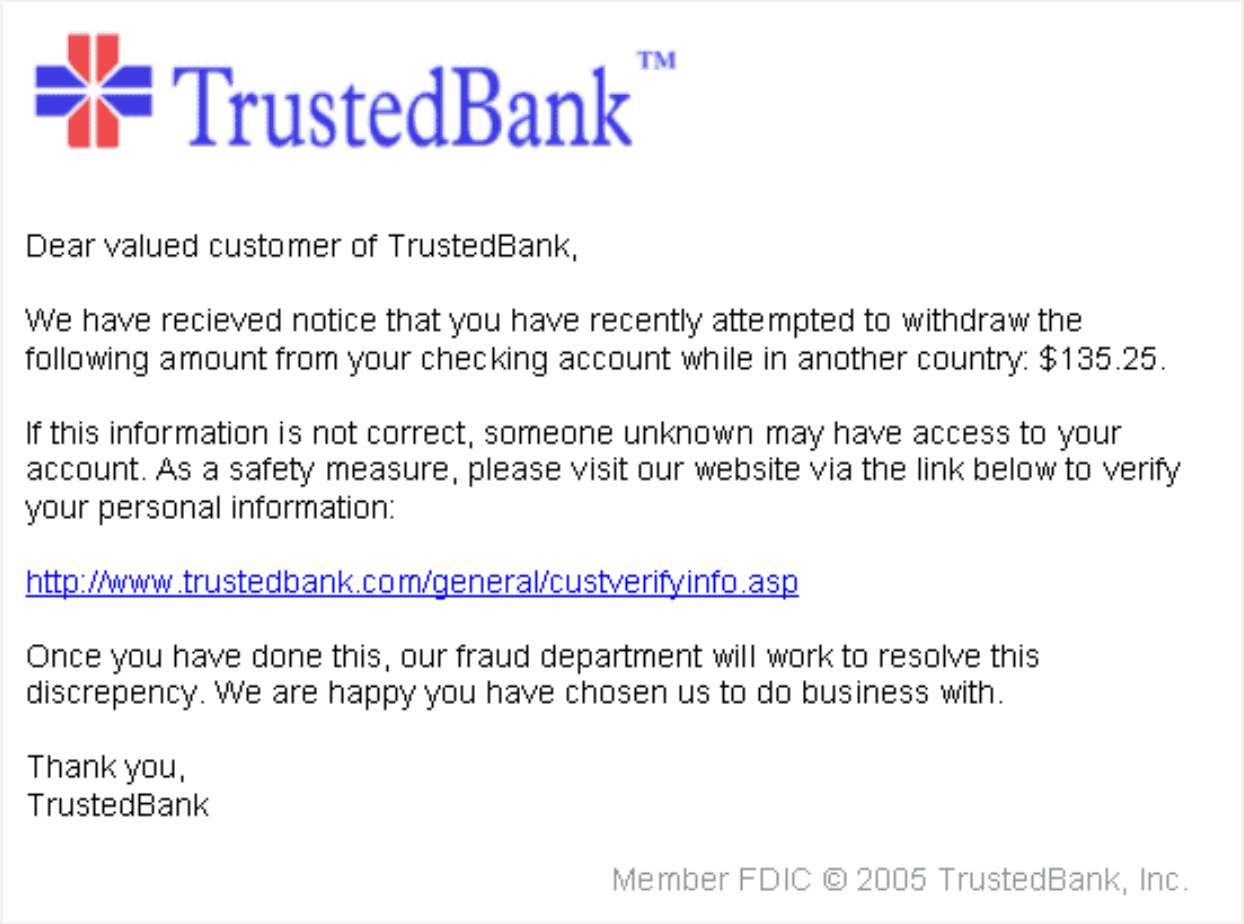
2021 Cybersecurity Trends

- Data breaches exposed 36 billion records in the first half of 2020. (RiskBased)
- An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)
- 86% of breaches were financially motivated and 10% were motivated by espionage. (Verizon)
- 45% of breaches featured hacking, 17% involved malware and 22% involved phishing. (Verizon)
- The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%. (Symantec)

CYBERCRIME UP 600% DUE TO COVID-19 PANDEMIC



CYBERCRIME UP 600% DUE TO COVID-19 PANDEMIC



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

These emails are designed to deceive and trick recipients into taking an action such as clicking a malicious link, or opening an attachment with a virus.

WHAT'S REALLY GOING ON HERE

Causes of CyberCrimes:

- Easy to access
- Capacity to store data in comparatively small space
- Complex (Technologies)
- Negligence
- Loss of evidence

Types of CyberCrimes :

- Piracy or Theft
- Cyber Stalking
- Identity Theft
- Computer Vandalism
- Malicious Software
- Fraud Calls/eMails
- Fake news sharing in social media
- Online illegal selling (Dark Web)
- Child pornography and Abuse
- Cyber Terrorism

Contexts :

- Network security
- Application security
- Information security
- Operational security
- Critical infrastructure security
- Cloud security
- Internet of things (IoT) security

WHAT IS "CYBERSECURITY?"

People often believe that cybersecurity is all about technology and hacking. It is somewhat true, but cybersecurity is much more than that.

SOME DEFINITIONS

- n. **cybersecurity**: See "information security"

- n. **information security**: The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

MORE DEFINITIONS

Computer security

From Wikipedia, the free encyclopedia

Computer security, **cybersecurity** or **information technology security** (**IT security**) is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.[1]

The field is becoming increasingly significant due to the increased reliance on computer systems, the Internet[2] and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.[3]

CIA TRIAD


CONFIDENTIALITY
INTEGRITY
Data
protected
by CIA Triad
AVAILABILITY

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

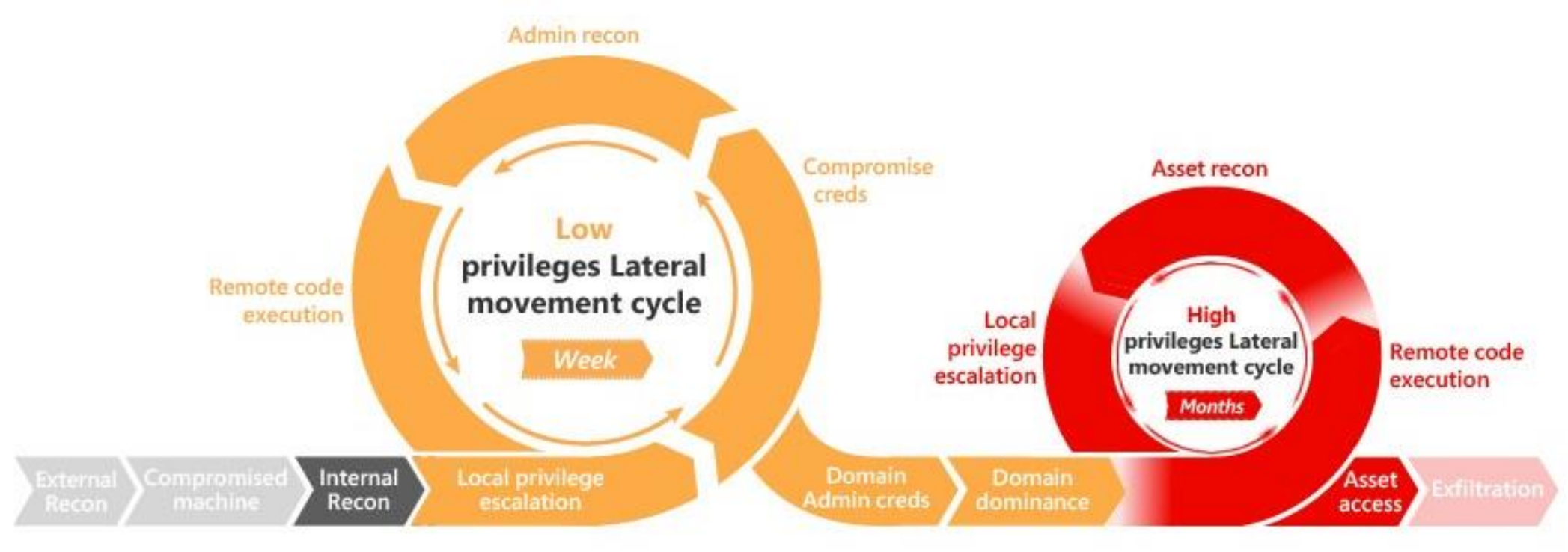
Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to **www.ncsc.gov.uk** **@ncsc**

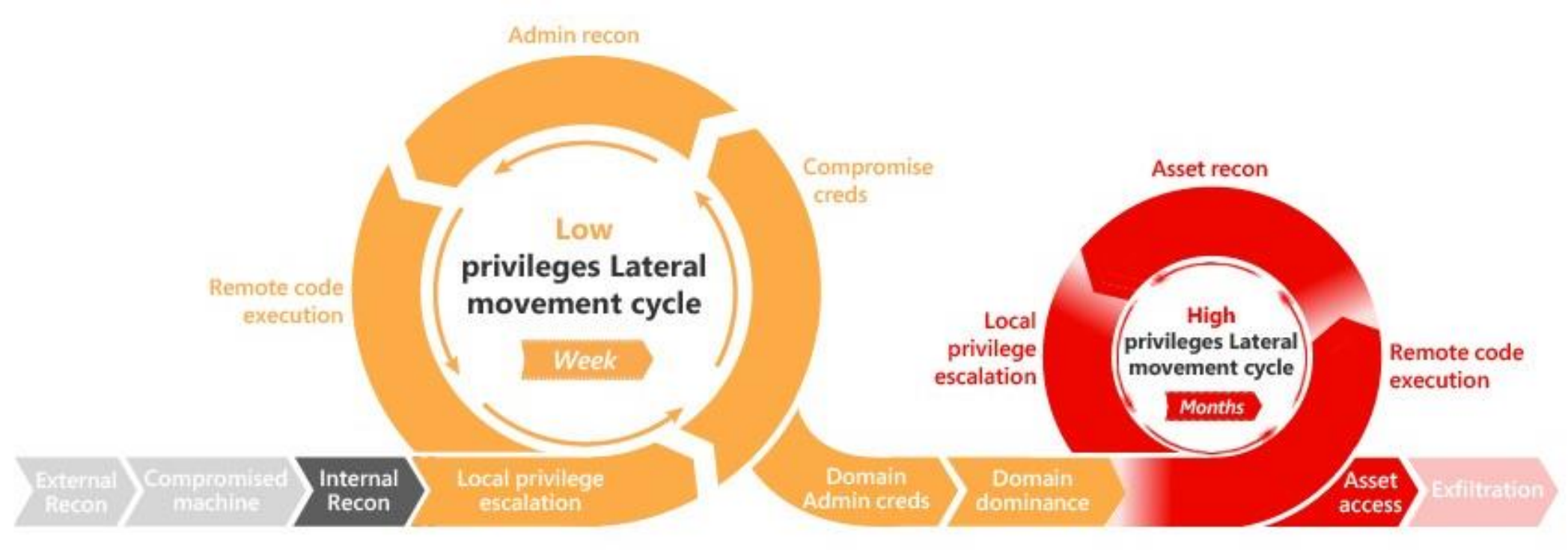
CYBER KILL CHAIN

CYBER KILL CHAIN



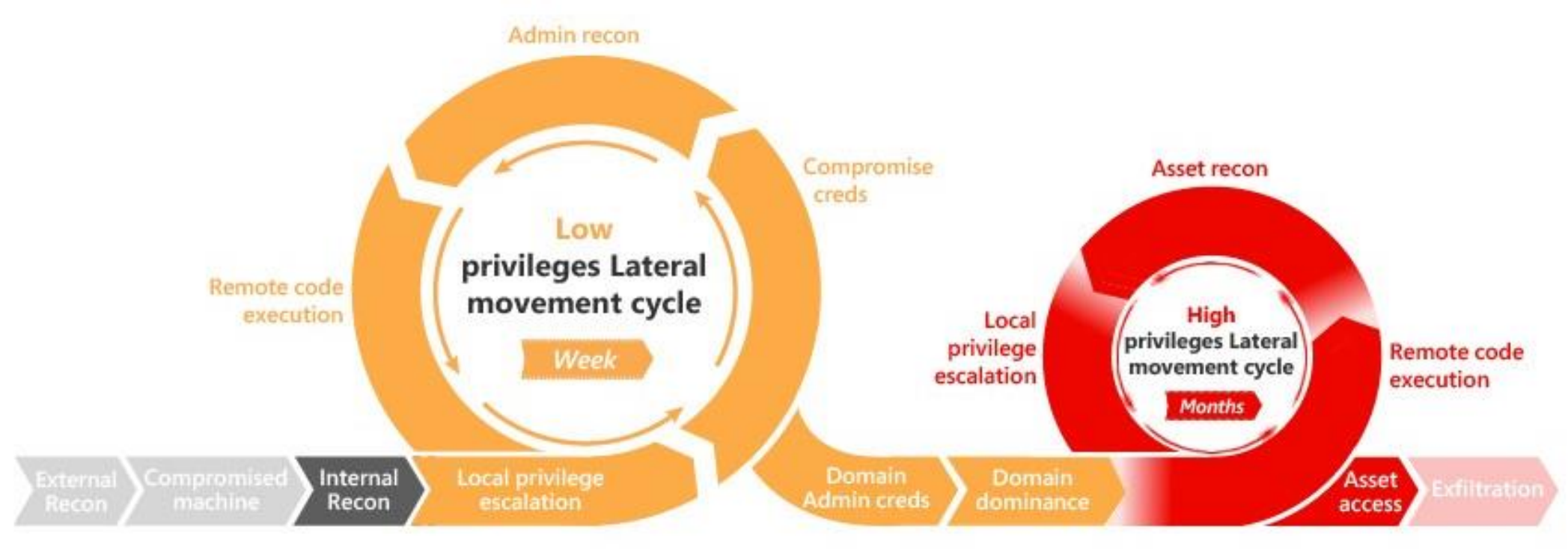
Internal Recon: From there, an Advanced Persistent Threat starts is internal recon and attempts to pivot around the network while leveraging privilege escalation. An APT lives in an environment an average of 200 days before being discovered.

CYBER KILL CHAIN



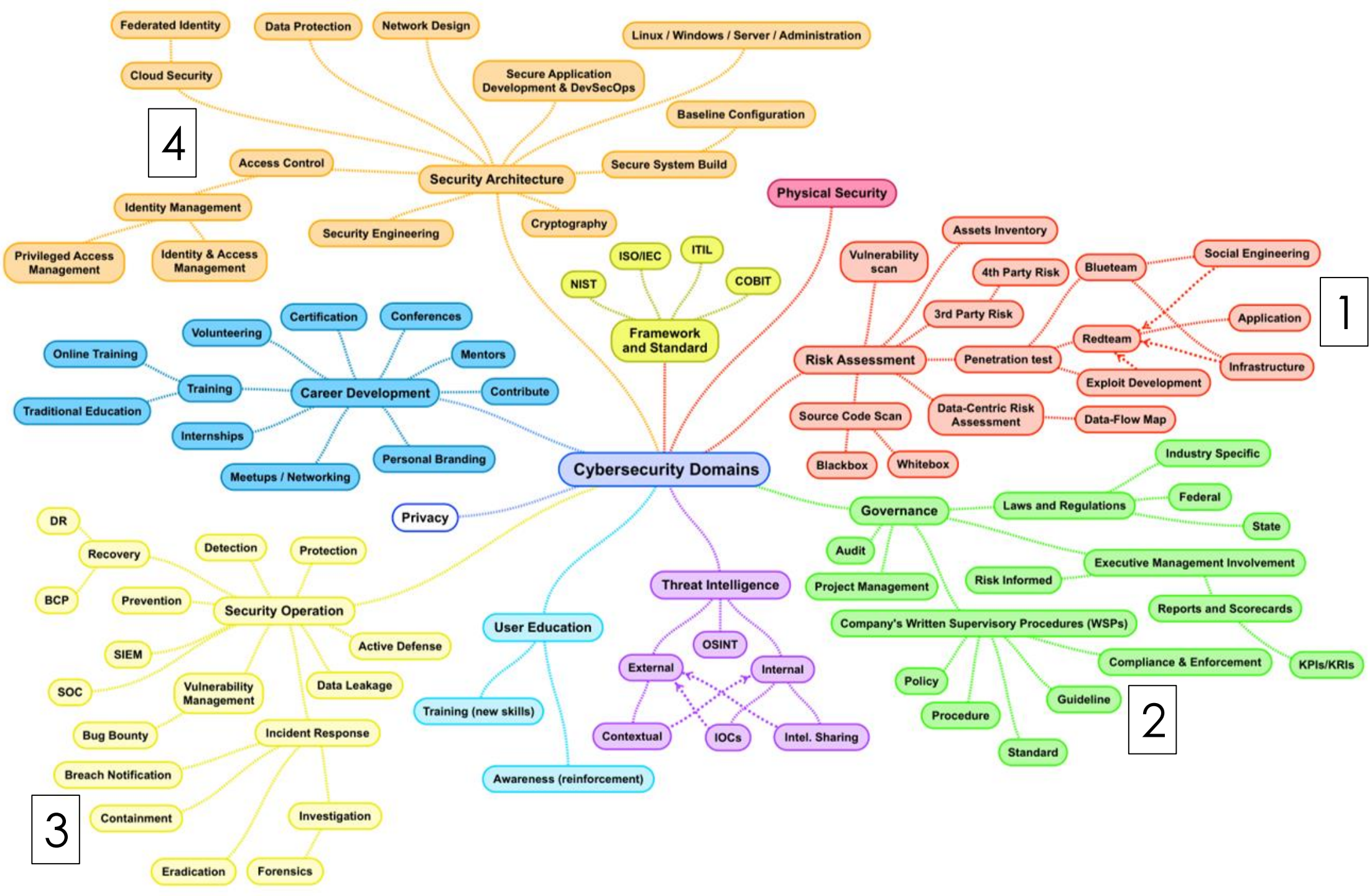
Compromised Machine: 91% of Cyberattacks start with a phishing email, according to a study done by phishing defense company PhishMe in 2016.

CYBER KILL CHAIN



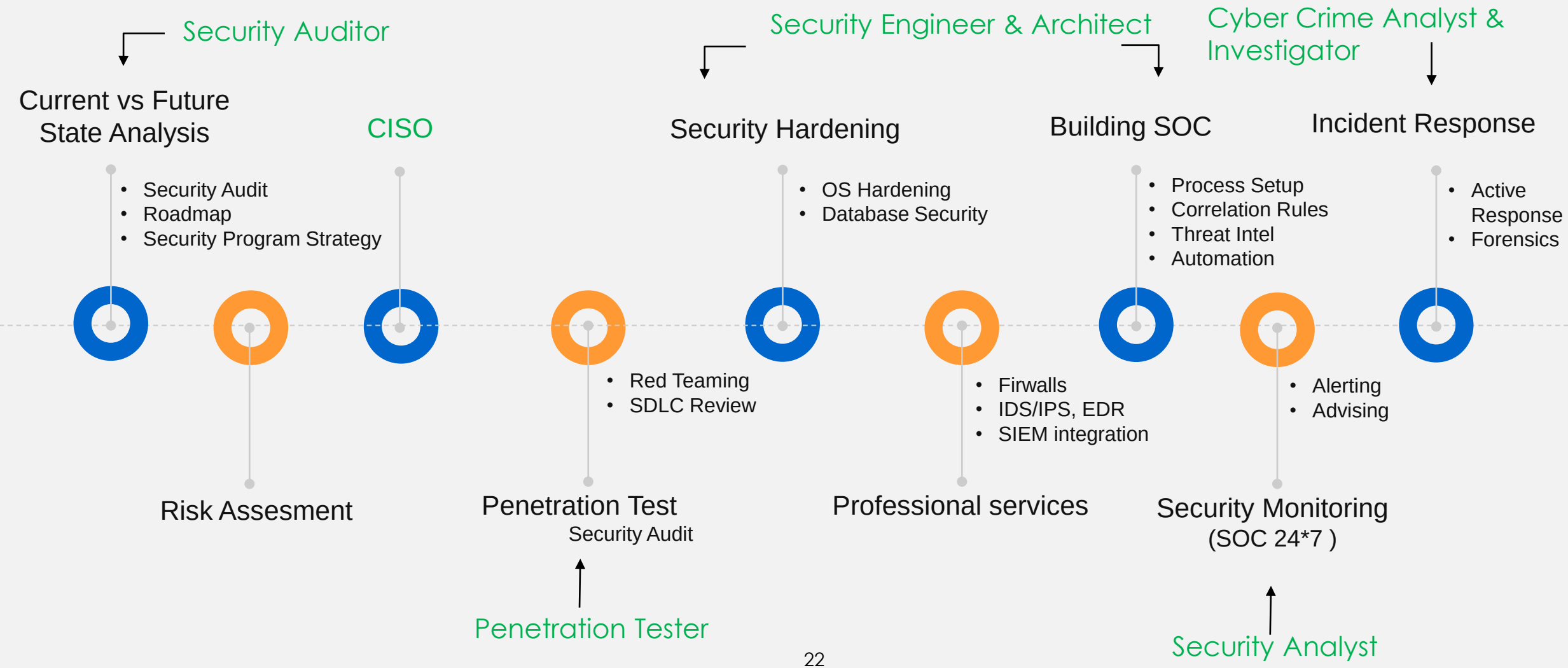
Domain Dominance: Local admin, then domain admin rights, is the last step before finding the Holy Grail (sensitive information valuable on the black market). This allows a hacker to usually fully recon the environment looking for sensitive assets and data if not isolated. Remote Code Execution (RCE) is trivial with Domain Admin privileges. An APT may stay in the environment indefinitely until caught.

FIELDS OF CYBER SECURITY


Cybersecurity Domains
Security Architecture
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development & DevSecOps
Linux / Windows / Server / Administration
Baseline Configuration
Secure System Build
Access Control
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Cryptography
4
Physical Security
Framework and Standard
ISO/IEC
ITIL
NIST
COBIT
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Social Engineering
Application
Redteam
Infrastructure
Exploit Development
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
1
Career Development
Certification
Conferences
Volunteering
Mentors
Online Training
Training
Contribute
Traditional Education
Internships
Personal Branding
Meetups / Networking
Governance
Industry Specific
Laws and Regulations
Federal
State
Audit
Executive Management Involvement
Project Management
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard
2
Threat Intelligence
OSINT
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Privacy
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
Active Defense
SIEM
SOC
Vulnerability Management
Data Leakage
Bug Bounty
Incident Response
Breach Notification
Containment
Investigation
Eradication
Forensics
3

CYBER SECURITY DEFENSE PROCESS

CYBER SECURITY DEFENSE PROCESS



HOW TO GET INTO

Cyber Security World

WHICH SKILLS ?

Computer Science

Basics of Networking

Systems Administration

Scripting & Programming

Basics of Security

Ability to Search

The Hacker Mindset

Cyber Security

CompTIA Security+
(Basic level)

CompTIA CySA+
(Intermediate level)

CISSP - Certified Information Systems Security Professional
(Advanced level)

Penetration Testing

CEH - Certified Ethical Hacker
(Intermediate level)

CompTIA Pentest+
(Intermediate level)

OSCP - Offensive Security Certified Professional
(Advanced level)

- GIAC Certified Penetration Tester
(Advanced level)

GWAPT - GIAC Web Application Penetration Tester
(Advanced level)

Offensive Security Exploitation Expert (OSEE)
(Expert level)

IT Basics

CompTIA IT Fundamentals
(Entry level)

CompTIA A+ Core 1 and core 2
(Entry level)

Security Management / CISO

CISM - Certified Information Security Manager
(Advanced level)

ITIL & PRINCE 2
(Intermediate level)

Cloud

CompTIA Cloud+
(Basic level)

Microsoft Azure
(Intermediate level)

Amazon Web Services (AWS)
(Intermediate level)

Networking

CompTIA Network+
(Basic level)

Cisco CCNA
(Intermediate level)

Cisco CCNP Security
(Intermediate level)

GET INTO

E-learning platfrom

Training platform

MORE INTO

- Set up a virtual lab to gain hands-on experience.
- Activate on the practical security platform (hackthebox, tryhackme, webSecurityAcademy …)
- Join social networks (Twitter, LinkedIn, Blogs), follow security news!
- Participate in meetings and make active networking (Club, Event).
- Do all cybersecurity related work to gain experience.

ANY QUESTIONS?

THANK YOU