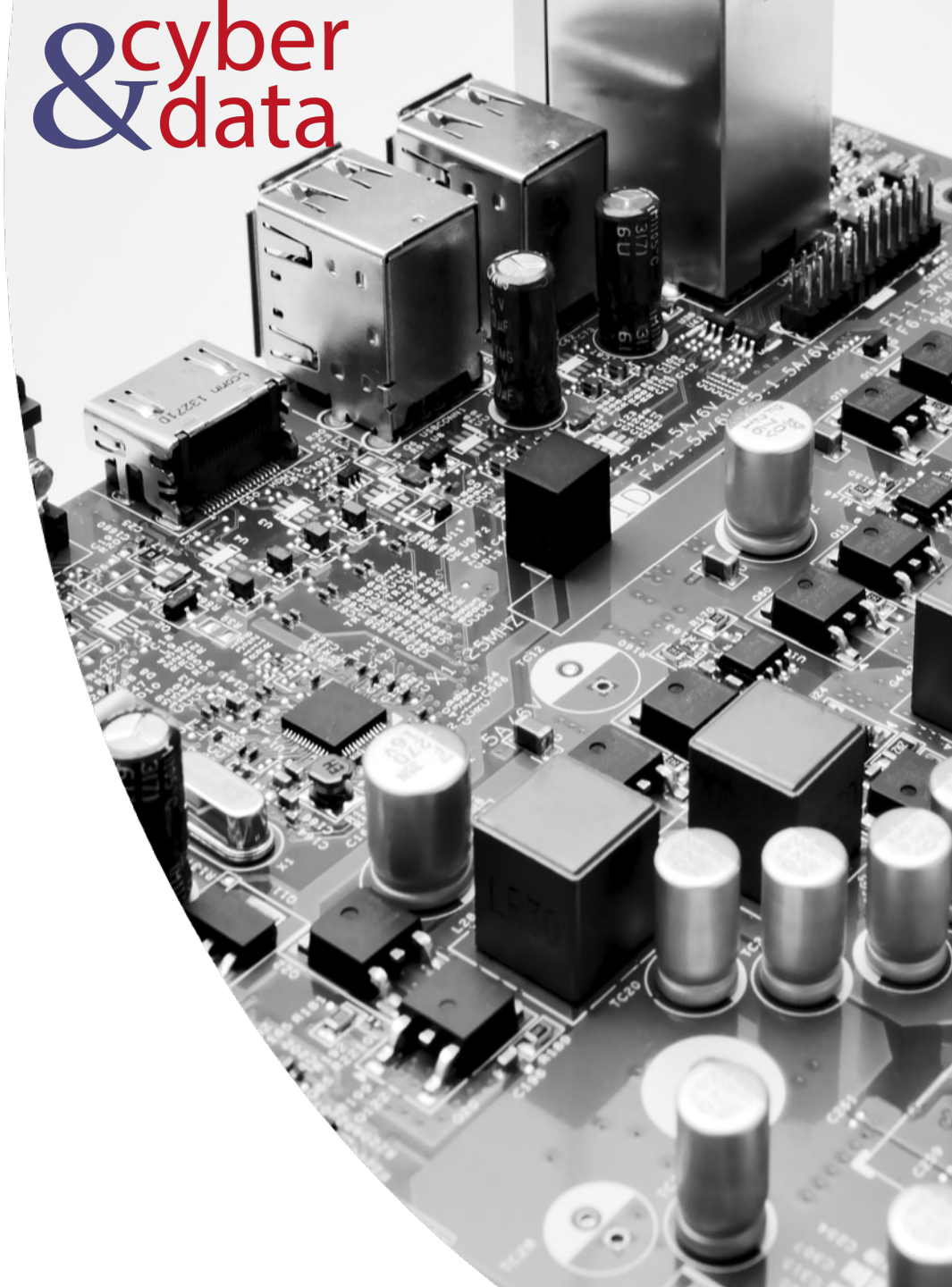
cyber & data

"From bits to information"

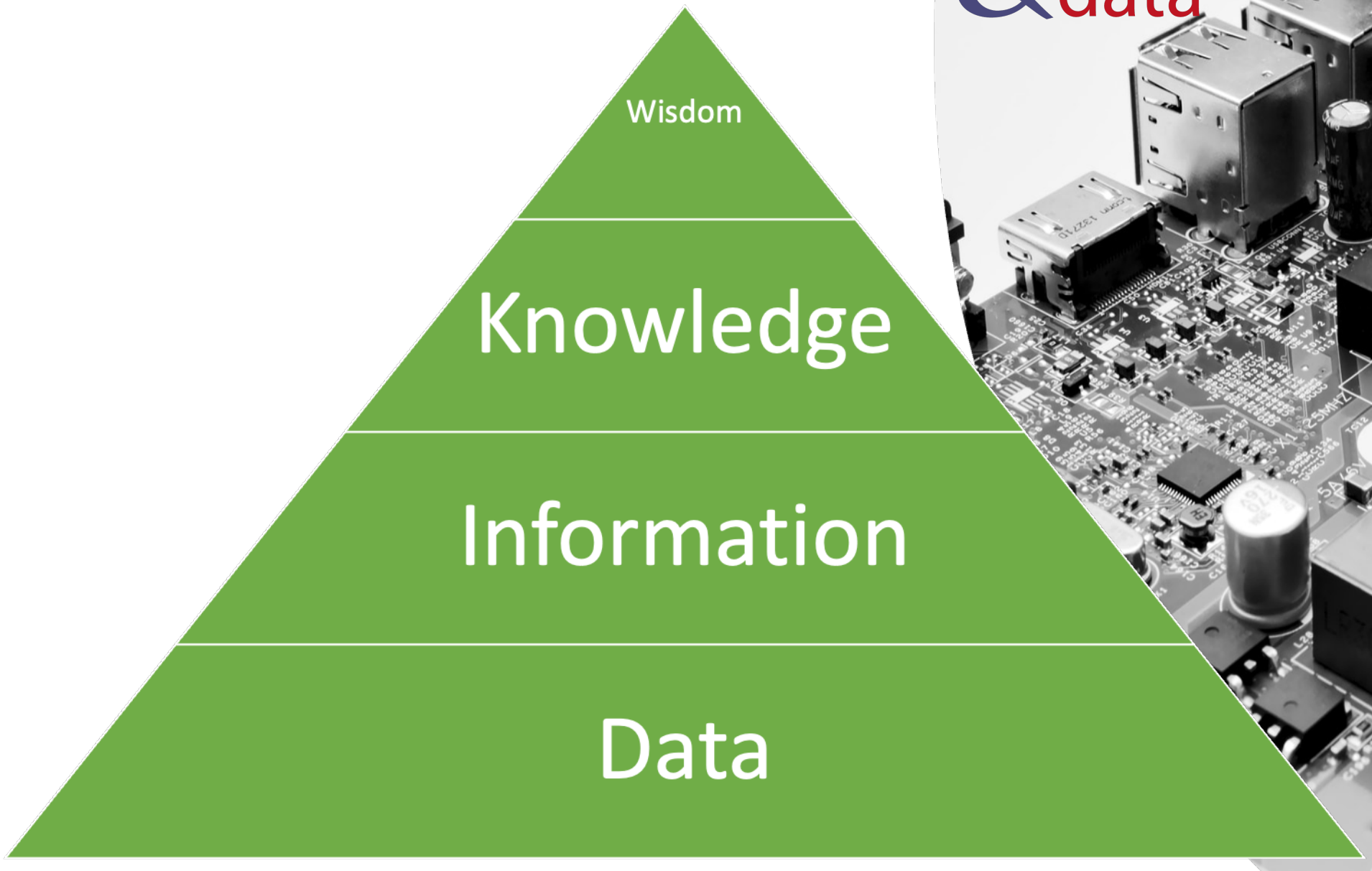
Network Security (Risks and Models)

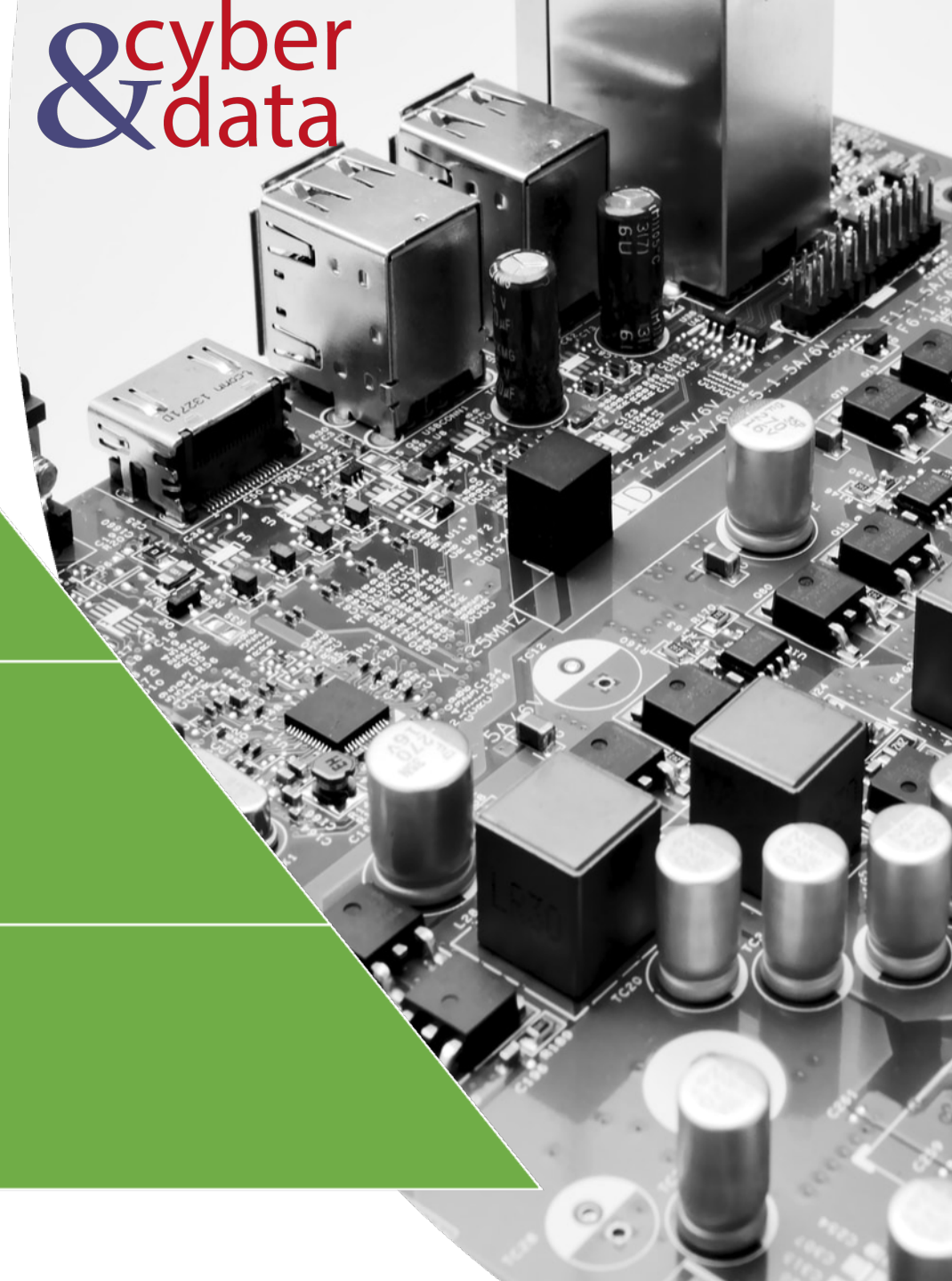
Outline

- Basics: Security Policy, Risk and Benefits.
- Kill Chain Model, MITRE ATT&CK and EMB3D.
- Basic Terms: Defence in Depth, IDS.
- Cryptography Basics.
- Secure Infrastructures.
- Secure Enclaves.
- Network Security: NAT, Stateful Firewalls.



Data to Wisdom



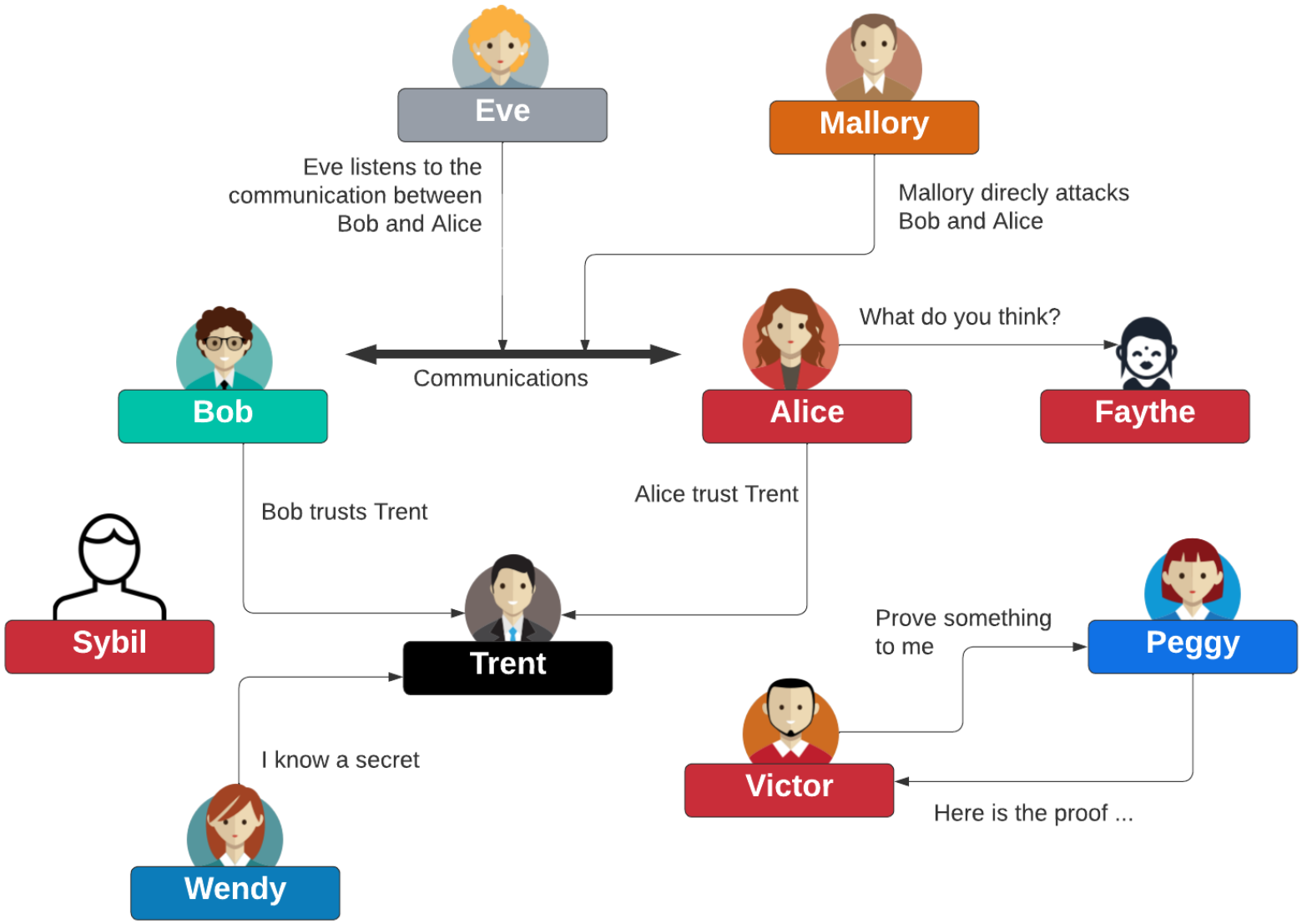


cyber & data

"From bits to information"

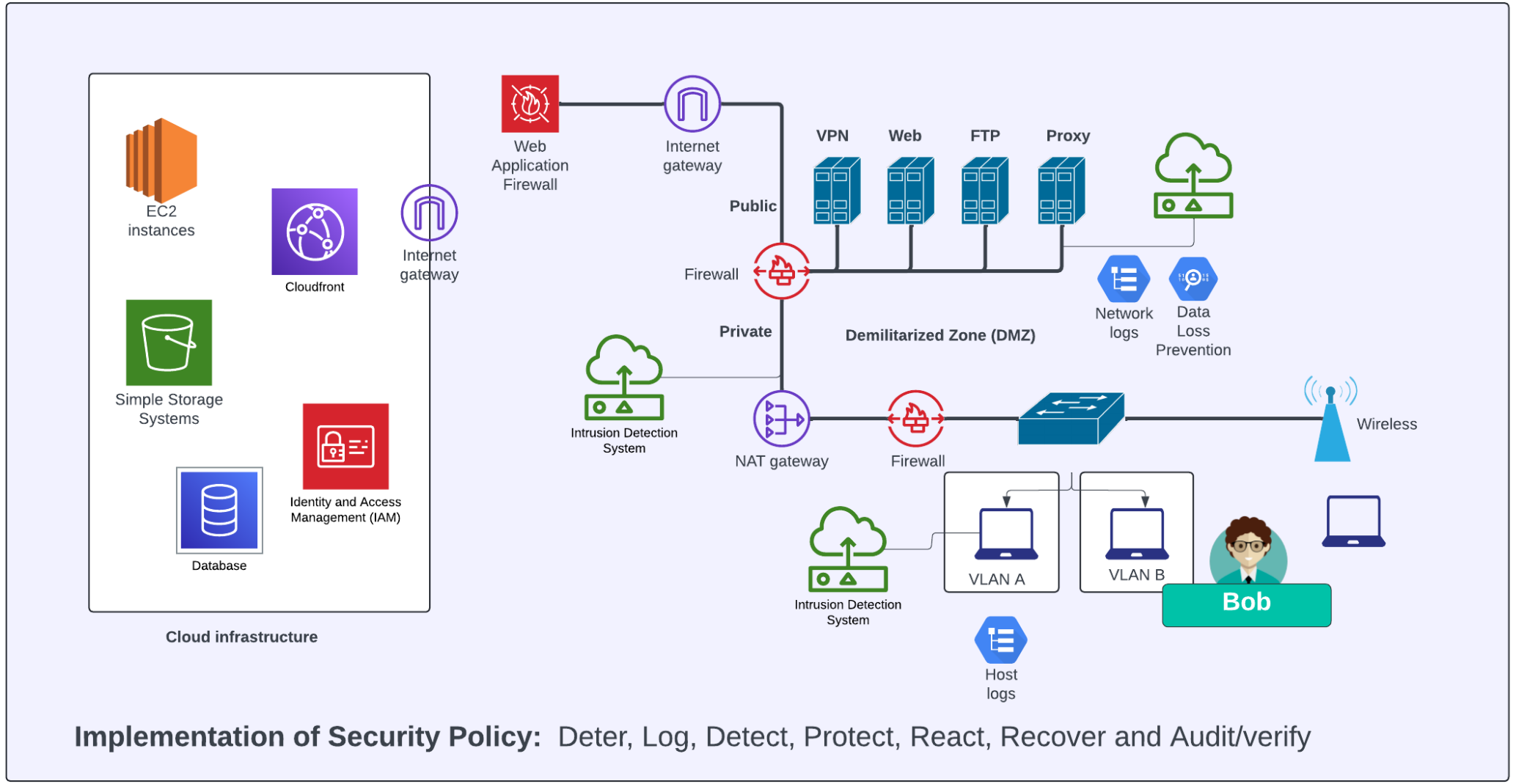
Introduction

Bob, Alice and Eve



&cyber data

Information Security



Implementation of Security Policy: Deter, Log, Detect, Protect, React, Recover and Audit/verify

&cyber data

Due Care and Due Diligence

Due Care: Correct steps for security policy and risk analysis

Bob

Cyber Infrastructure

Testing for compliance

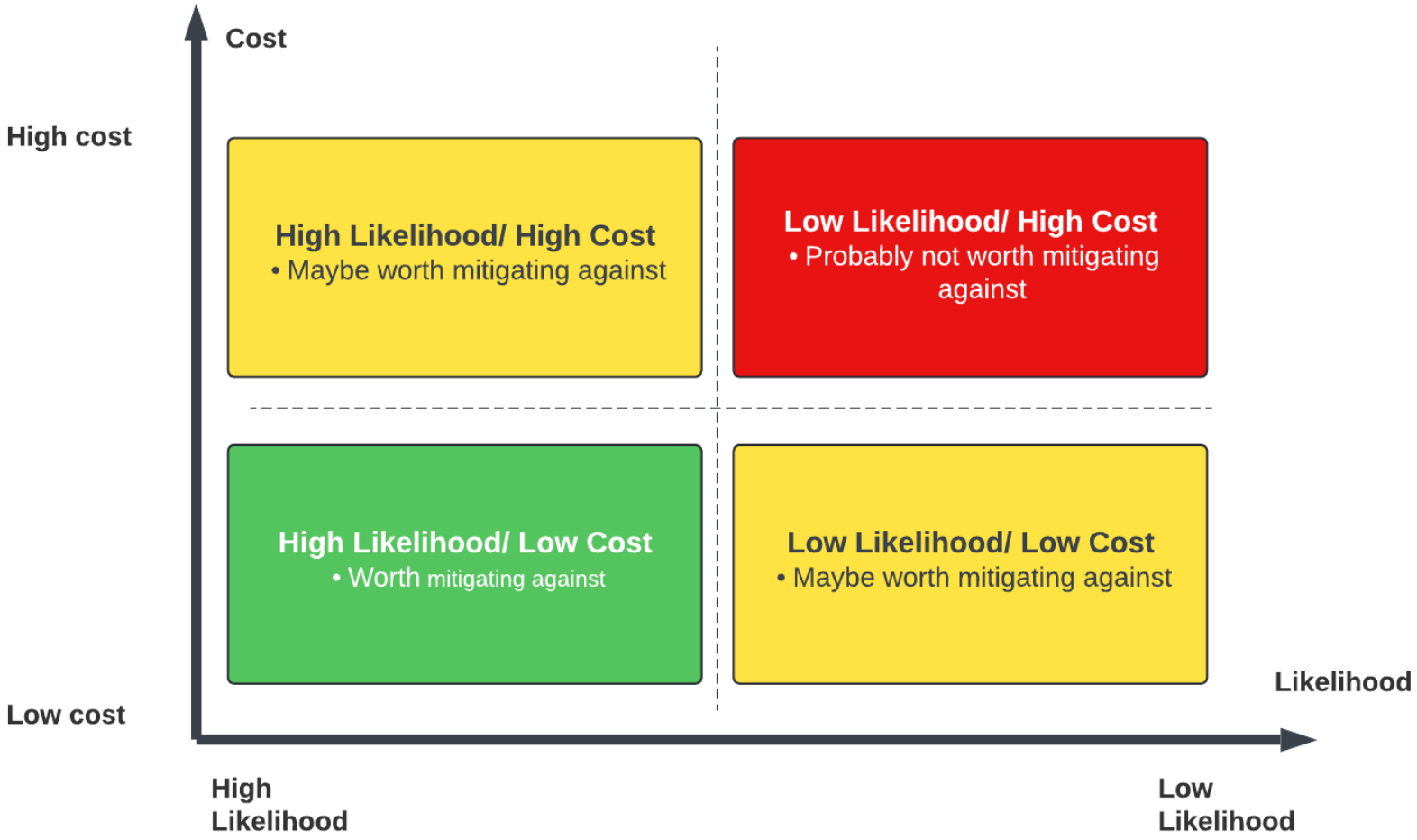
Due Diligence: Test for actions operation and maintenance of the security system, such as for vulnerability testing

&cyber data

Impact and Harm

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006.

Risks, Costs and Benefits

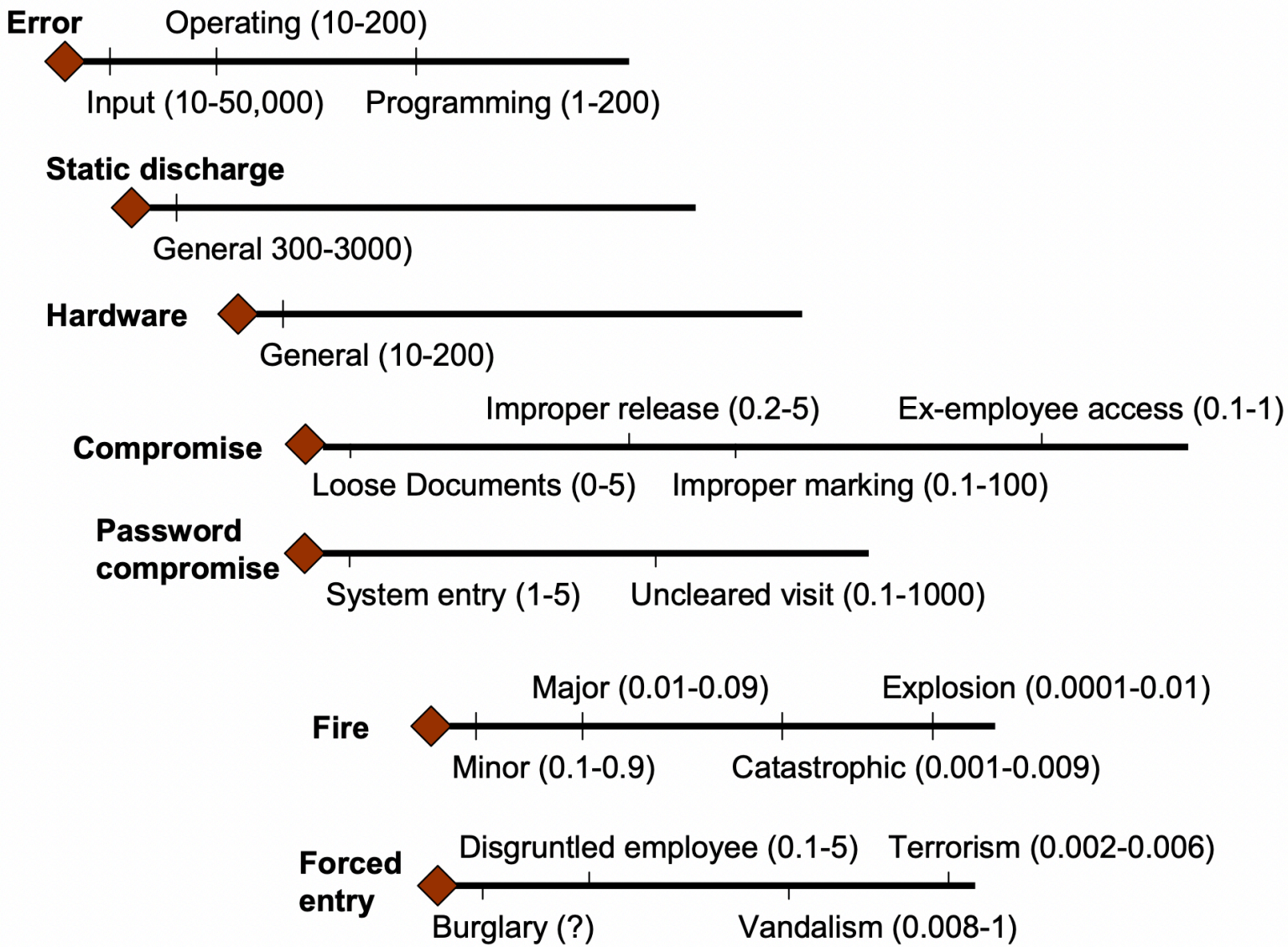


ALE = AV x ARO

ALE – Annual Loss Expectancy.
AV – Asset Value

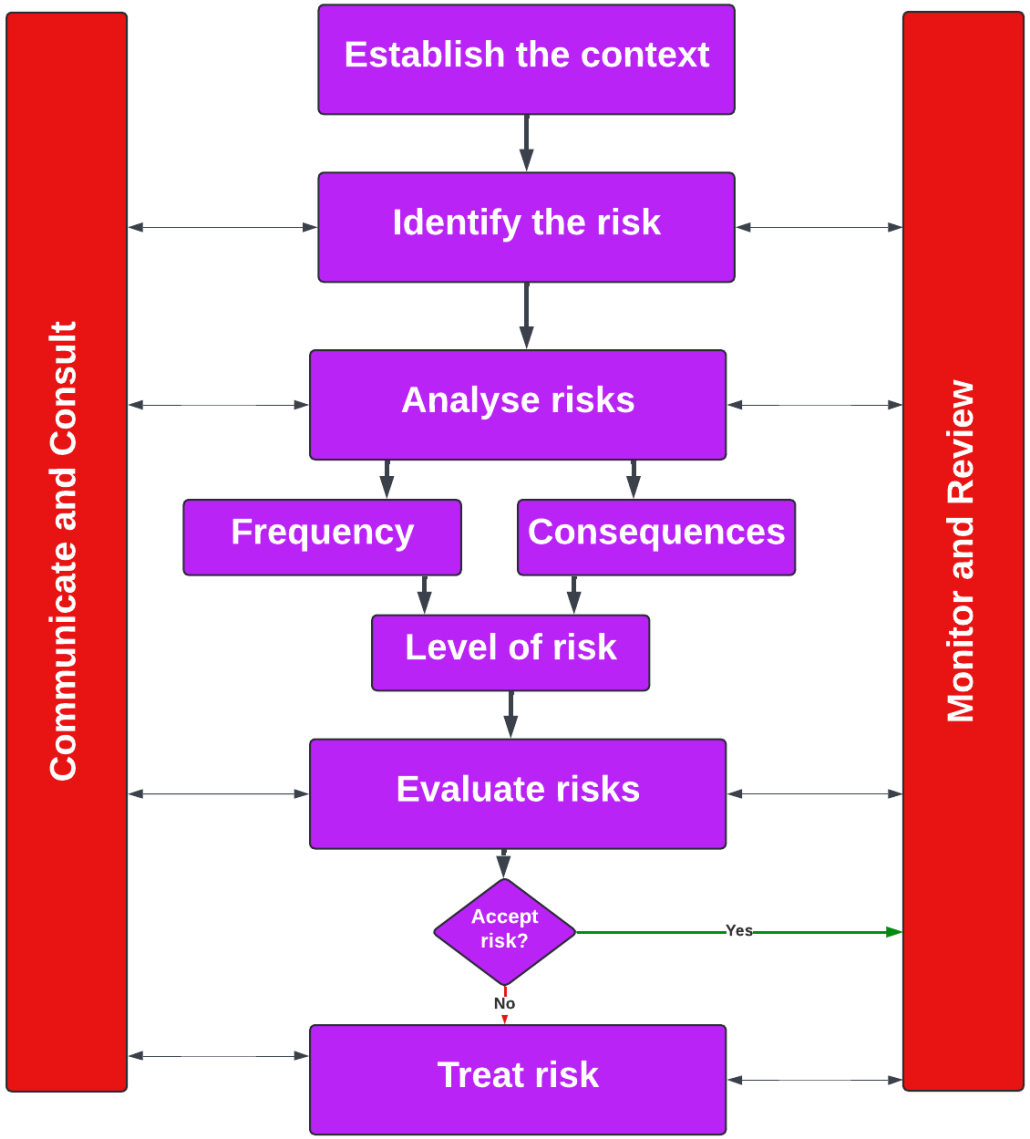
&cyber data

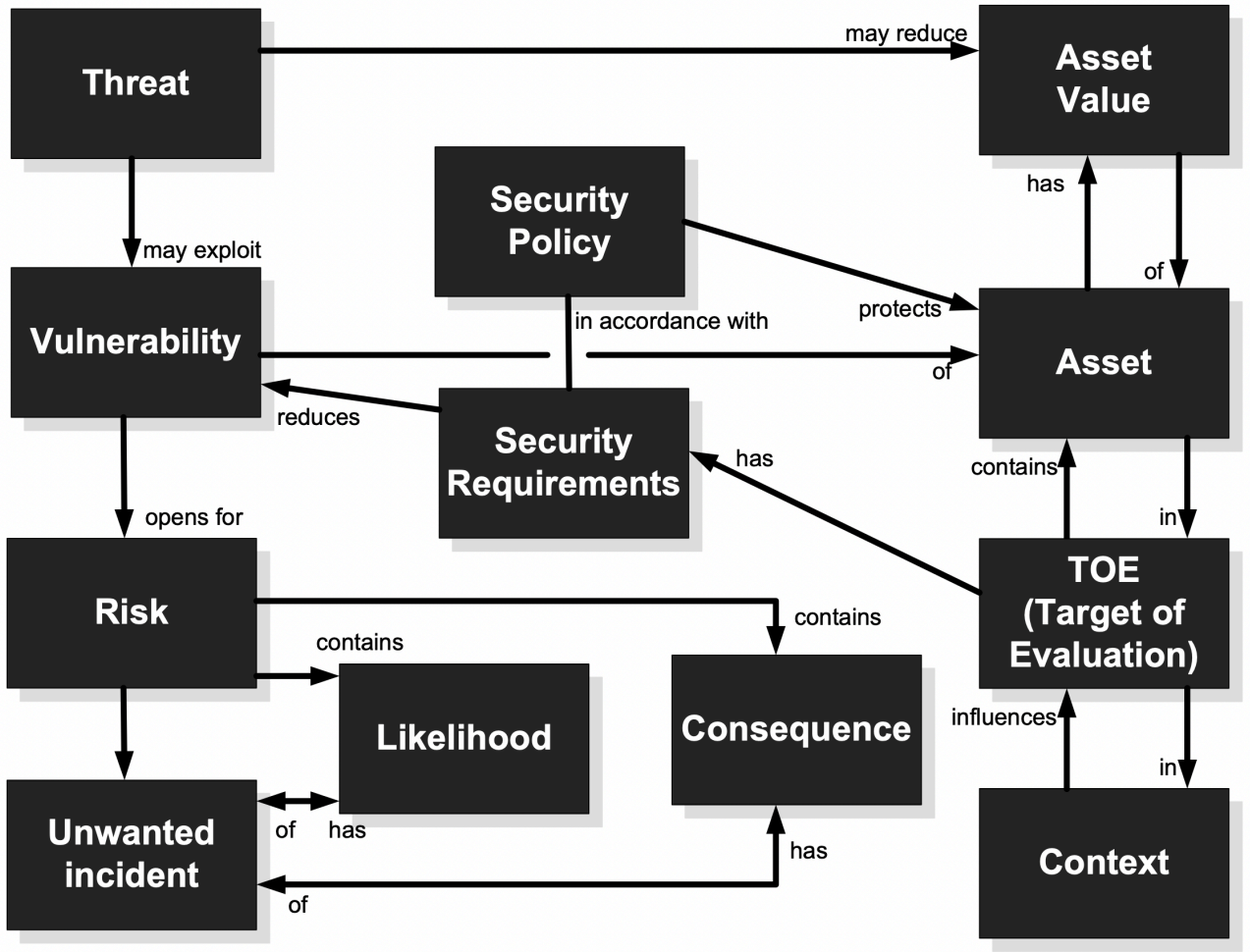
Risks, Costs and Benefits



&cyber data

CORAS Risk Management/Ontology





&cyber data

cyber & data

"From bits to information"

Kill Chain Model

CVE Reporting

CVE-2024-31497 PUBLISHED

View JSON | User Guide

Collapse all

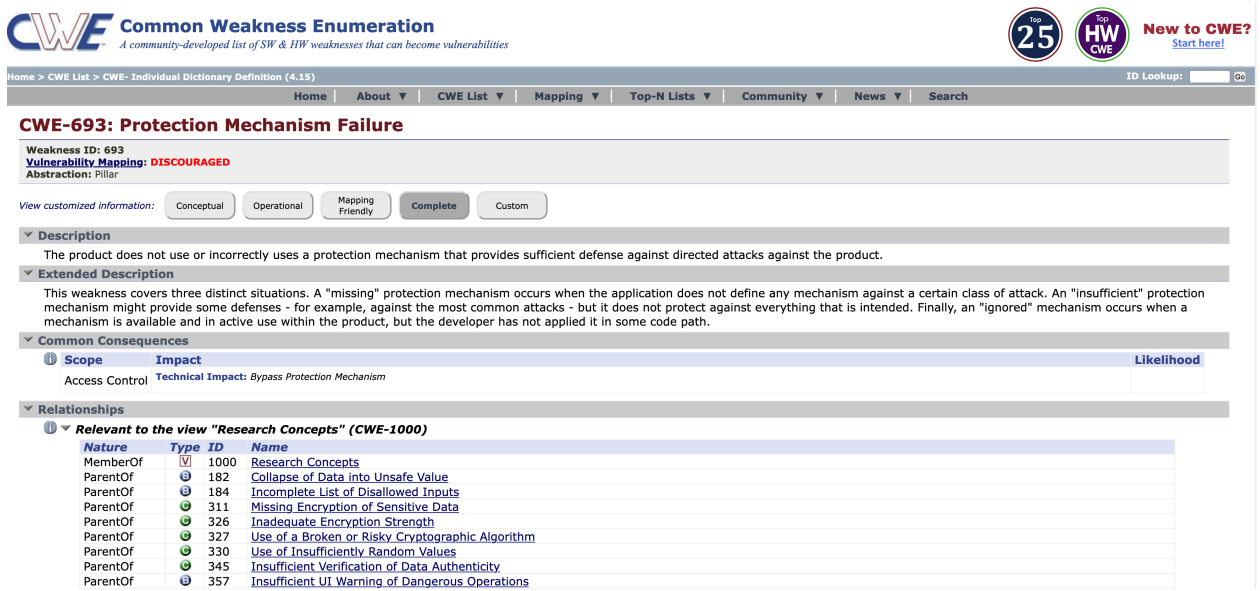
Required CVE Record Information

CNA: MITRE Corporation

Published: 2024-04-15 **Updated:** 2024-06-20

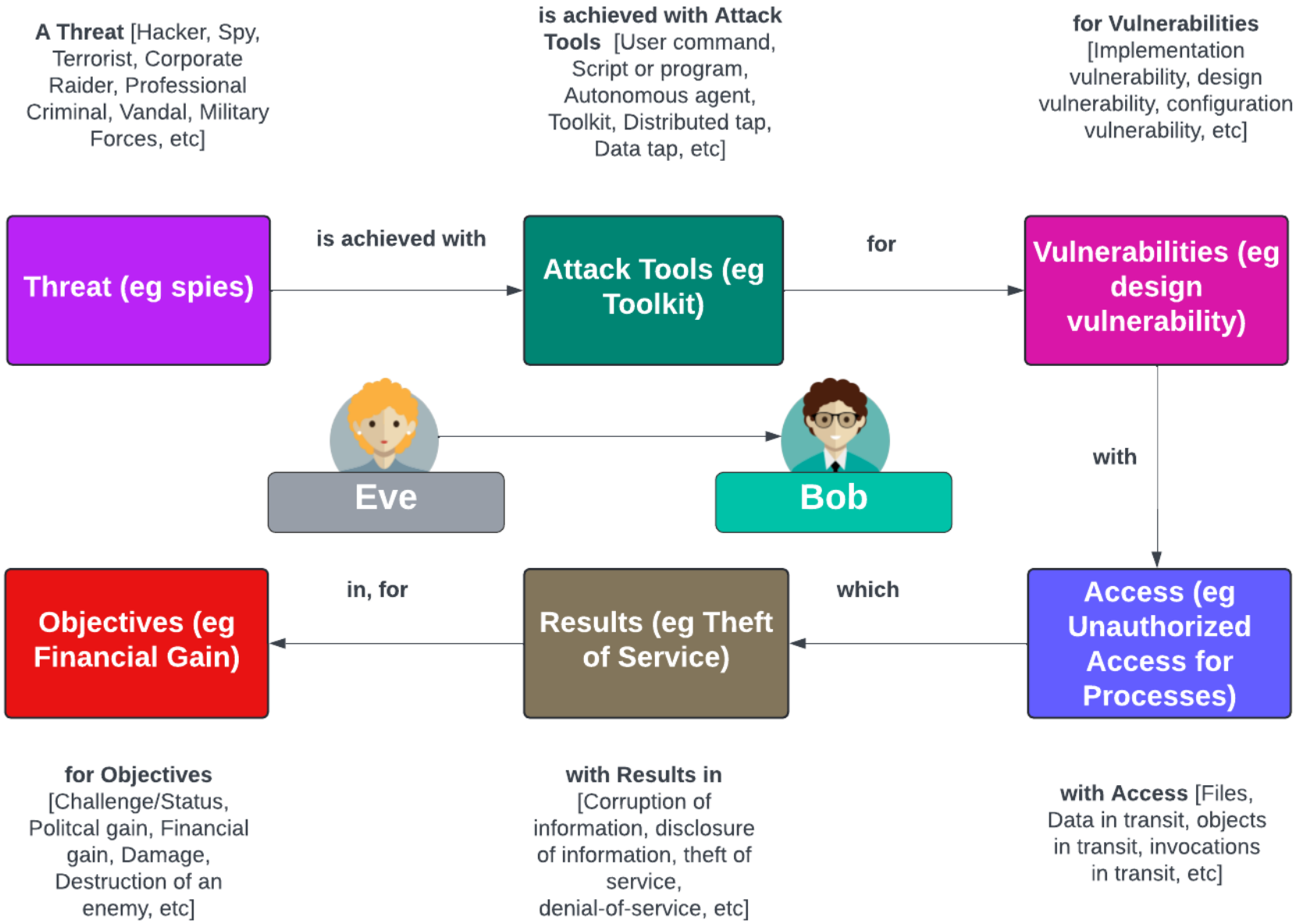
Description

In PuTTY 0.68 through 0.80 before 0.81, biased ECDSA nonce generation allows an attacker to recover a user's NIST P-521 secret key via a quick attack in approximately 60 signatures. This is especially important in a scenario where an adversary is able to read messages signed by PuTTY or Pageant. The required set of signed messages may be publicly readable because they are stored in a public Git service that supports use of SSH for commit signing, and the signatures were made by Pageant through an agent-forwarding mechanism. In other words, an adversary may already have enough signature information to compromise a victim's private key, even if there is no further use of vulnerable PuTTY versions. After a key compromise, an adversary may be able to conduct supply-chain attacks on software maintained in Git. A second, independent scenario is that the adversary is an operator of an SSH server to which the victim authenticates (for remote login or file copy), even though this server is not fully trusted by the victim, and the victim uses the same private key for SSH connections to other services operated by other entities. Here, the rogue server operator (who would otherwise have no way to determine the victim's private key) can derive the victim's private key, and then use it for unauthorized access to those other services. If the other services include Git services, then again it may be possible to conduct supply-chain attacks on software maintained in Git. This also affects, for example, FileZilla before 3.67.0, WinSCP before 6.3.3, TortoiseGit before 2.15.0.1, and TortoiseSVN through 1.14.6.



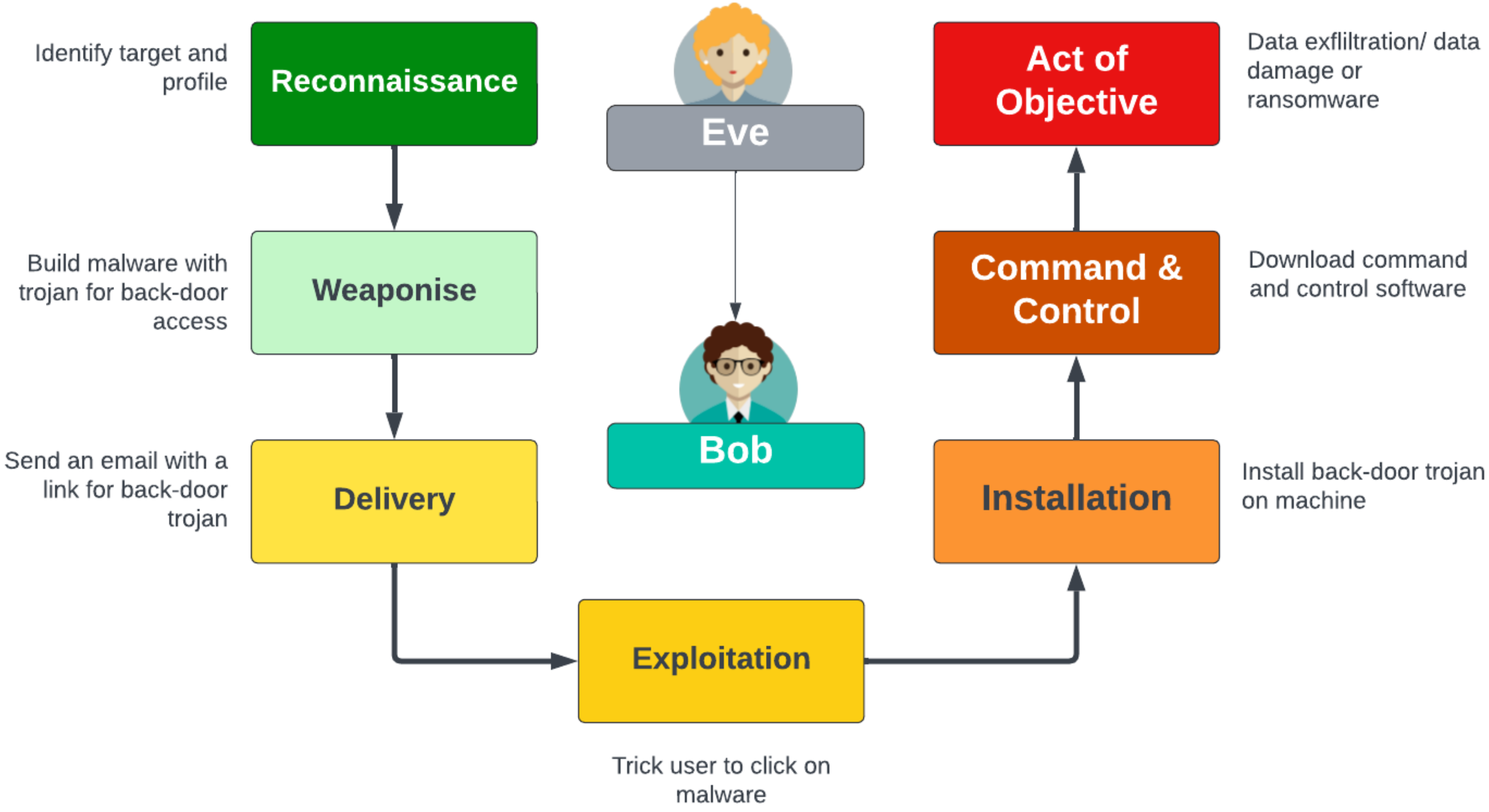
&cyber data

Incident Taxonomy



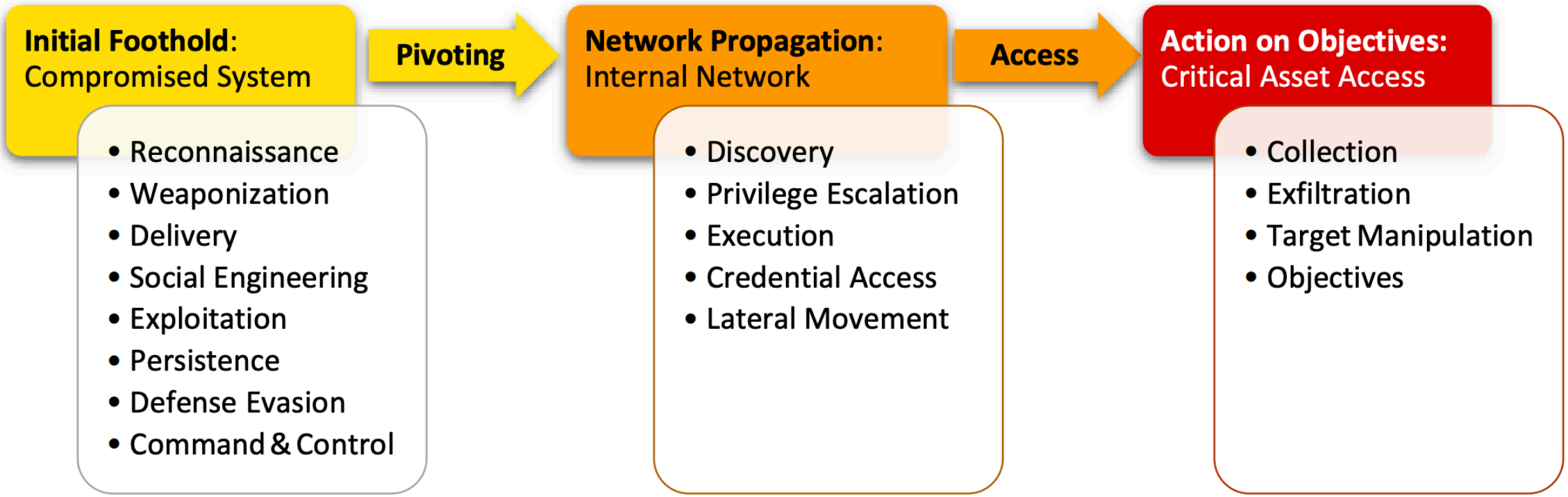
&cyber data

Kill Chain Model



&cyber data

Unified Kill Chain Phases



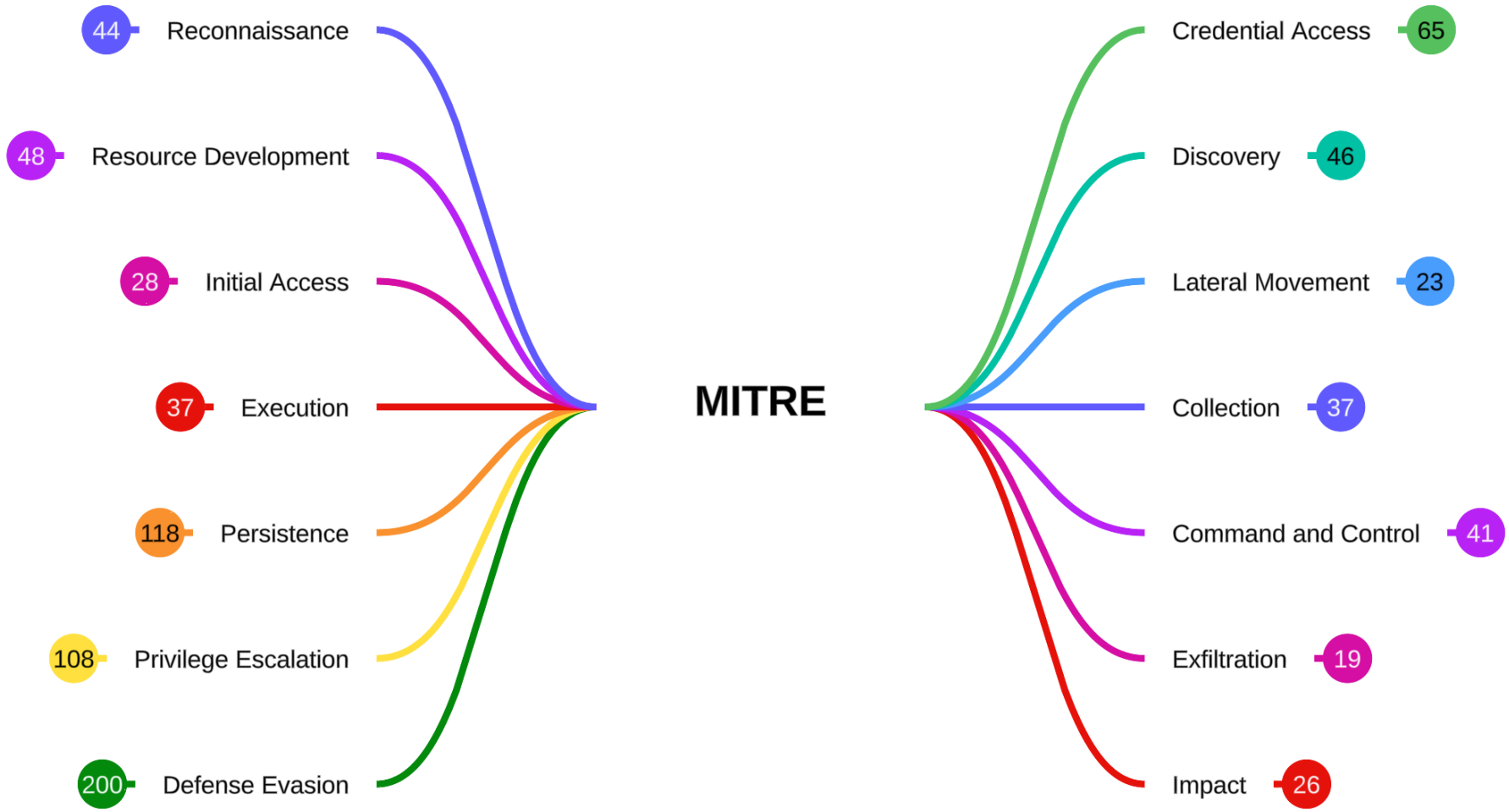
Pols, P., & van den Berg, J. (2017). The unified kill chain. *CSA Thesis, Hague*, 1-104.

&cyber data

"From bits to information"

MITRE ATT&CK

MITRE ATT&CK (Enterprise)



&cyber data

MITRE ATT&CK (Enterprise)

Techniques

Techniques: 10

ID	Name	Description
T1595	Active Scanning	Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
.001	Scanning IP Blocks	Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.
.002	Vulnerability Scanning	Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.
.003	Wordlist Scanning	Adversaries may iteratively probe infrastructure using brute-forcing and crawling techniques. While this technique employs similar methods to Brute Force, its goal is the identification of content and infrastructure rather than the discovery of valid credentials. Wordlists used in these scans may contain generic, commonly used names and file extensions or terms specific to a particular software. Adversaries may also create custom, target-specific wordlists using data gathered from other Reconnaissance techniques (ex: Gather Victim Org Information, or Search Victim-Owned Websites).

Procedure Examples

ID	Name	Description
C0030	Triton Safety Instrumented System Attack	In the Triton Safety Instrumented System Attack, TEMP.Veles engaged in network reconnaissance against targets of interest.[3]

Mitigations

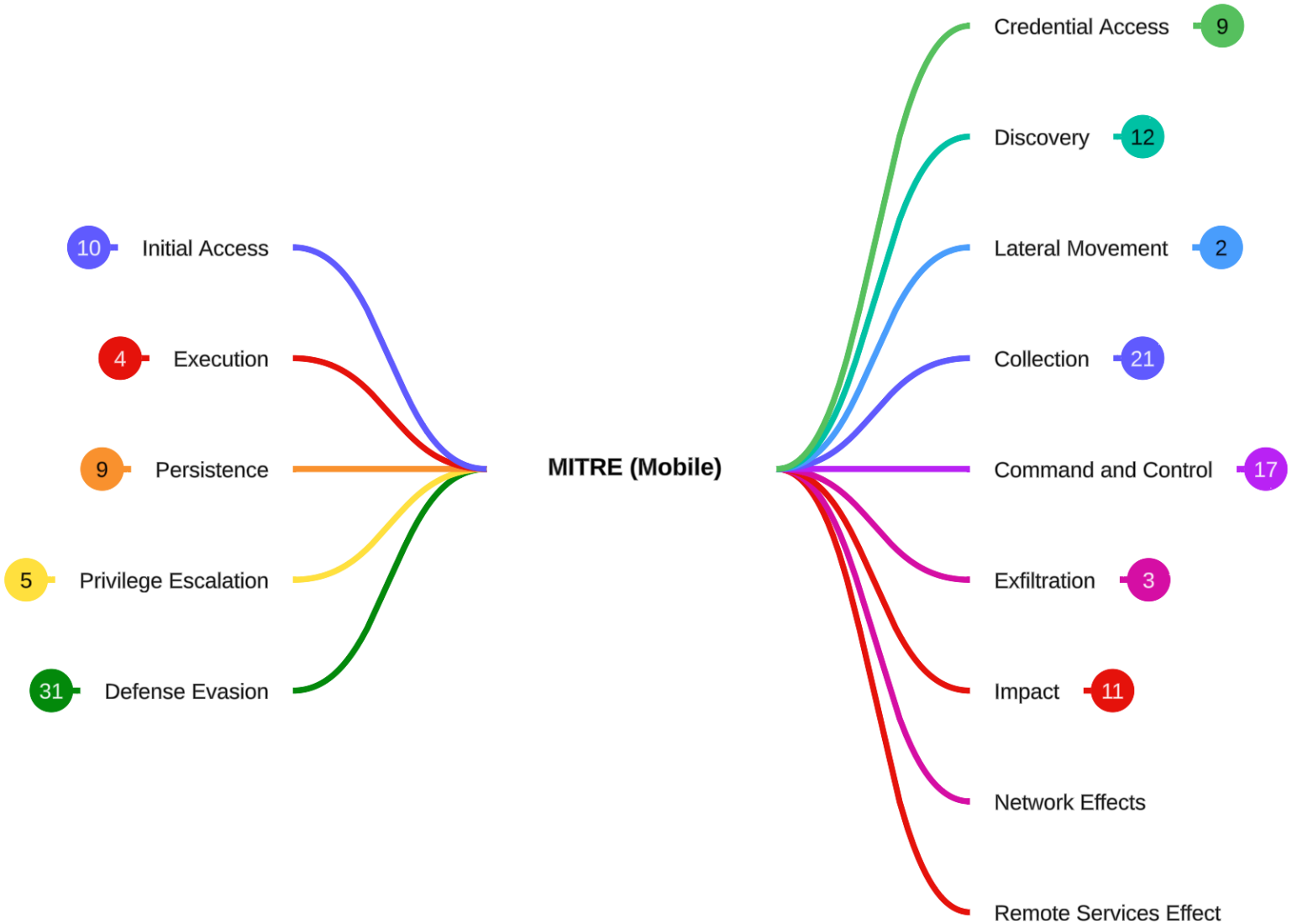
ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

ID	Data Source	Data Component	Detects
DS0029	Network Traffic	Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
		Network Traffic Flow	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

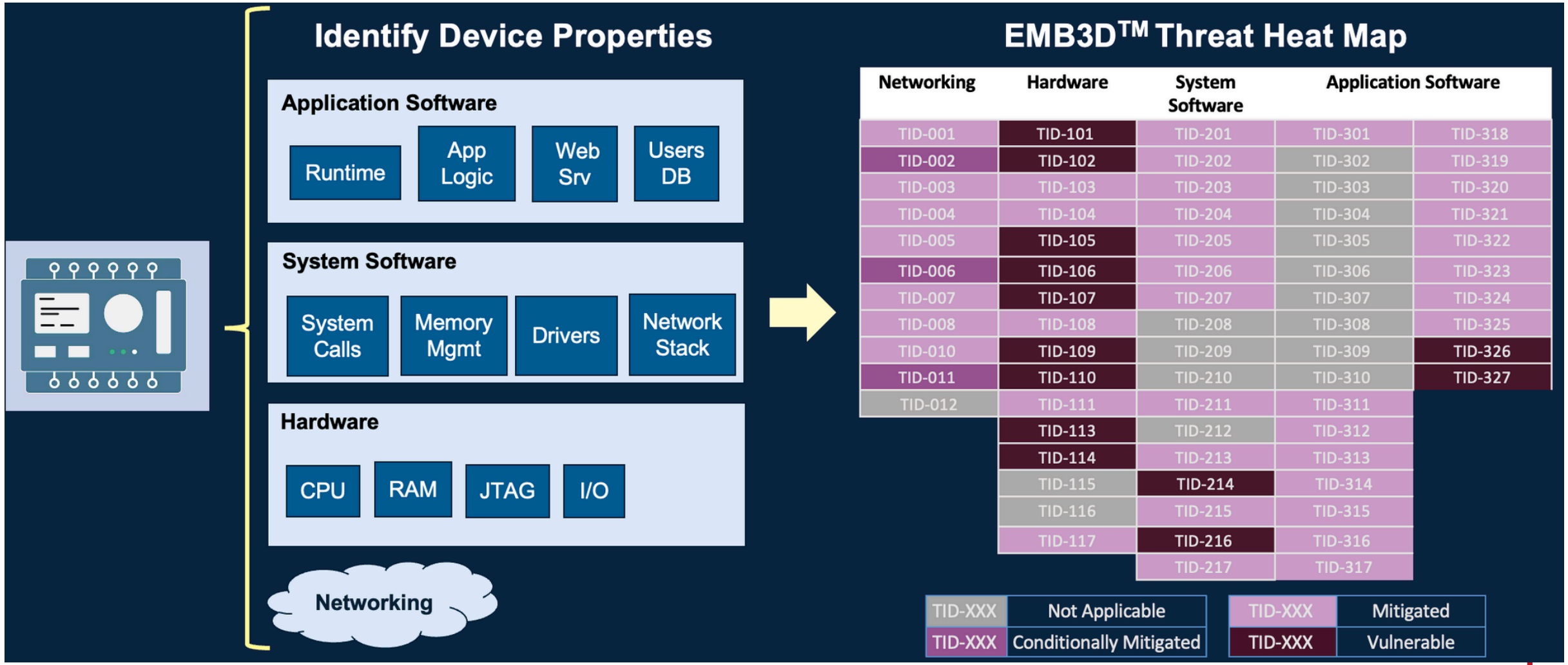
&cyber&data

MITRE ATT&CK (Mobile)



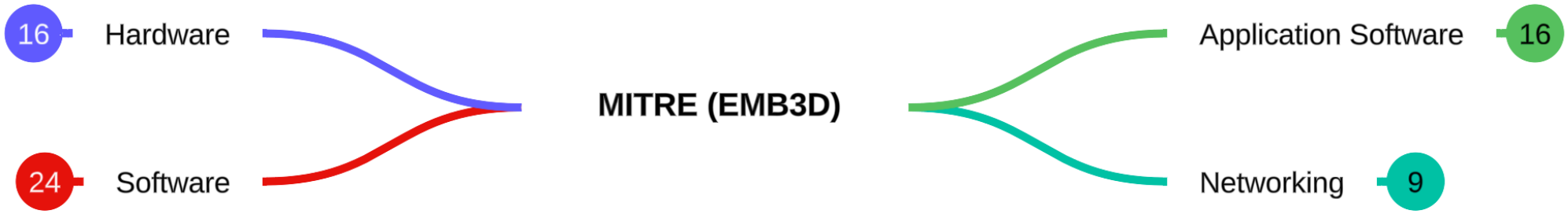
&cyber data

MITRE EMB3D (Embedded Devices)



&cyber data

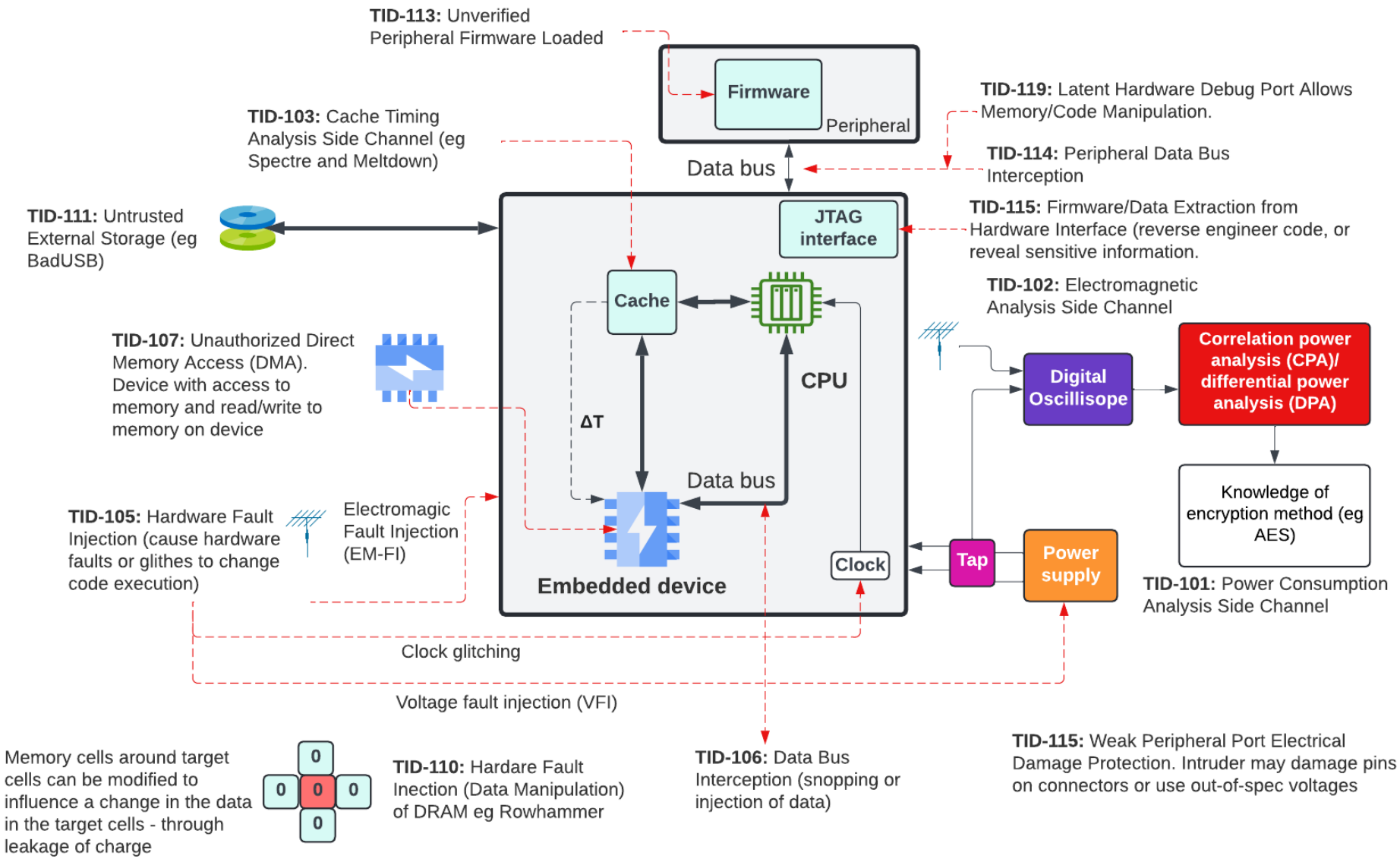
MITRE EMB3D (Embedded Devices)



&cyber data

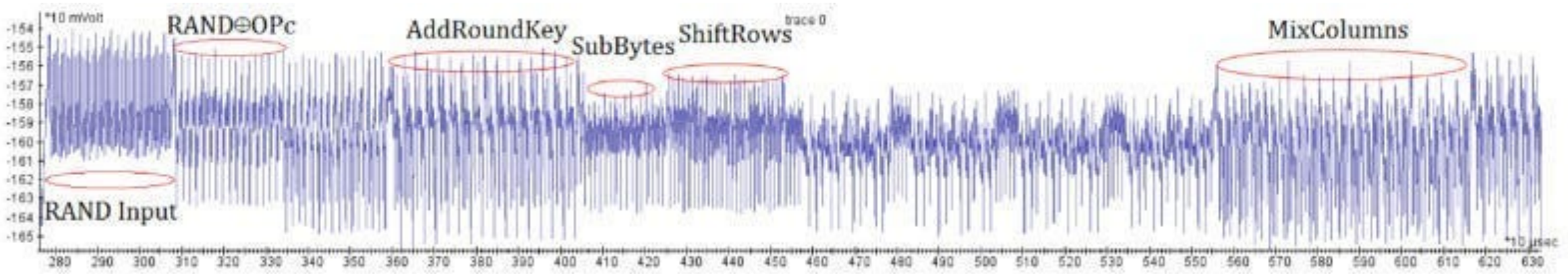
MITRE EMB3D (Embedded Devices)

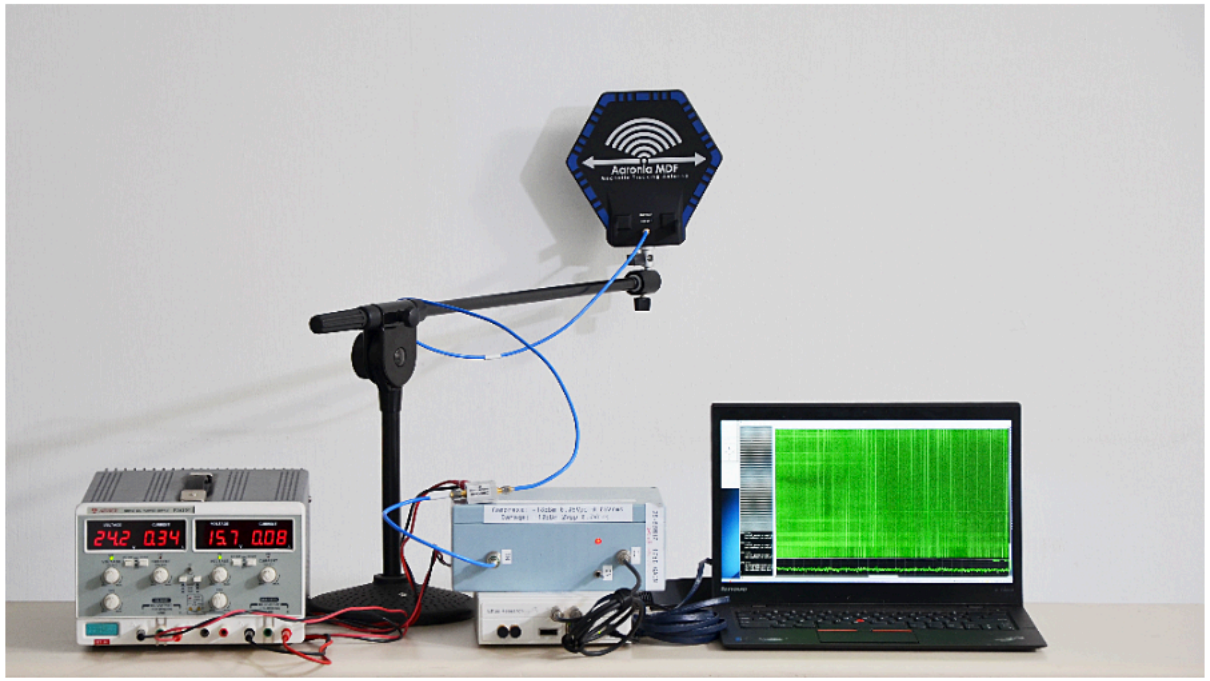
MITRE EMB3D (Embedded Devices)



&cyber data

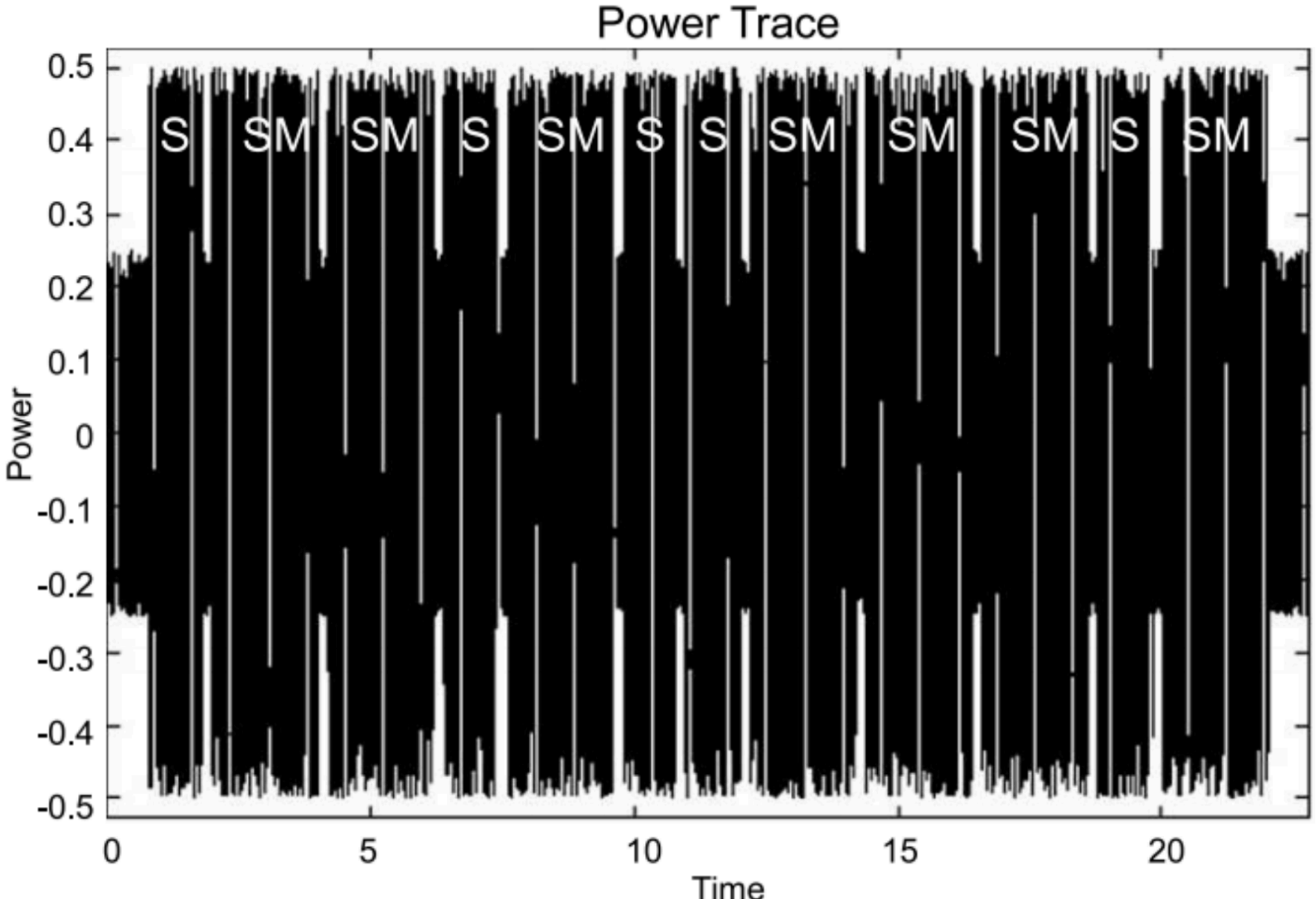
MITRE EMB3D (Embedded Devices) – Symmetric Key Crack





&cyber data

MITRE EMB3D (Embedded Devices) – RSA Crack



&cyber data

MITRE EMB3D (Embedded Devices)

EUCLEAK

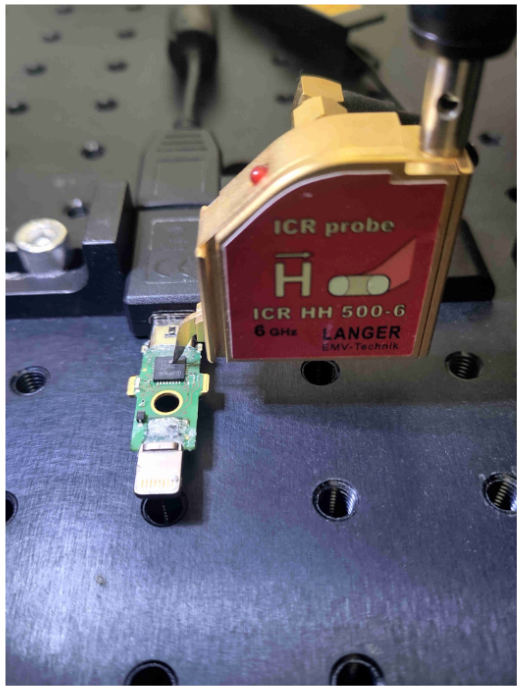
Side-Channel Attack on the YubiKey 5 Series

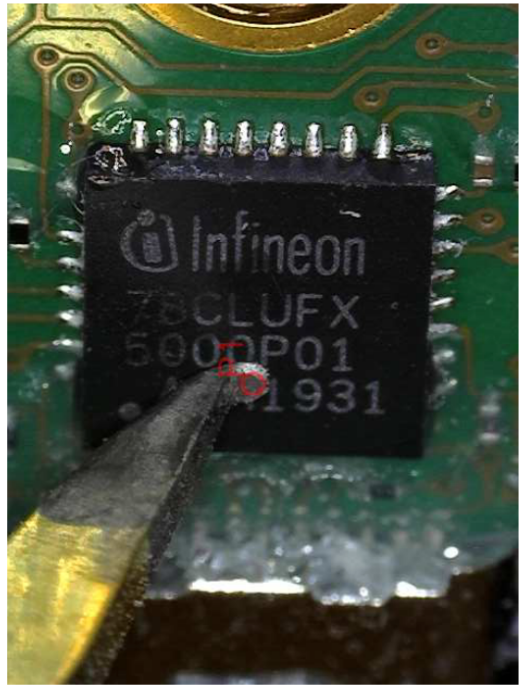
(Revealing and Breaking Infineon ECDSA Implementation on the Way)

Thomas Roche

NinjaLab, Montpellier, France
thomas@ninjalab.io

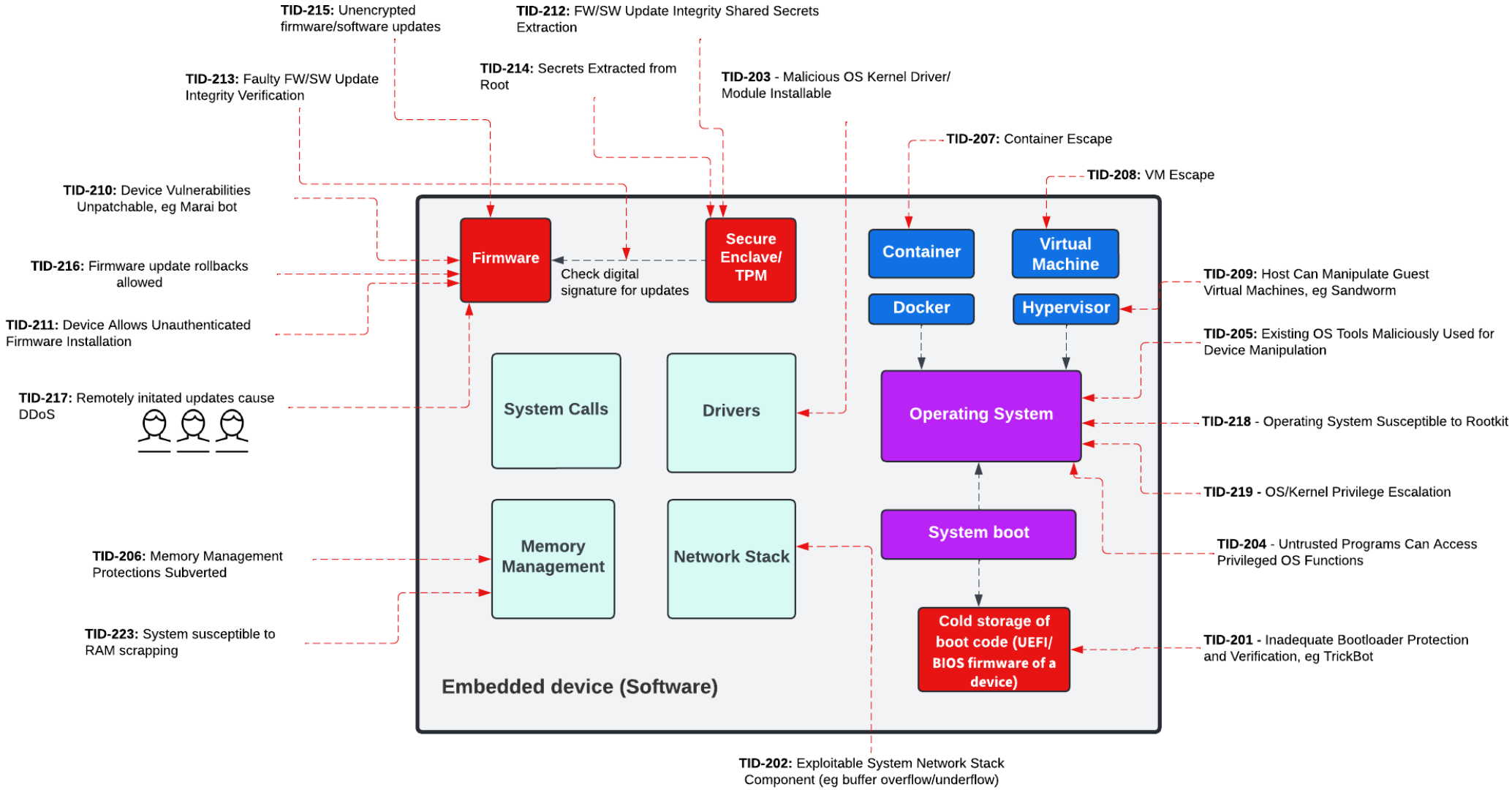
September 3rd, 2024





&cyber data

MITRE EMB3D (Embedded Devices)



&cyber data

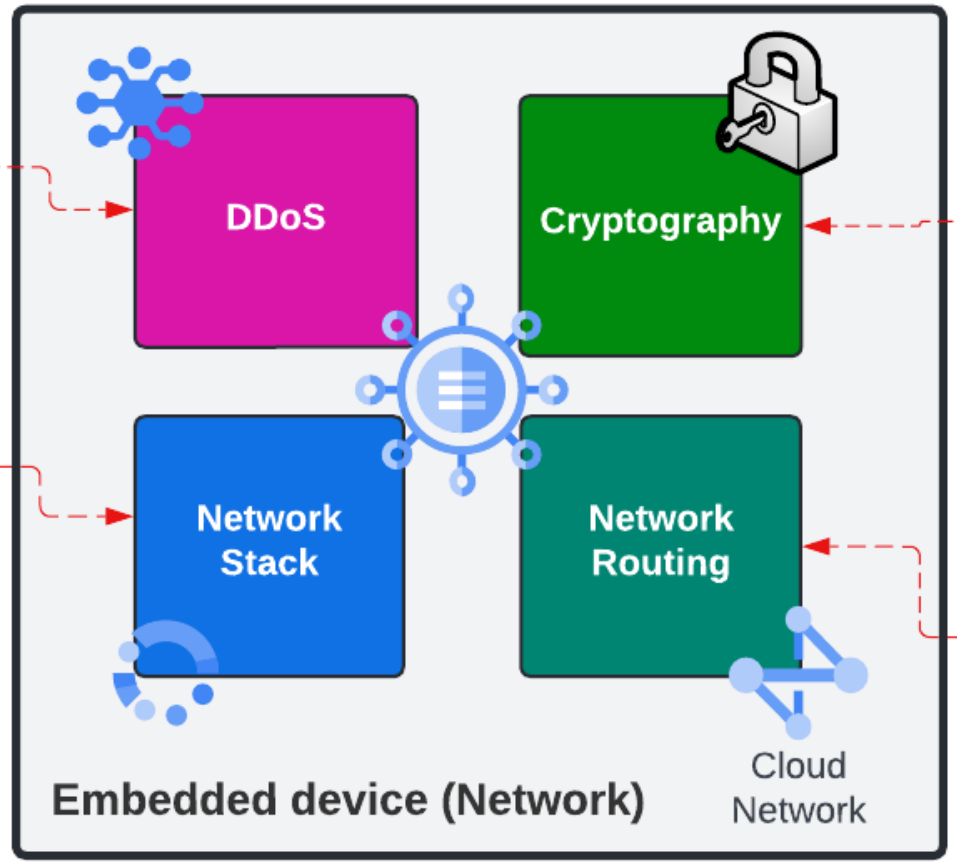
MITRE EMB3D (Embedded Devices)

TID-404 - Remotely Triggerable Deadlock/DoS

TID-405 - Network Stack Resource Exhaustion

TID-406 - Unauthorized Messages or Connections

TID-407 - Missing Message Replay Protection



TID-408 - Unencrypted Sensitive Data Communication

TID-410 - Cryptographic Protocol Side Channel

TID-411 - Weak/Insecure Cryptographic Protocol

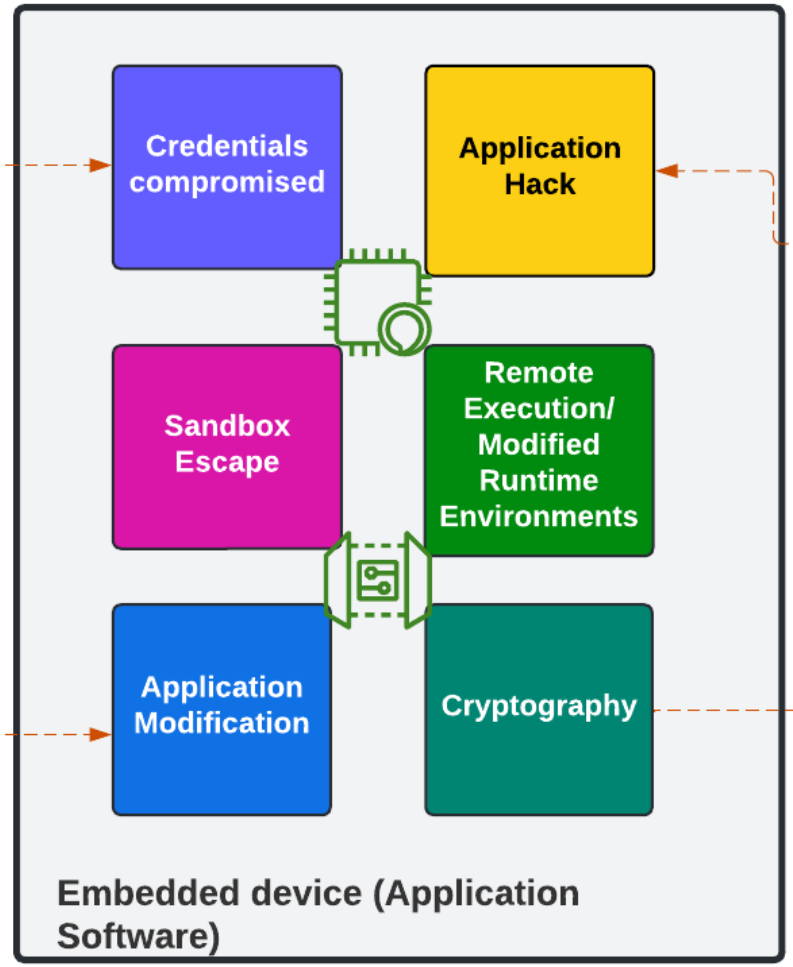
TID-412 - Network Routing Capability Abuse

TID-412 - Network Routing Capability Abuse

&cyber data

MITRE EMB3D (Embedded Devices)

TID-328 - Hardcoded Credentials
TID-311 - Default Credentials
TID-312 - Credential Change Mechanism Can Be Abused



TID-318 - Insecure Cryptographic Implementation
TID-319 - Cross Site Scripting (XSS)
TID-320 - SQL Injection
TID-321 - HTTP Application Session Hijacking
TID-322 - Cross Site Request Forgery (CSRF)
TID-323 - HTTP Path Traversal
TID-324 - HTTP Direct Object Reference
TID-325 - HTTP Injection/Response Splitting
TID-326 - Insecure Deserialization
TID-327 - Out of Bounds Memory Access

TID-301 - Applications Binaries Modified
TID-302 - Install Untrusted Application
TID-303 - Excessive Trust in Offboard Management/IDE Software

TID-317 - Predictable Cryptographic Key
TID-330 - Cryptographic Timing Side-Channel

&cyber&data

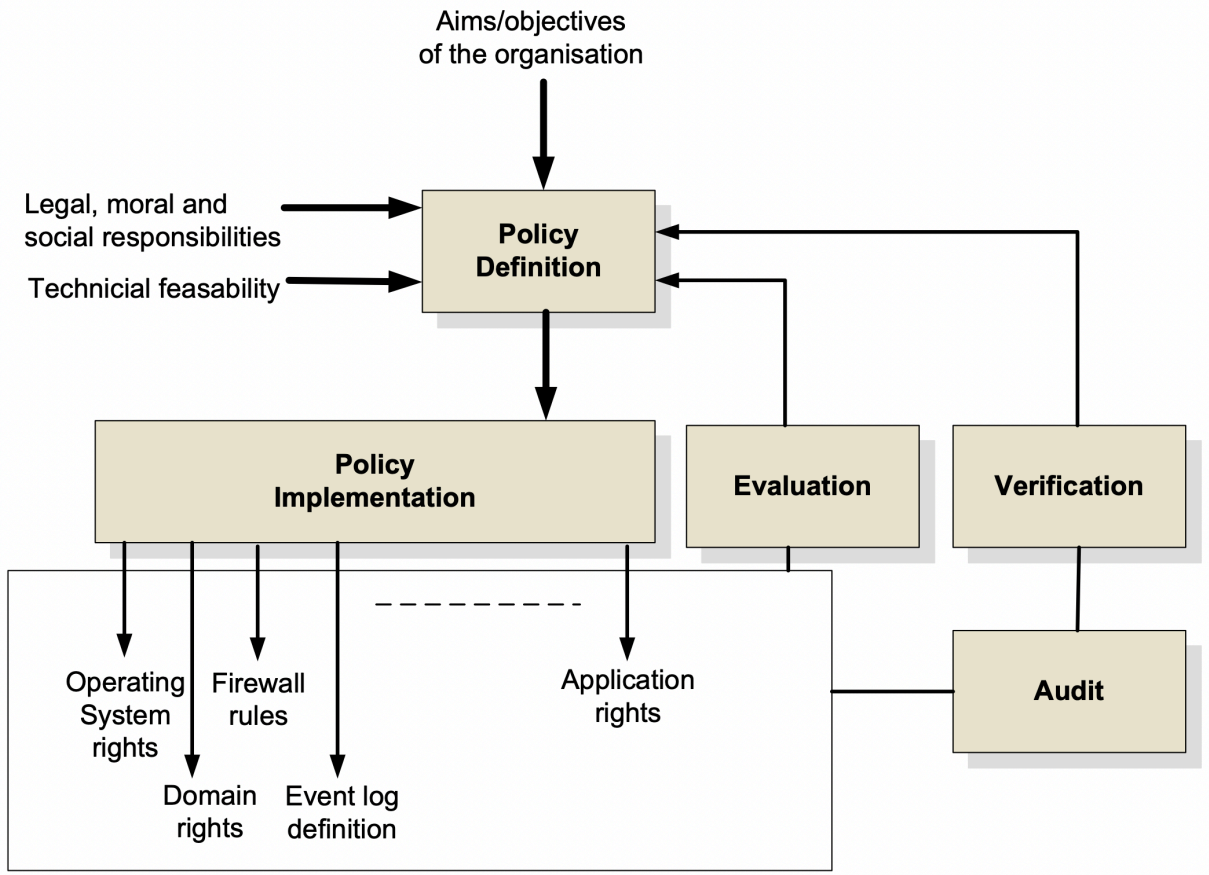
cyber & data

"From bits to information"

Basic Terms

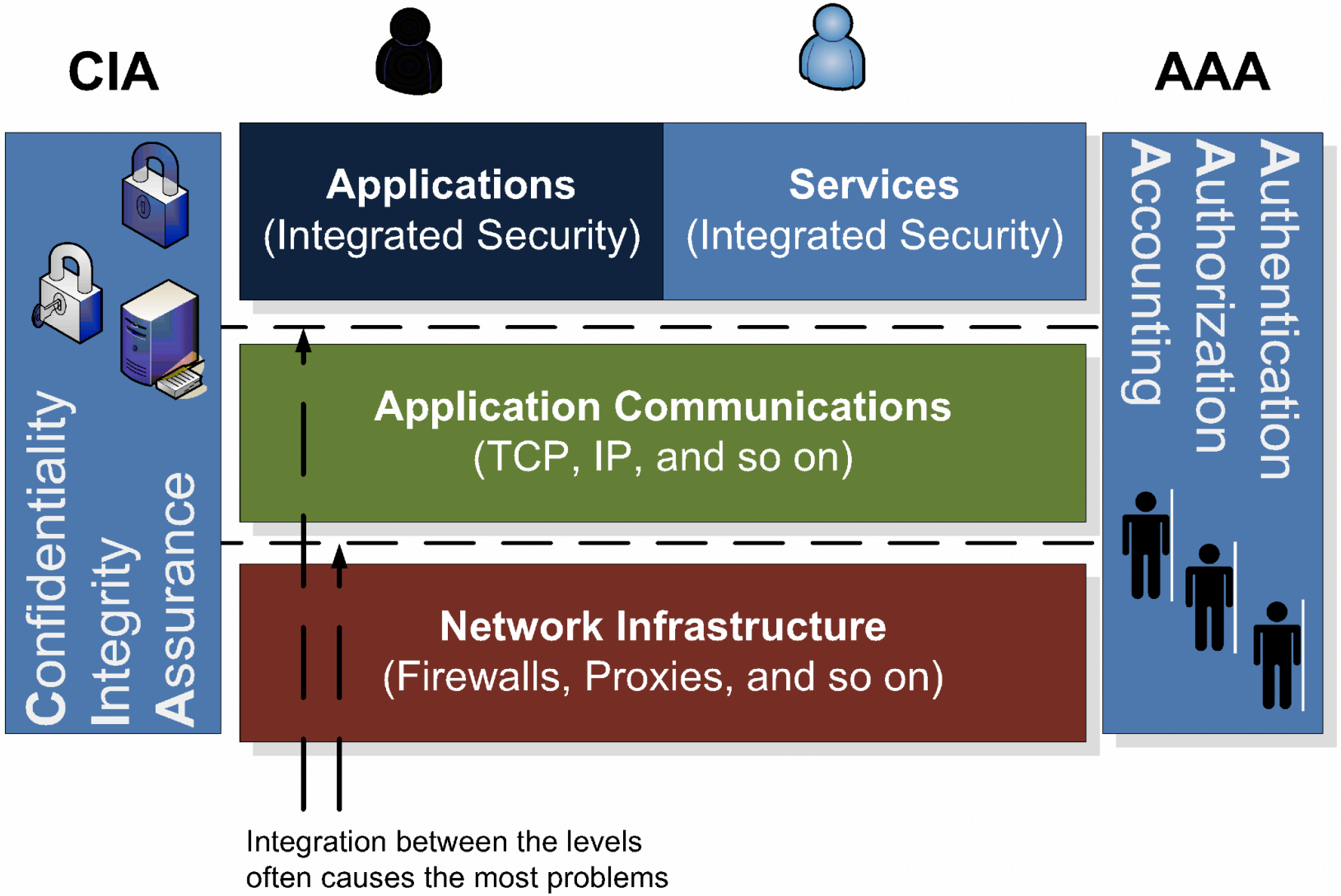
Policies

- **Deter**. This is where the system is designed and implemented in order to initially deter intruders from attacking the system in the first place.
- **Log**. This is a key element in modern systems which requires some form of logging system. It is important that the data that is logged does not breach any civil liberties, and is in a form which can be used to enhance the future security of the system.
- **Detect**. This is where detection agents are placed within the network to detect intrusions, and has methods of tracing the events that occurred in an intrusion, so that it can be used either in a forensic computing investigation, and/or to overcome a future intrusion. Organisations often have many reasons for detecting network traffic.
- **Protect**. This is where policies are created which protect systems, users and data against attack, and in reducing this potential damage. A key element of this is to protect them against accidental damage, as accidental damage is often more prevalent than non-accidental damage.
- **React**. This is where a policy is defined which reacts to intrusions, and defines ways to overcome them in the future. Often organisations do not have formal policies for this type of activity, and often rely on ad-hoc arrangements, where the method of reacting to a security breach is created after the event.
- **Recover**. This is where policies are defined to overcome any system damage, whether it is actual physical damage, the abuse of users; or the damage to data.
- **Audit/verify**. It is important that the security policy allows for auditing and for the verification that it achieves its requirements.



Policies

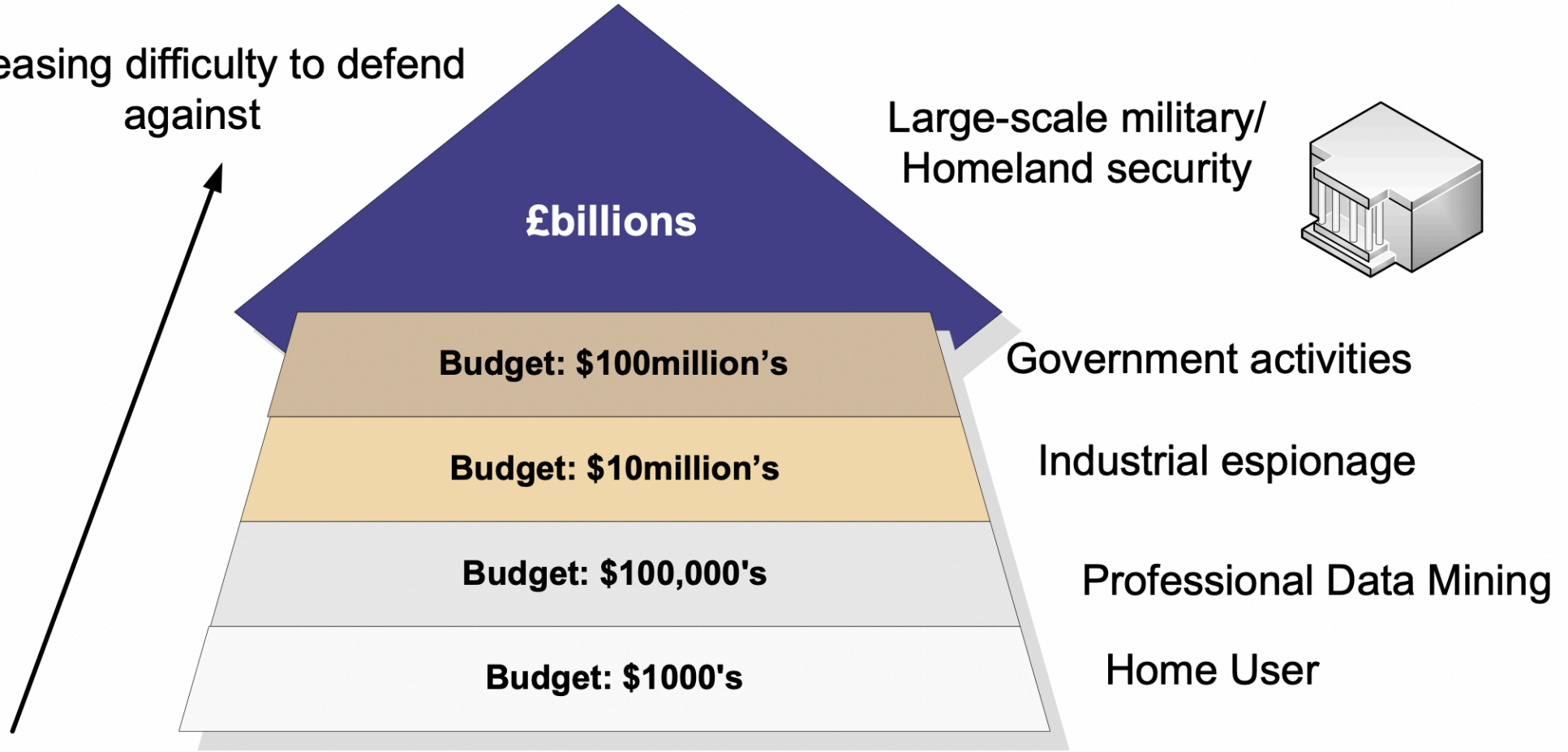
- **Deter**. This is where the system is designed anc order to initially deter intruders from attacking first place.
- **Log**. This is a key element in modern systems w form of logging system. It is important that the does not breach any civil liberties, and is in a fc used to enhance the future security of the syst
- **Detect**. This is where detection agents are plac network to detect intrusions, and has methods events that occurred in an intrusion, so that it in a forensic computing investigation, and/or tc future intrusion. Organisations often have man detecting network traffic.
- **Protect**. This is where policies are created whic users and data against attack, and in reducing t damage. A key element of this is to protect the accidental damage, as accidental damage is oft than non-accidental damage.
- **React**. This is where a policy is defined which re and defines ways to overcome them in the futu organisations do not have formal policies for th and often rely on ad-hoc arrangements, where reacting to a security breach is created after th
- **Recover**. This is where policies are defined to o system damage, whether it is actual physical da of users; or the damage to data.
- **Audit/verify**. It is important that the security policy allows for auditing and for the verification that it achieves its requirements.



&cyber data

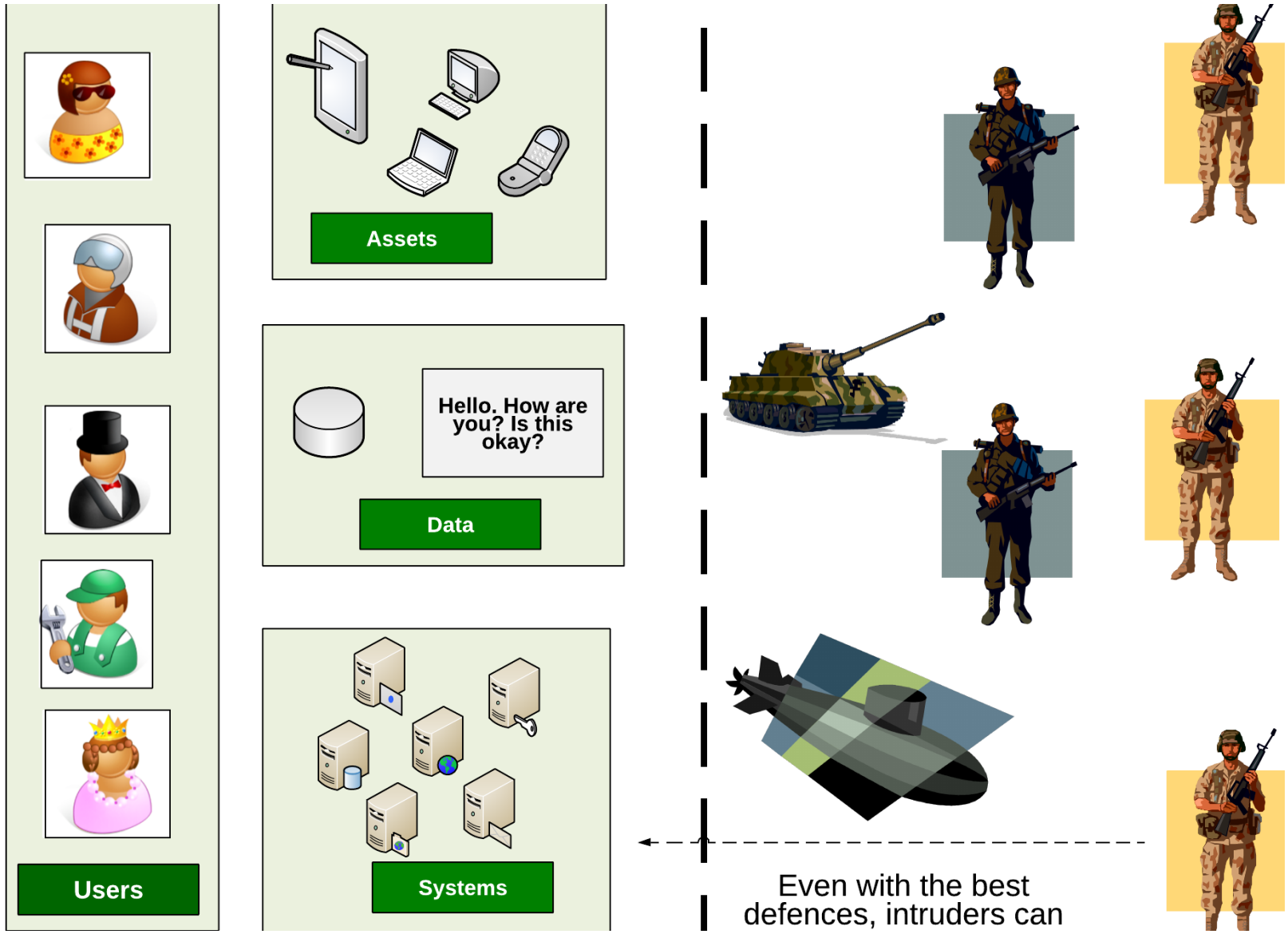
Policies

- **Dete**
  orde
  first
- **Log.**
  form
  does
  used
- **Dete**
  netw
  even
  in a
  futu
  dete
- **Prot**
  user
  dam
  acci
  than
- **Reac**
  and
  orga
  and
  reac
- **Reco**
  syste
  of us
- **Audi**
  audi



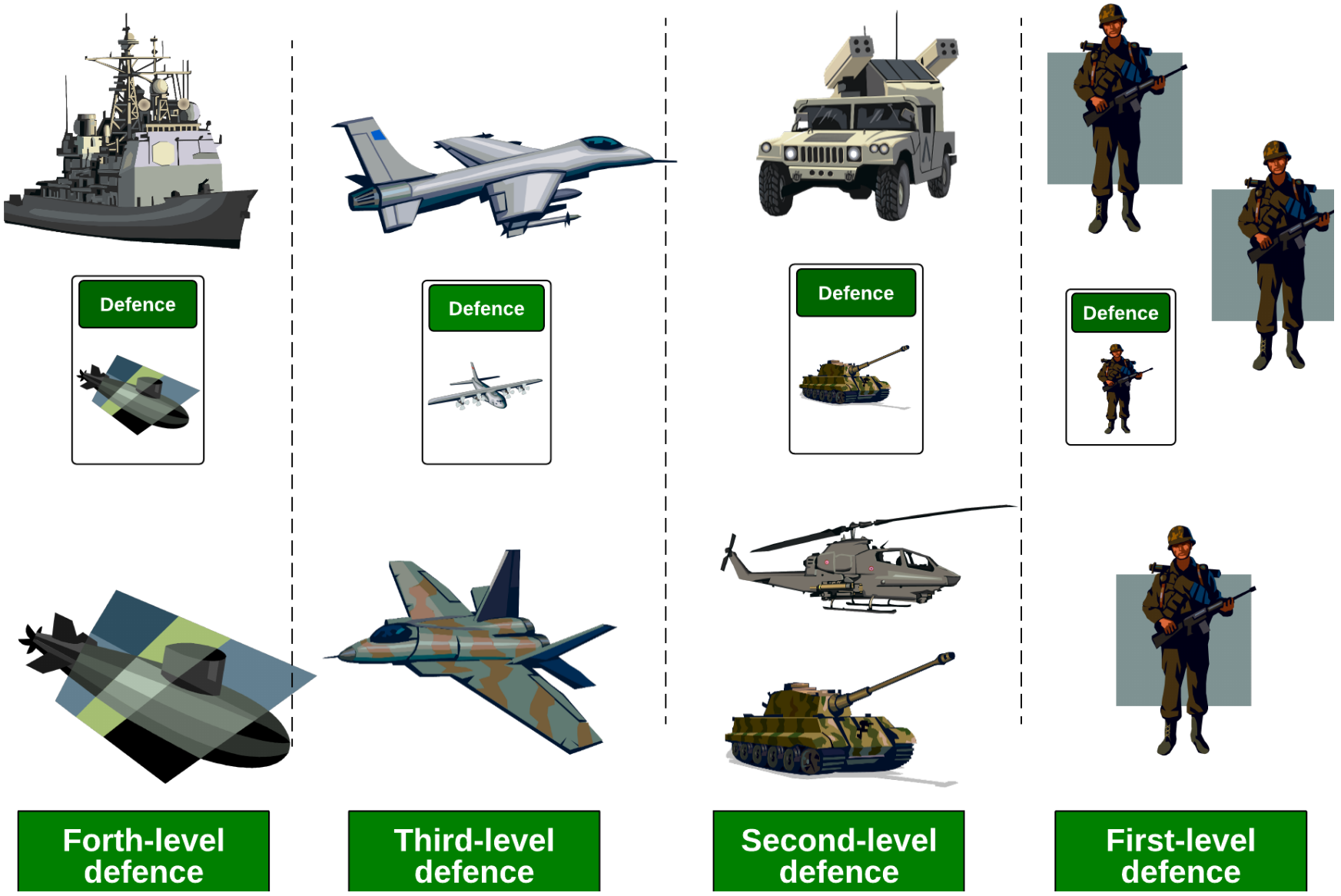
&cyber data

Defence in depth



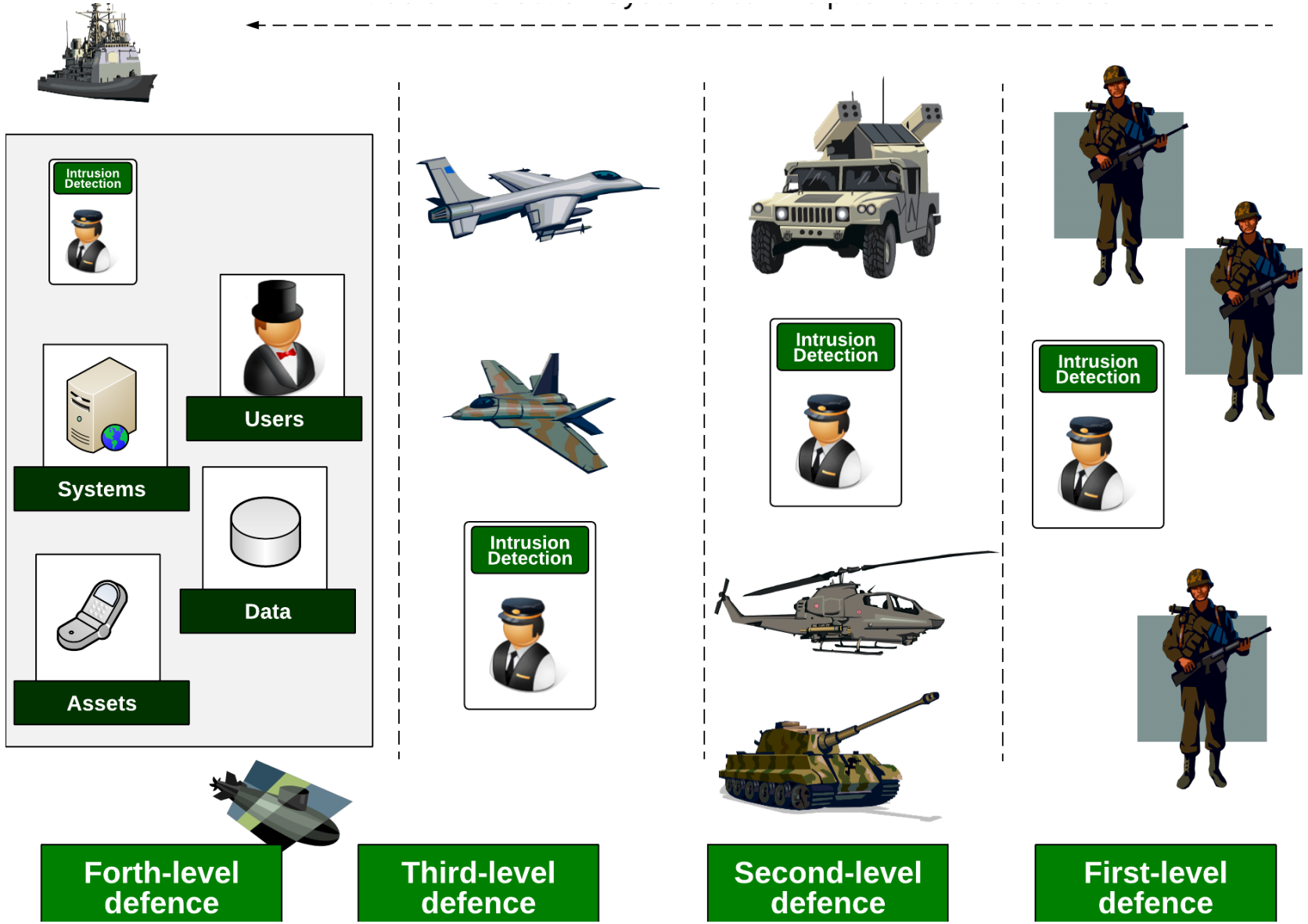
&cyber data

Defence in depth



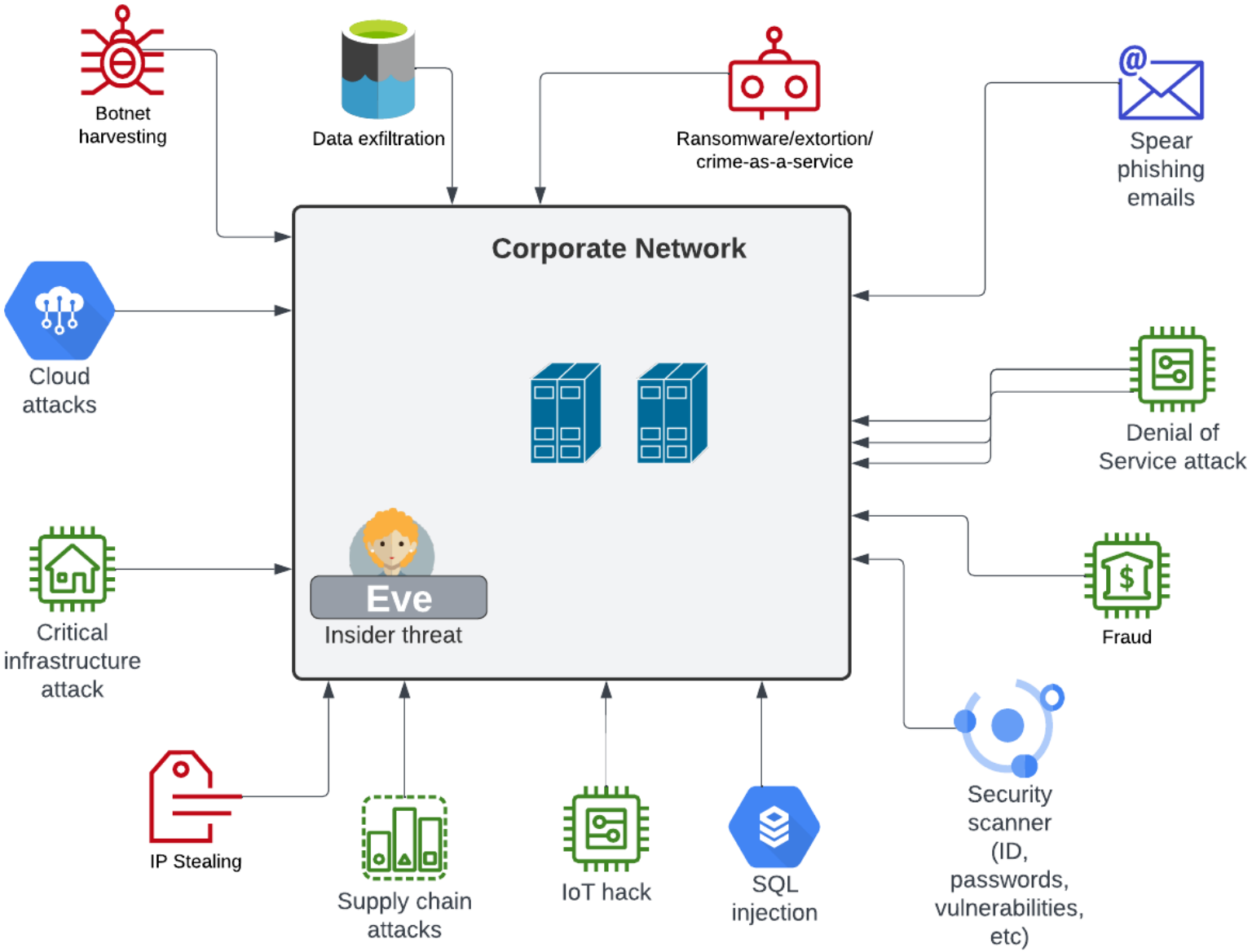
&cyber data

Intrusion Detection Systems (IDS)



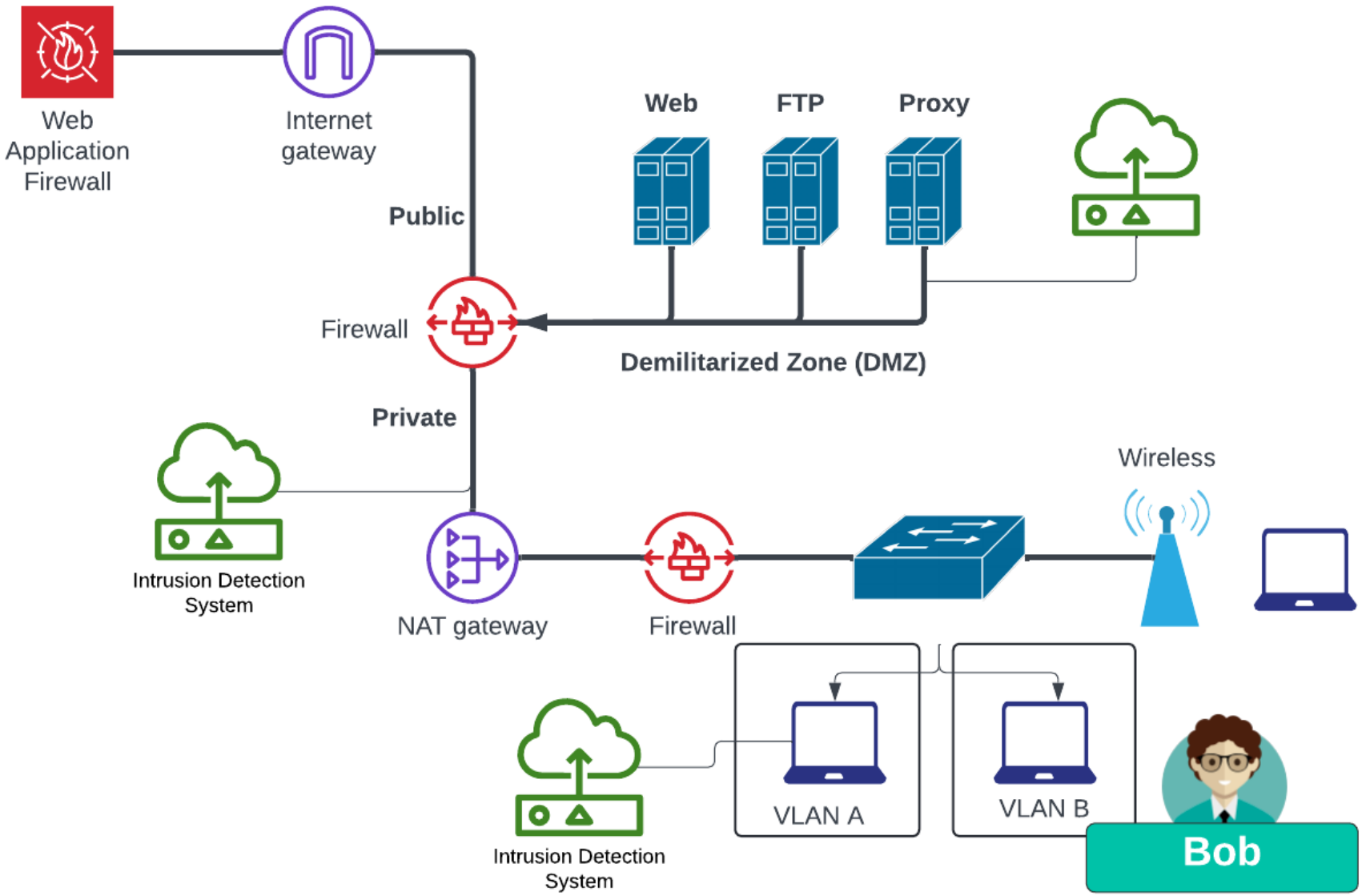
&cyber data

Threats

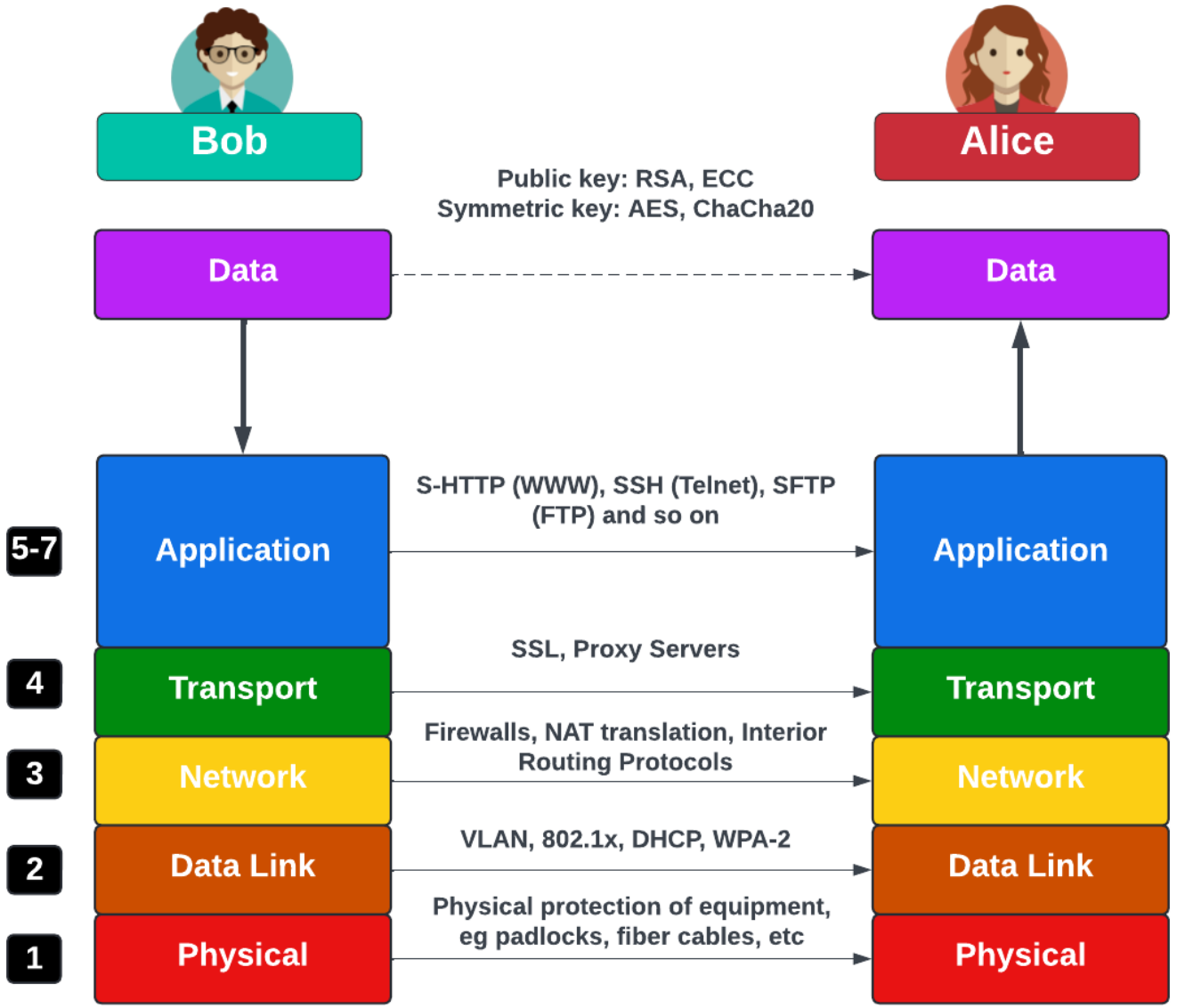


&cyber data

Defence in depth



OSI 7-Layered Model



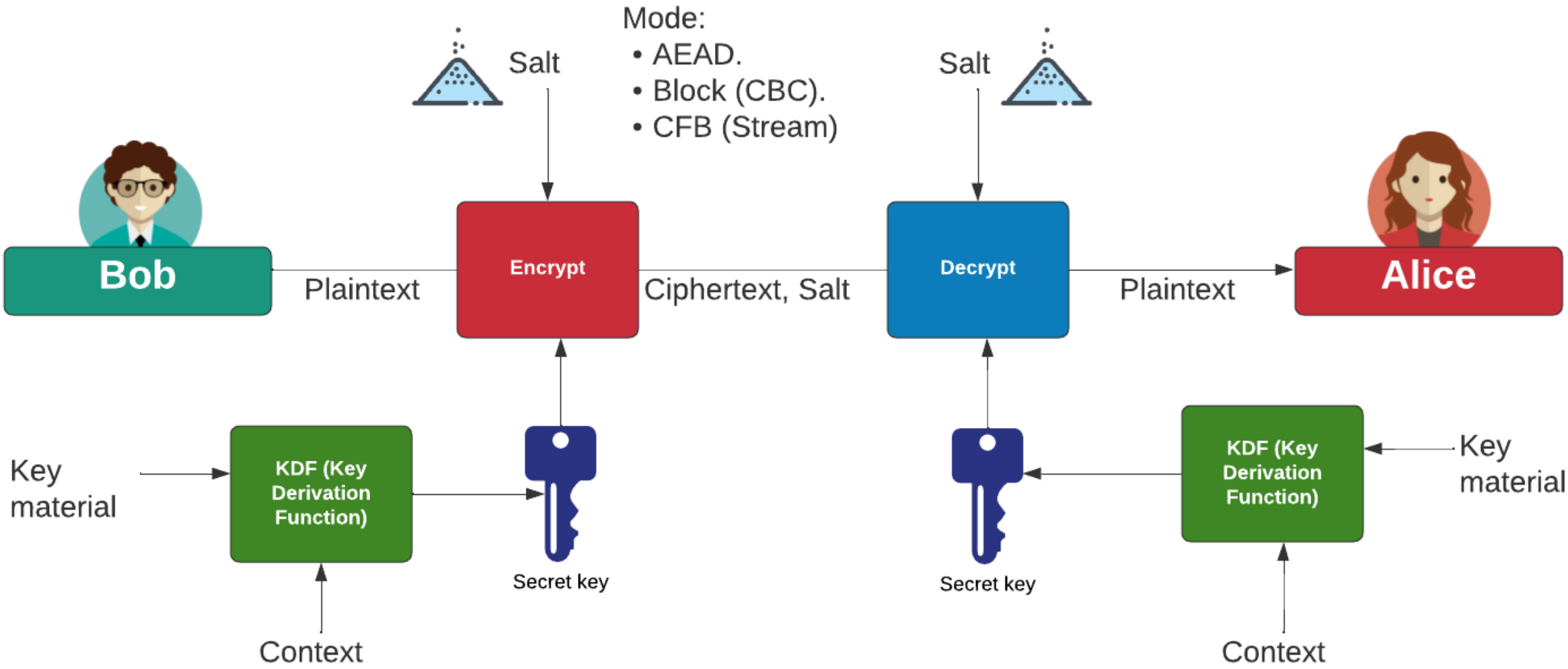
&cyber data

cyber & data

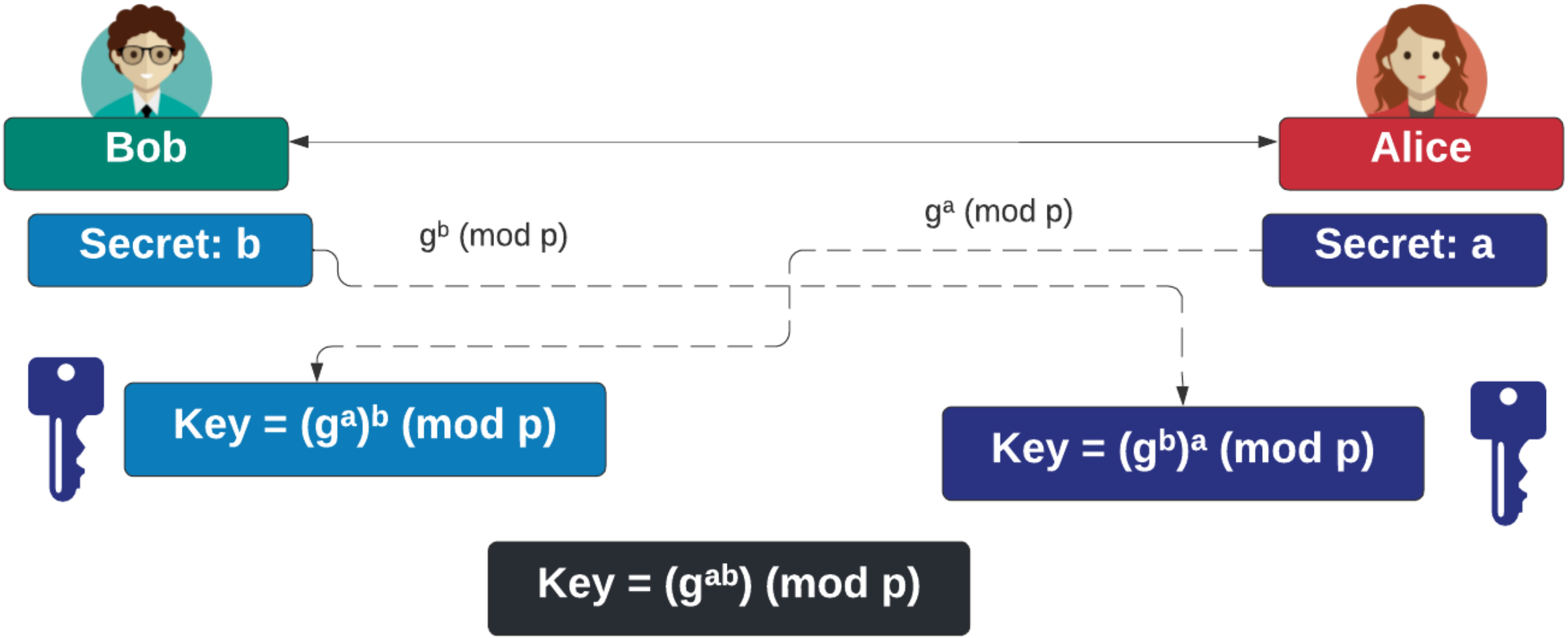
"From bits to information"

Basics of Cryptography

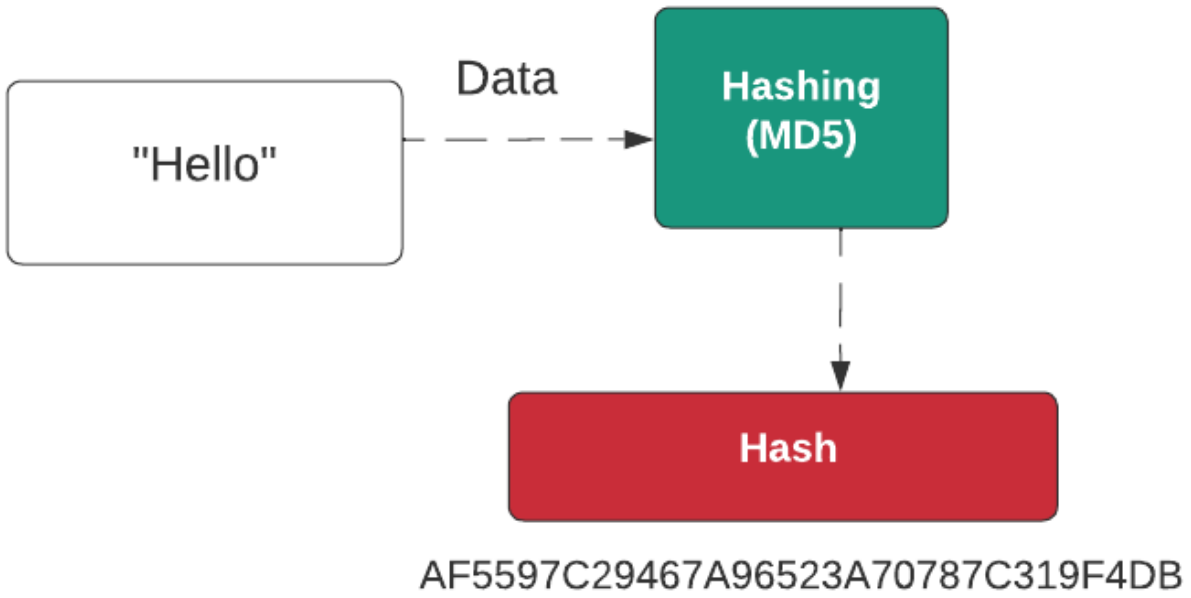
Symmetric Key Encryption



Key Exchange



Hashing



Hashed password

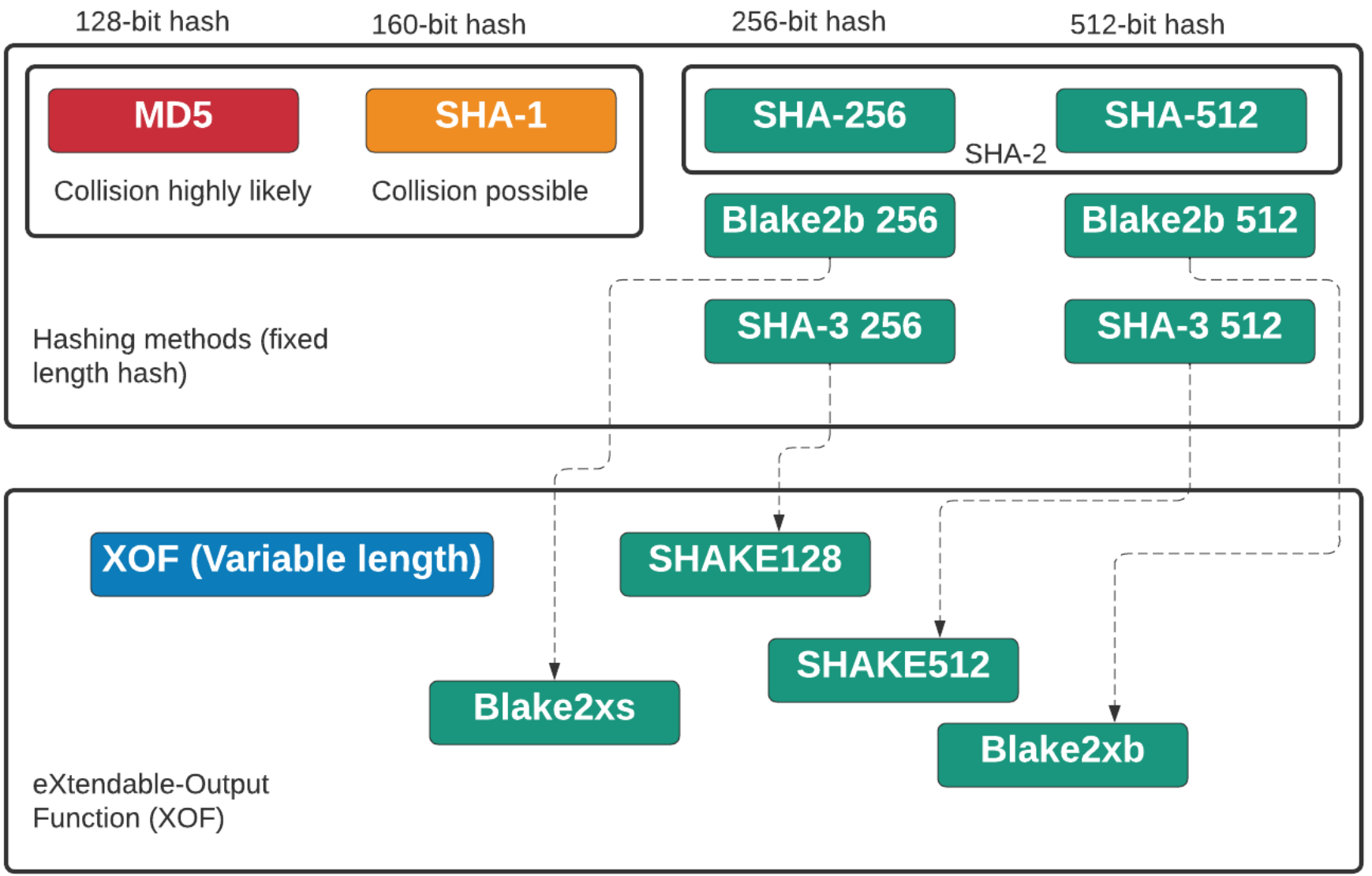
Bob: AF5597C29467A96523A70787C319F4DB

Hashed password with salt (hellozj8n)

Bob: zj8n:51A7C663A3BDCD06D6CE21E2BCB2AD5A

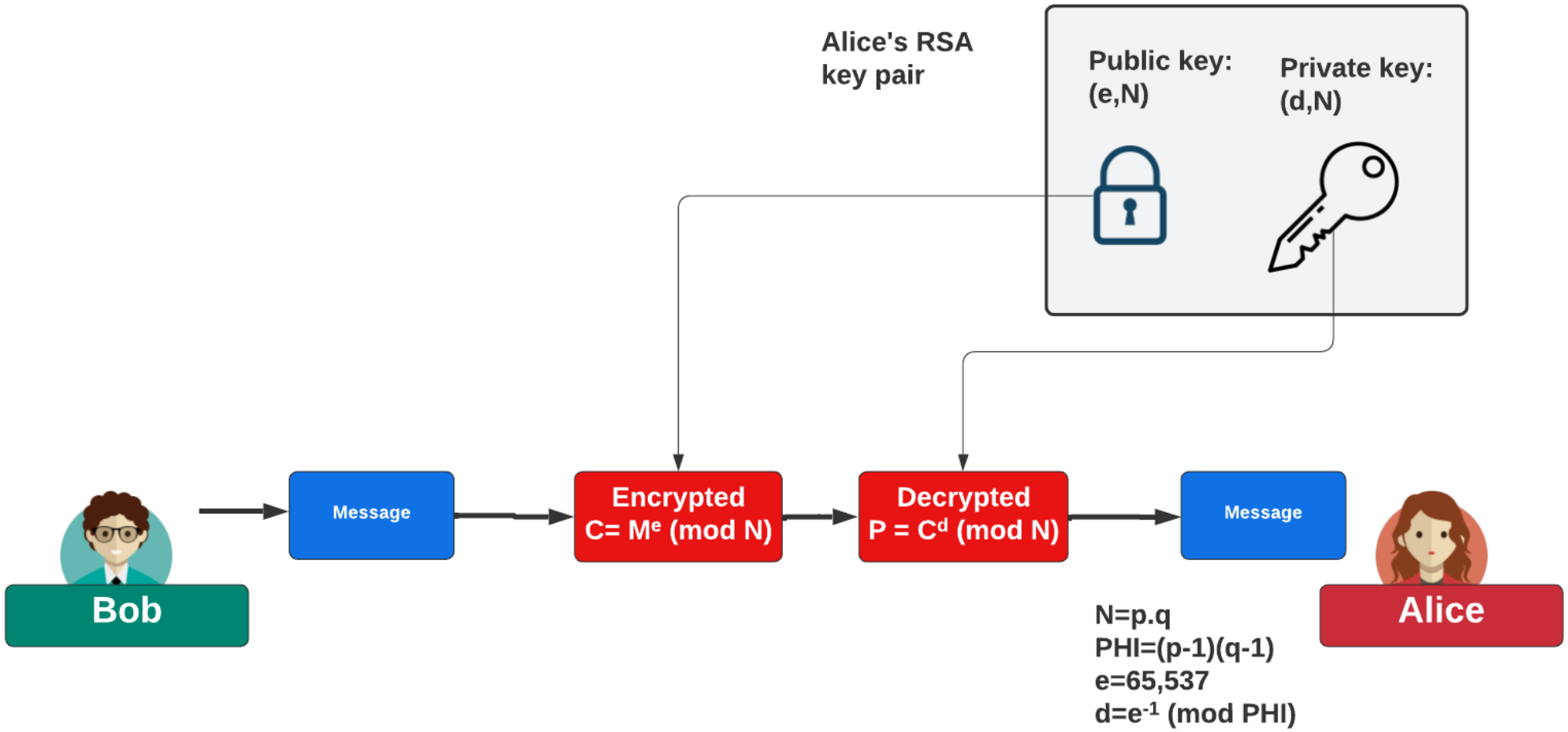
&cyber data

Hashing

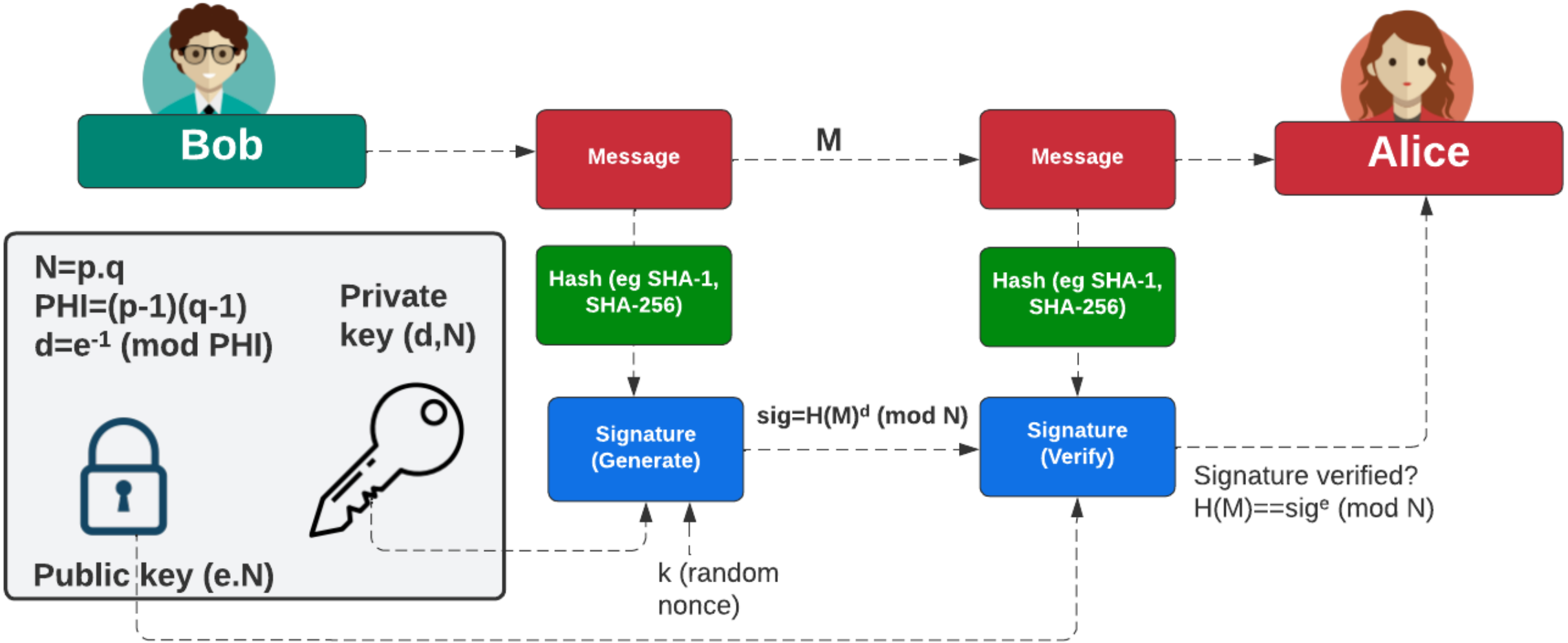


&cyber data

Public Key Encryption



Public Key (Digital Signing)



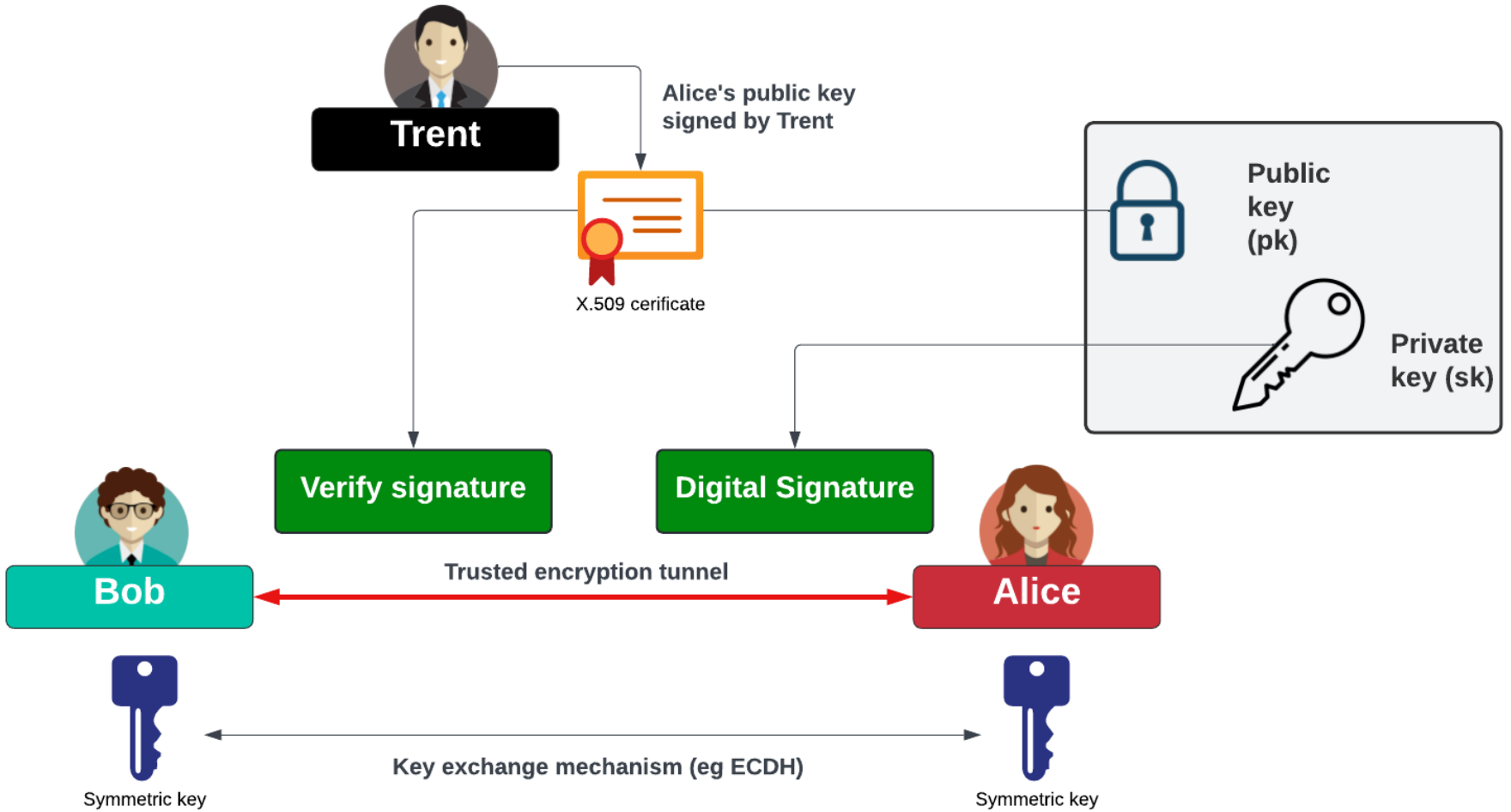
&cyber data

cyber & data

"From bits to information"

Outline of Secure Architectures

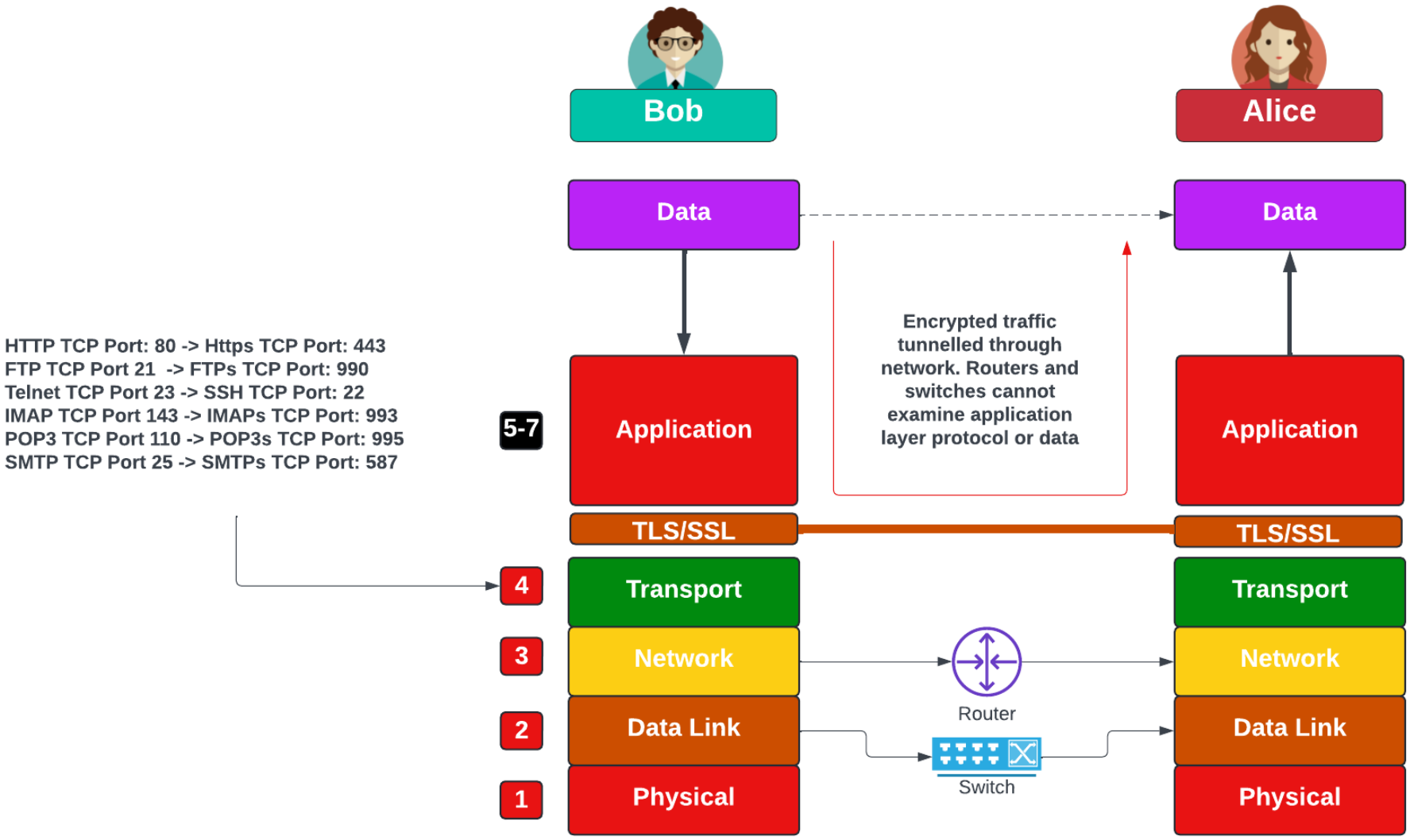
Trust, Privacy and Integrity



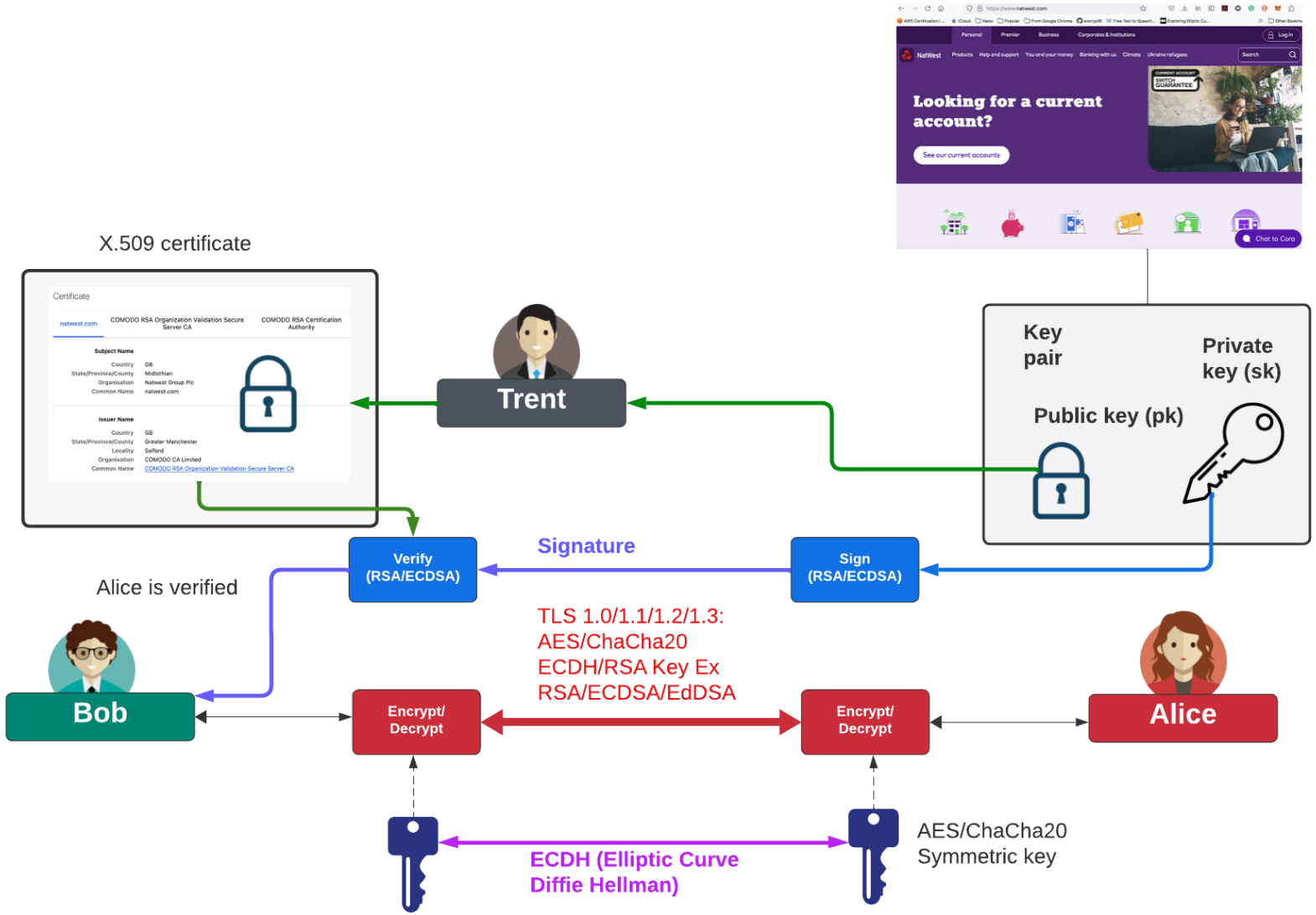
Public key method: RSA, ECDSA
Symmetric Key method: AES, ChaCha20
Integrity checking: SHA-1, SHA-256

&cyber data

Tunneled Traffic

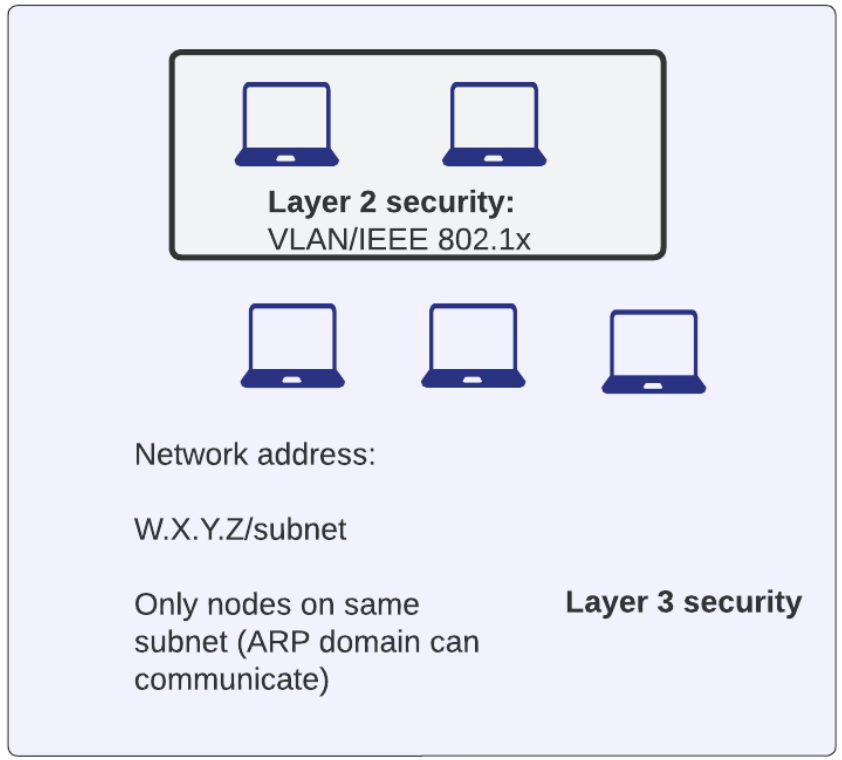


Tunneled Traffic

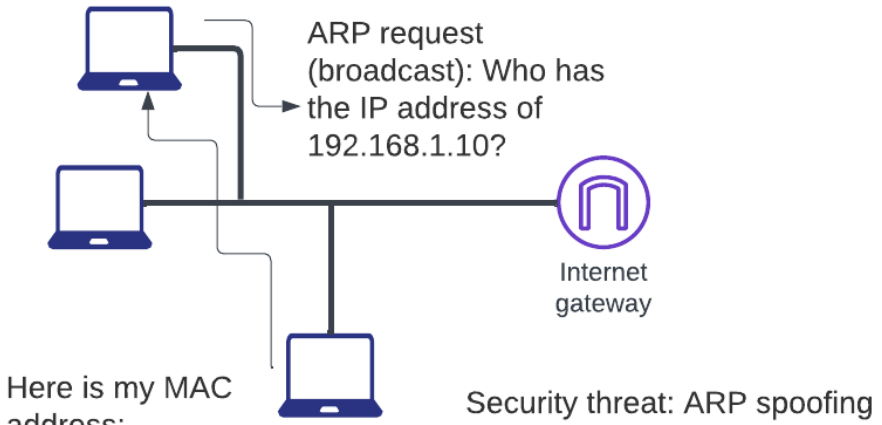


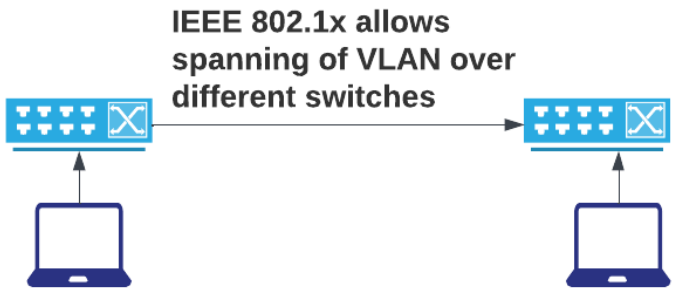
&cyber data

Layer 2 and Layer 3 Security



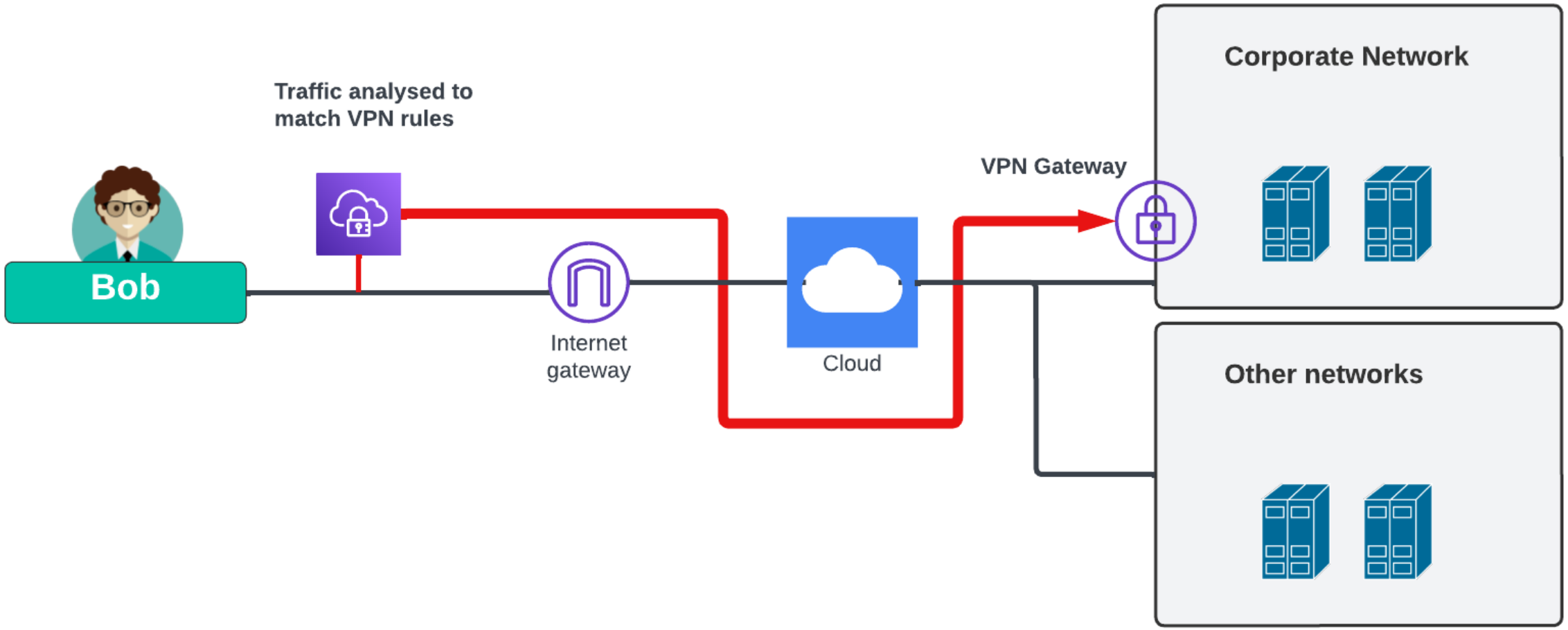
ARP Cache:
192.168.1.0 -> 11:22:33:44:55:66



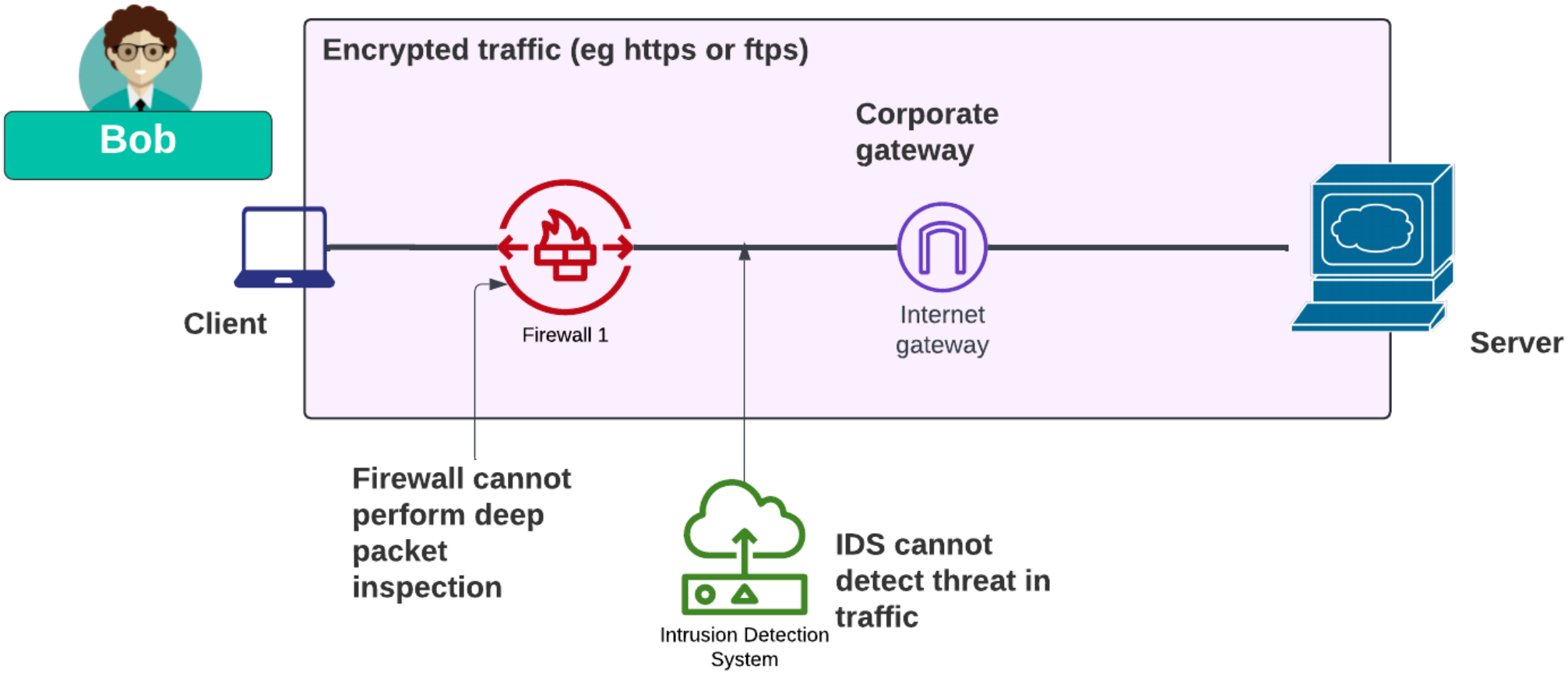


&cyber data

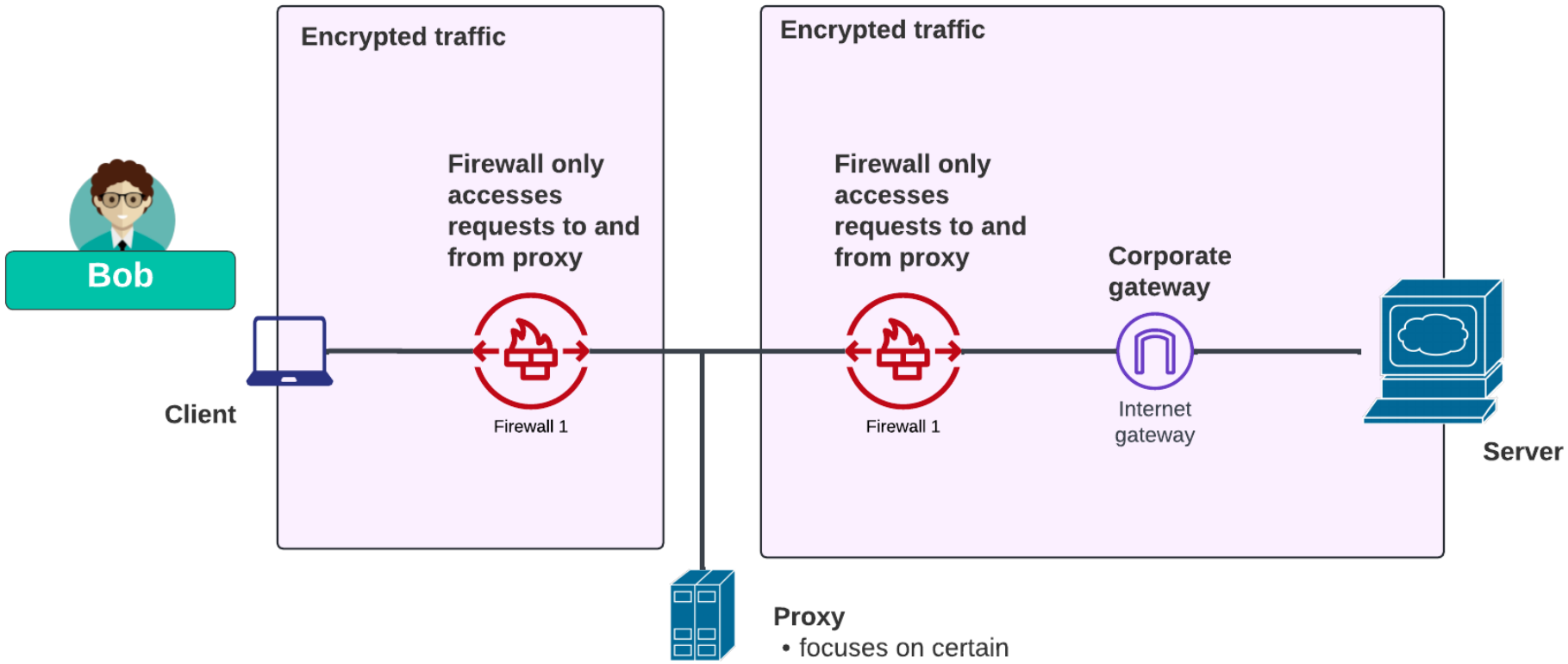
VPN (Virtual Private Network) Tunneling



Tunneled Traffic

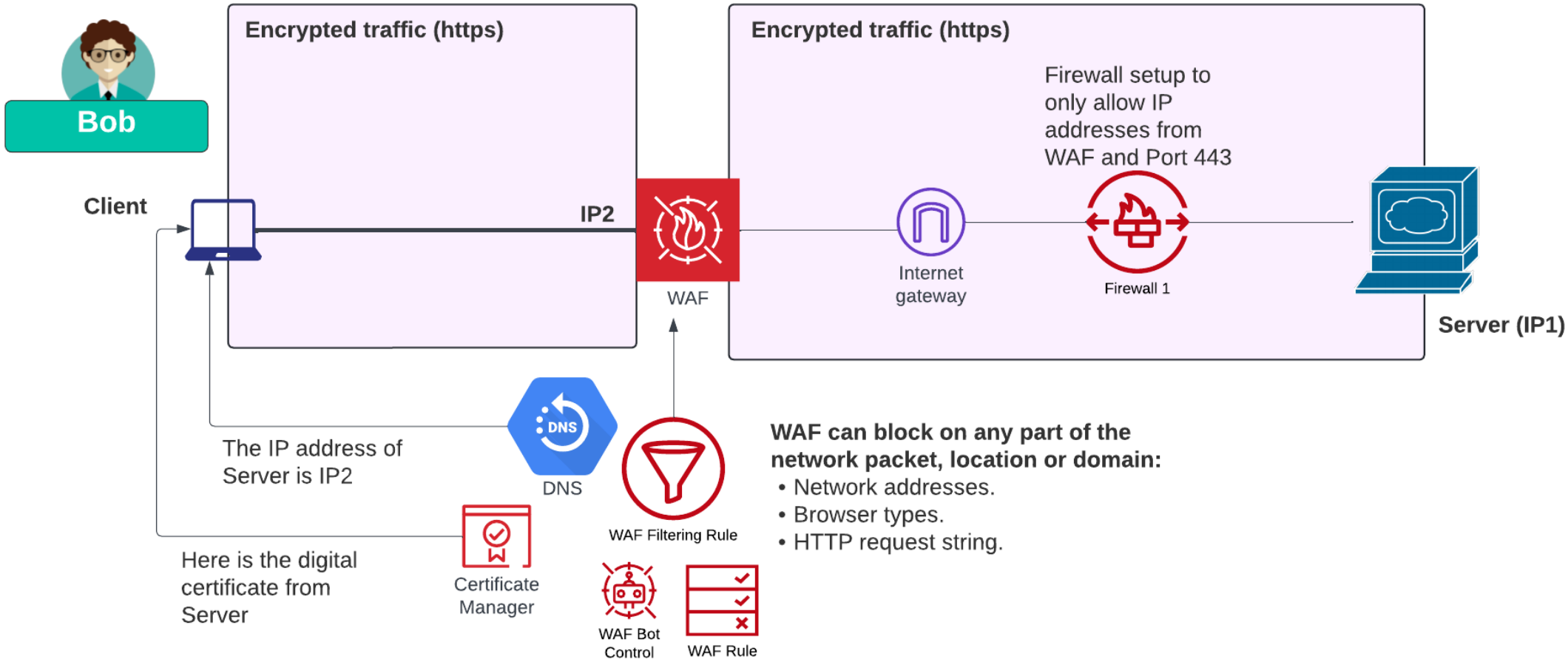


Dual-homed Architecture



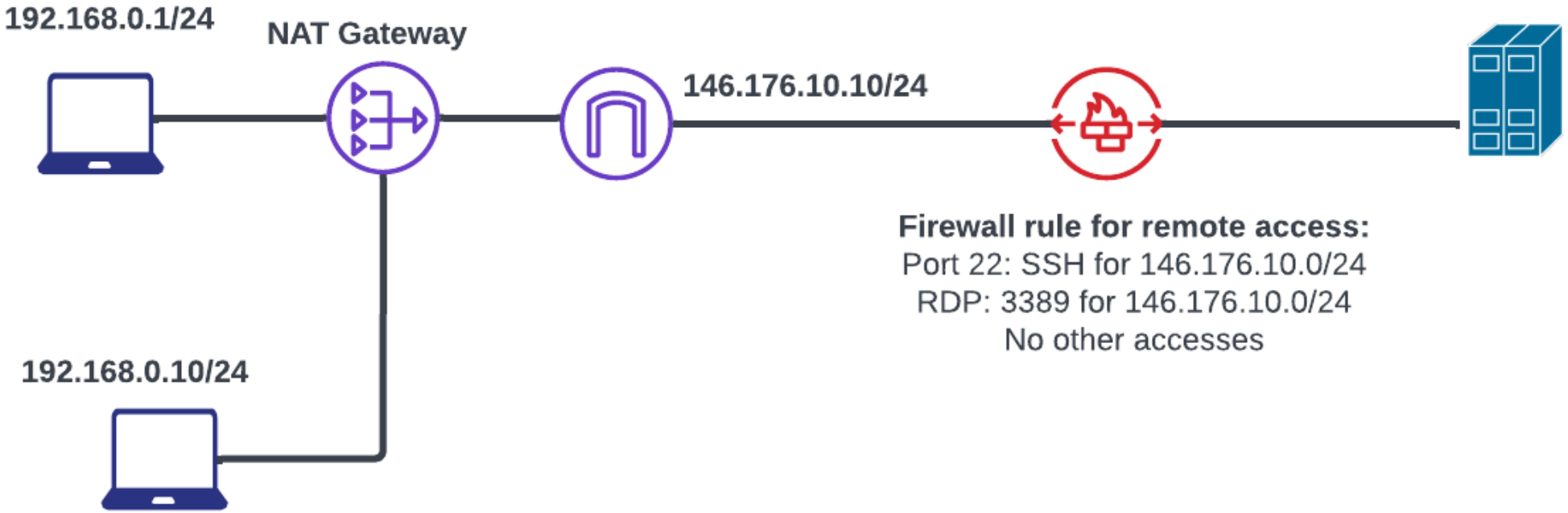
&cyber data

Web Application Firewall (WAF)



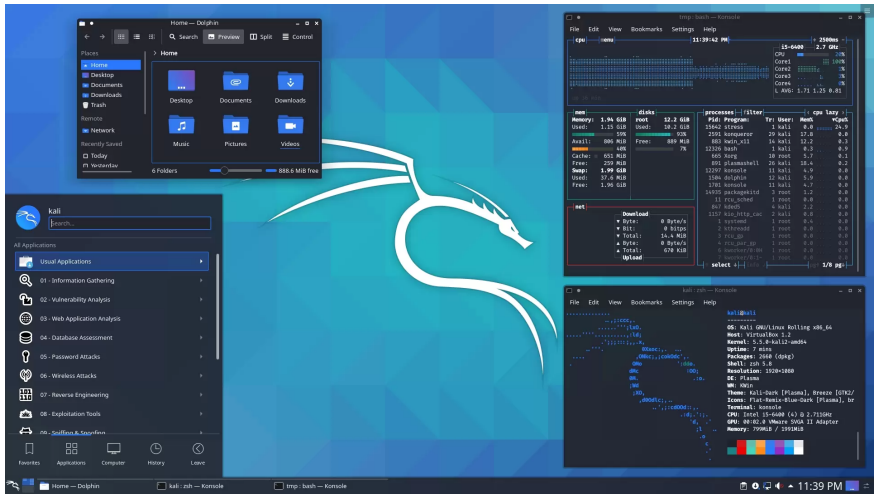
&cyber data

Remote Access to Device/Server



&cyber data

Pen Testing Tools



hydra -L list_user -P list_password 10.10.y.9 ftp

Hydra

nmap -O 10.10.10.10

Discover services
OS operating system
Devices connected

Creating exploits

metasploit

IP

BURPSUITE

Client setup for proxy at IP

Firewall

bill:$apr1$waZS/8Tm$jDZmiZBct/c2hysERc

Password database

Discoverting messages passed from client to server

Nessus

Scanning for know vulnerabilities

WIRESHARK

OWASP ZAP

Hashcat

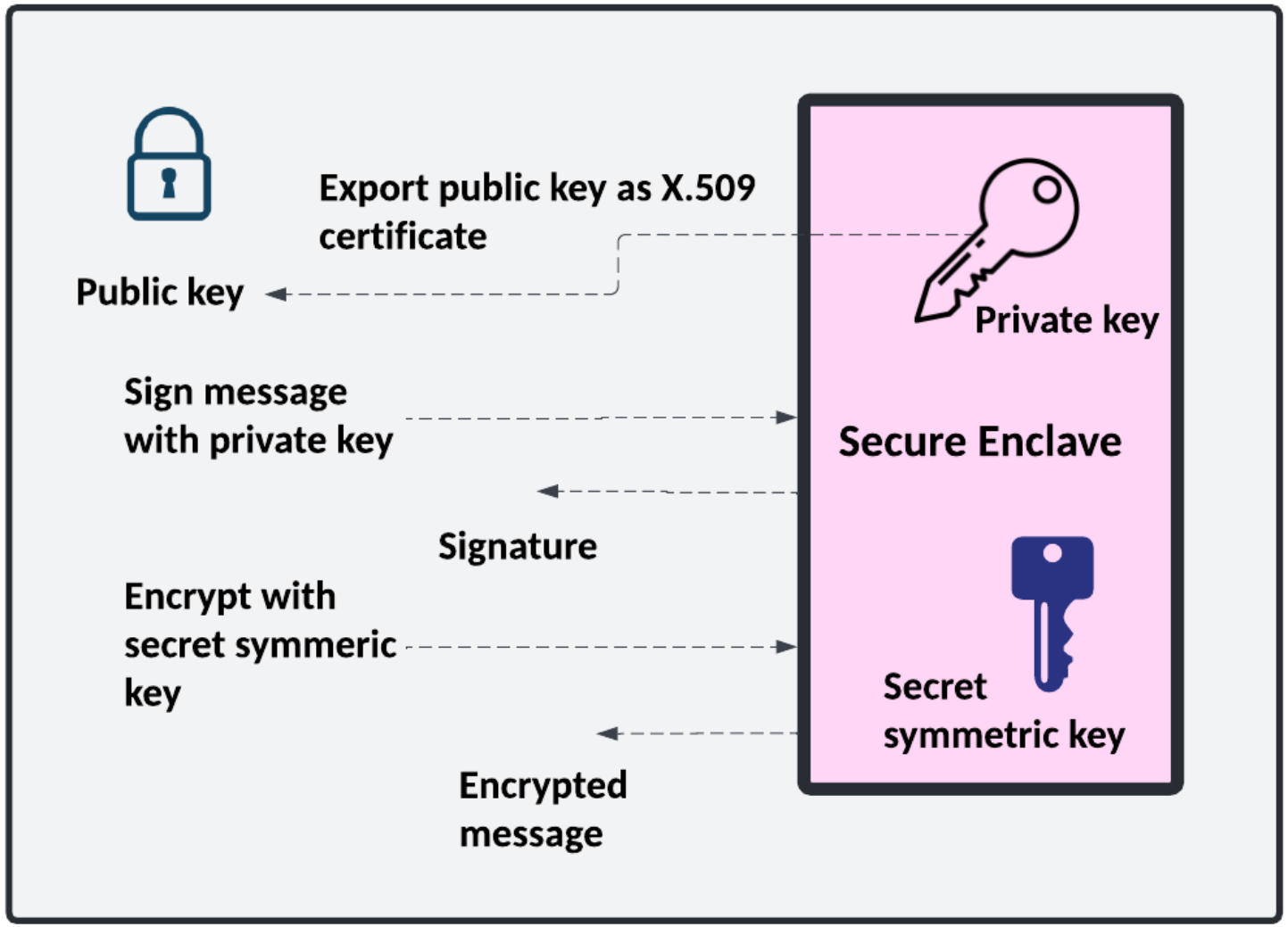
hashcat –m 0 hash1 words

&cyber data

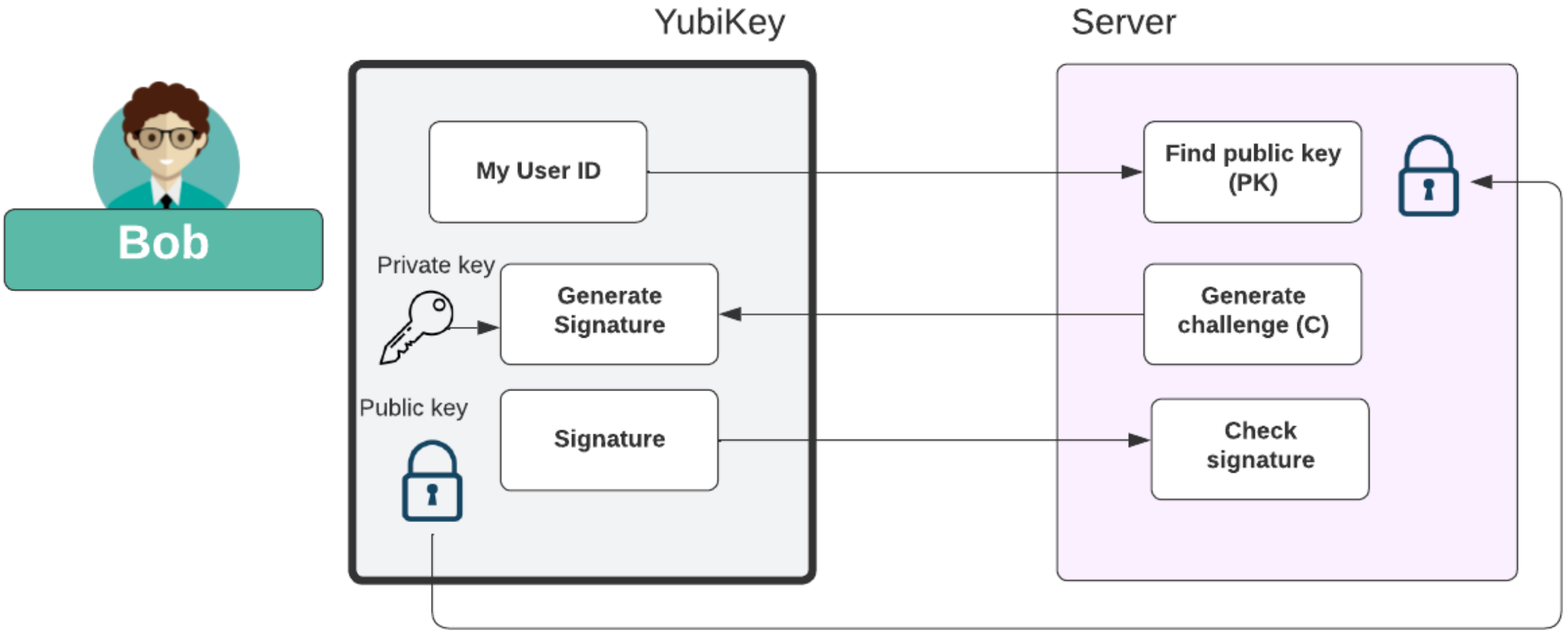
"From bits to information"

Secure Enclaves

Secure Enclaves

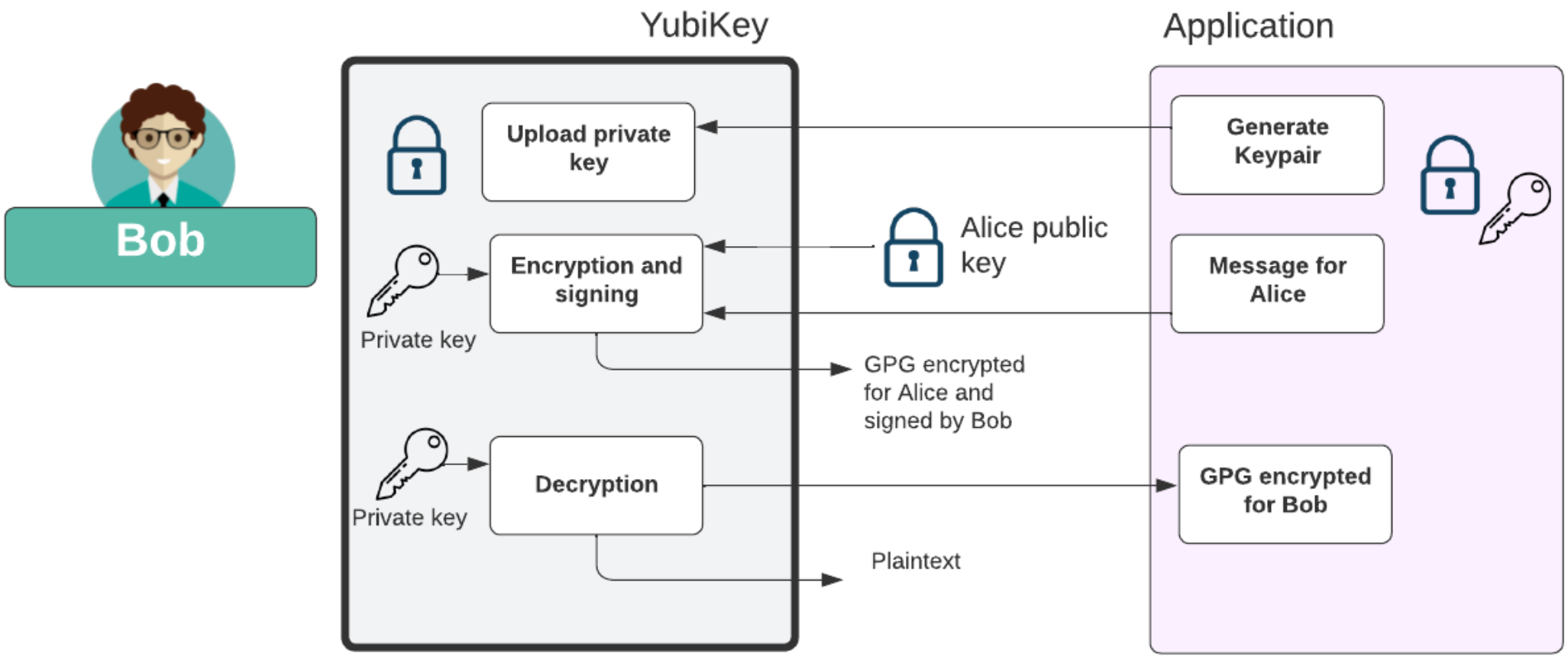


Secure Enclaves



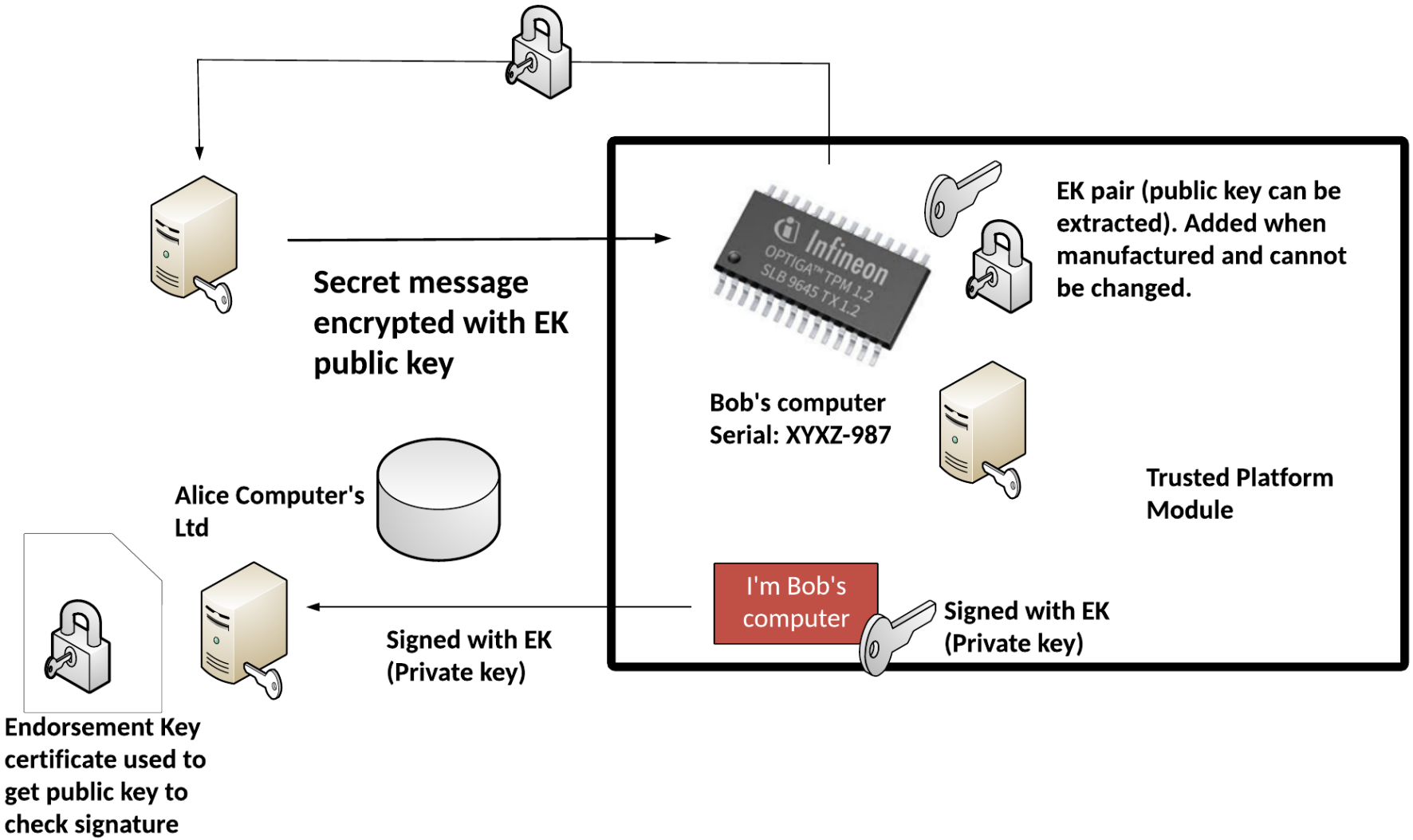
&cyber data

Secure Enclaves



&cyber data

MITRE EMB3D (Embedded Devices)



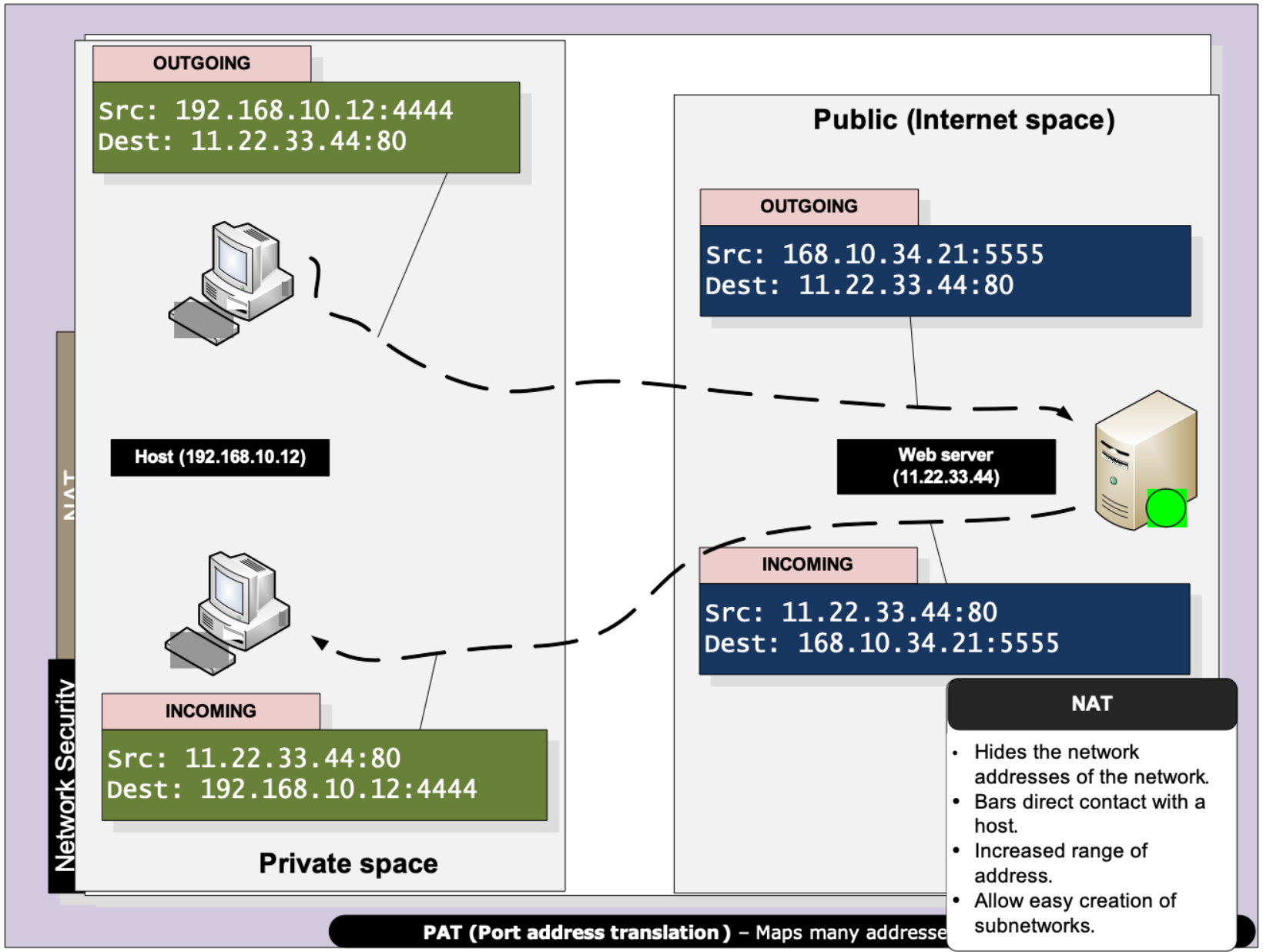
&cyber data

cyber & data

"From bits to information"

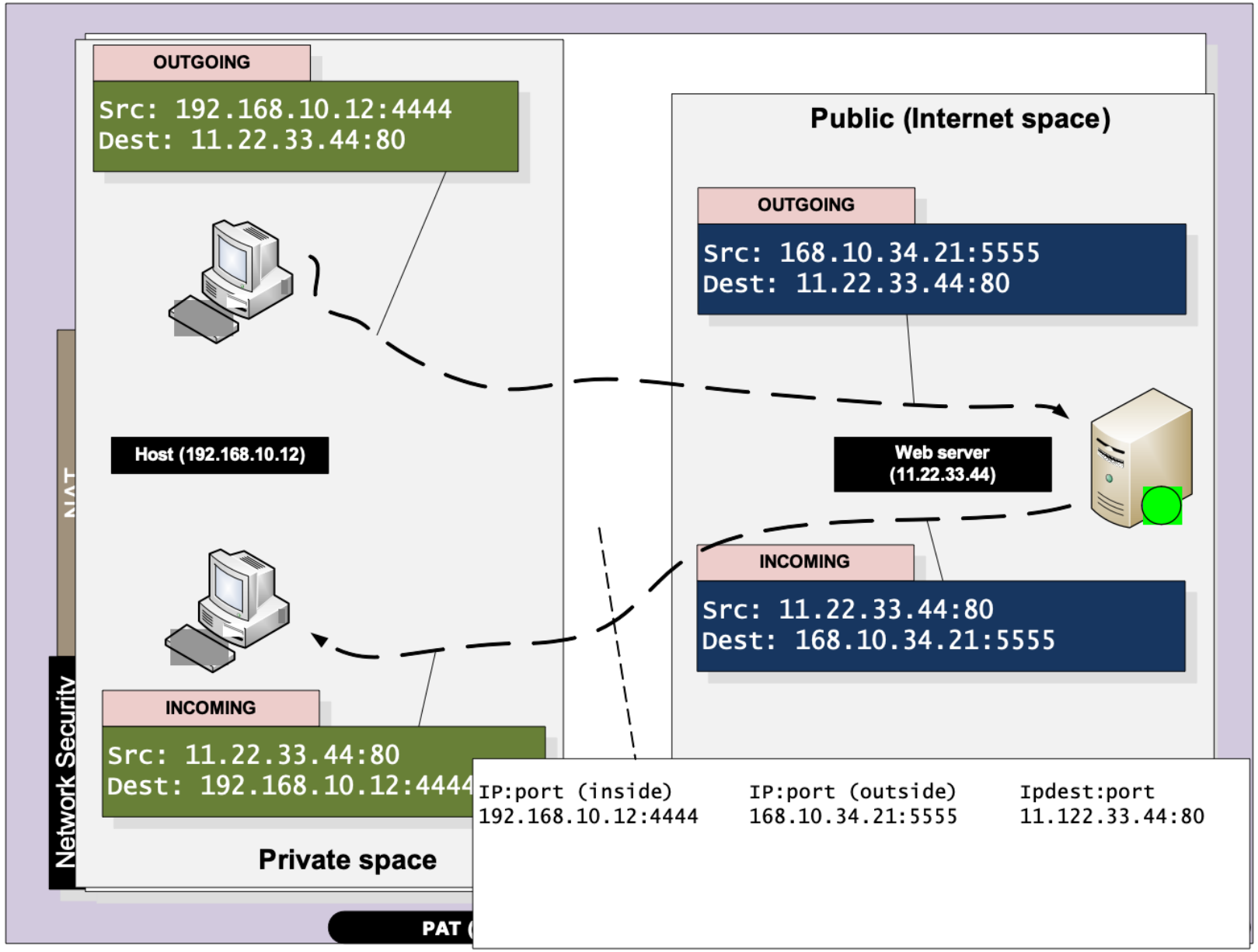
NAT

Layered Model



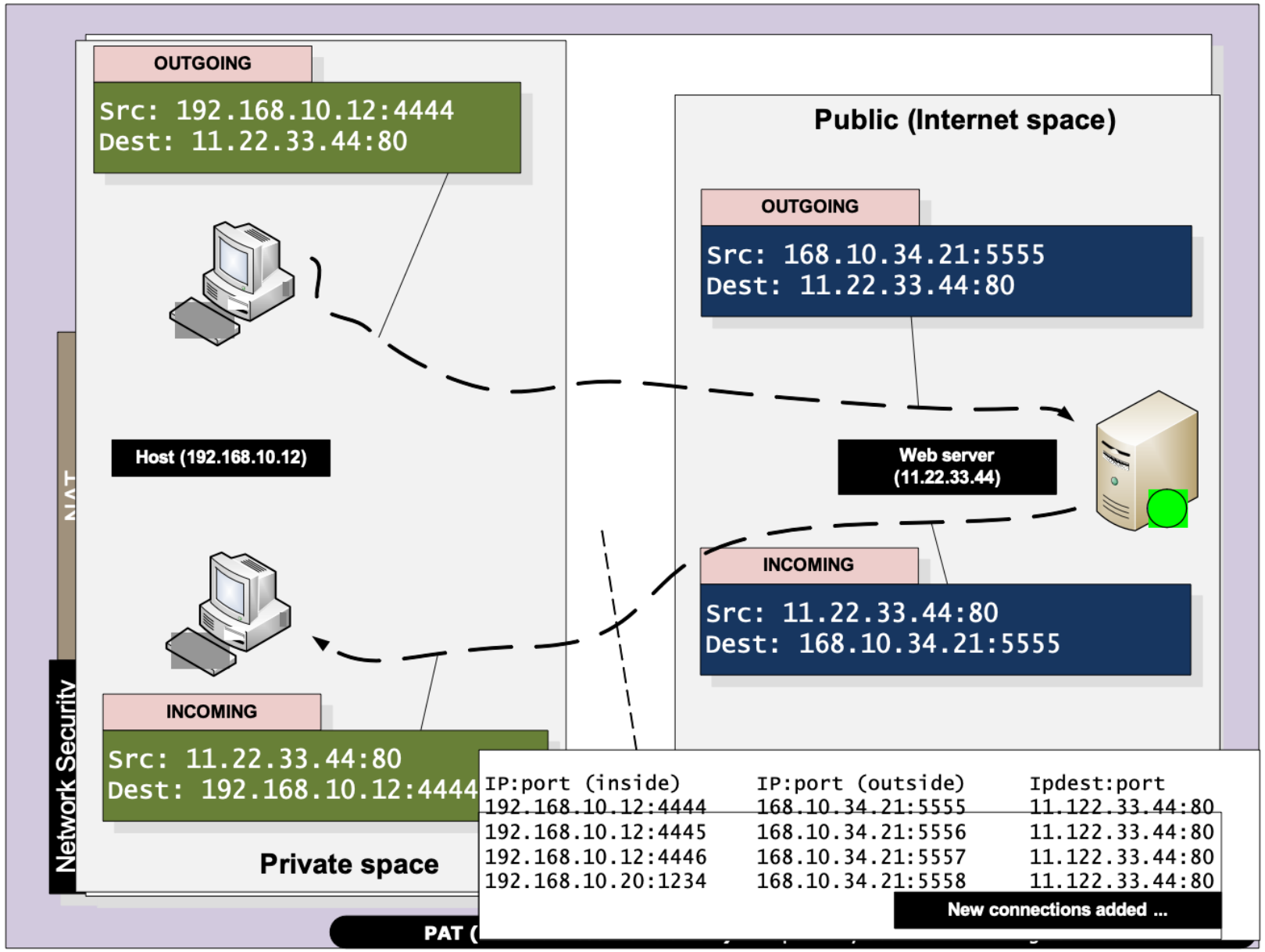
&cyber data

Layered Model



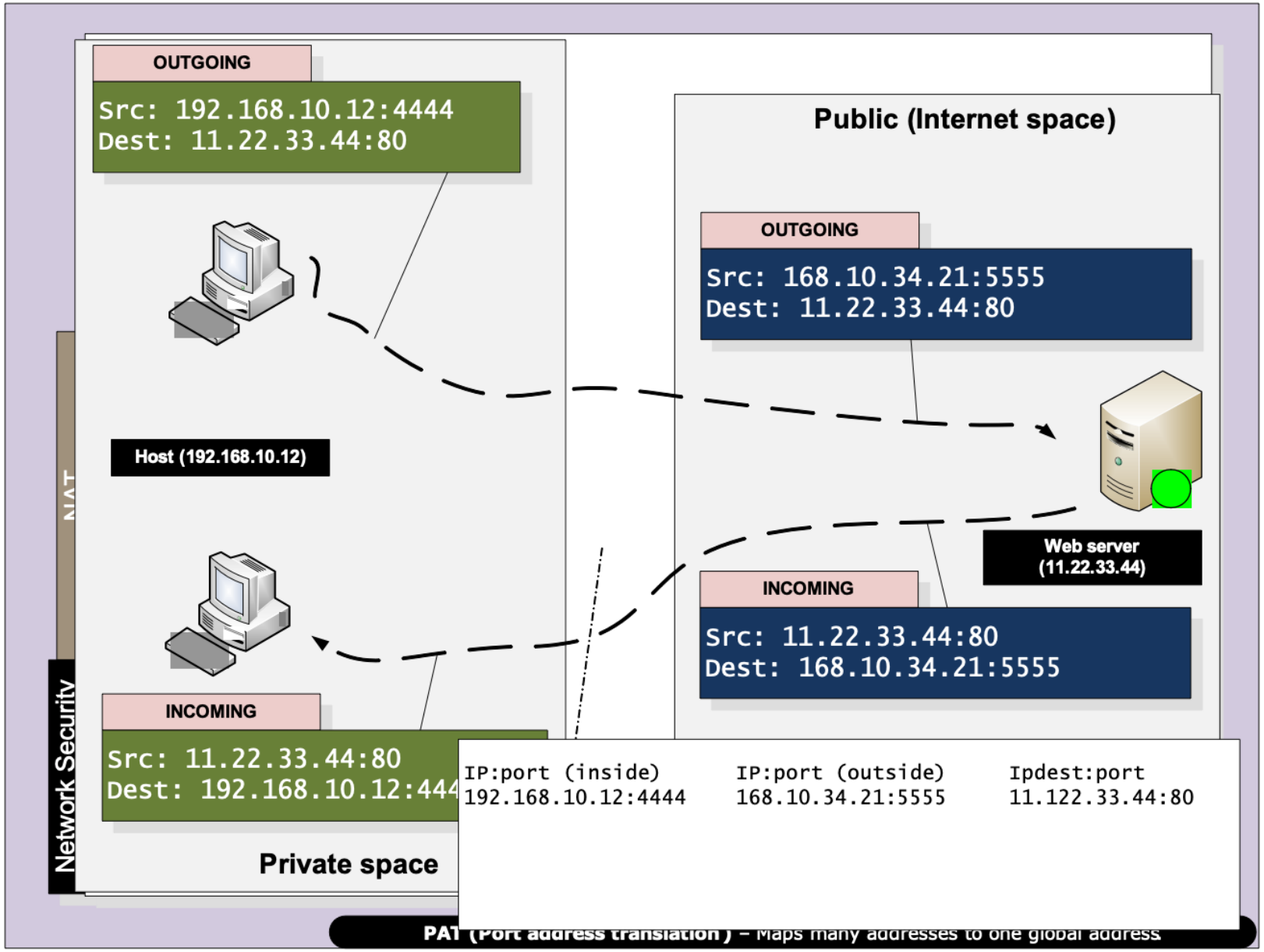
&cyber data

Layered Model



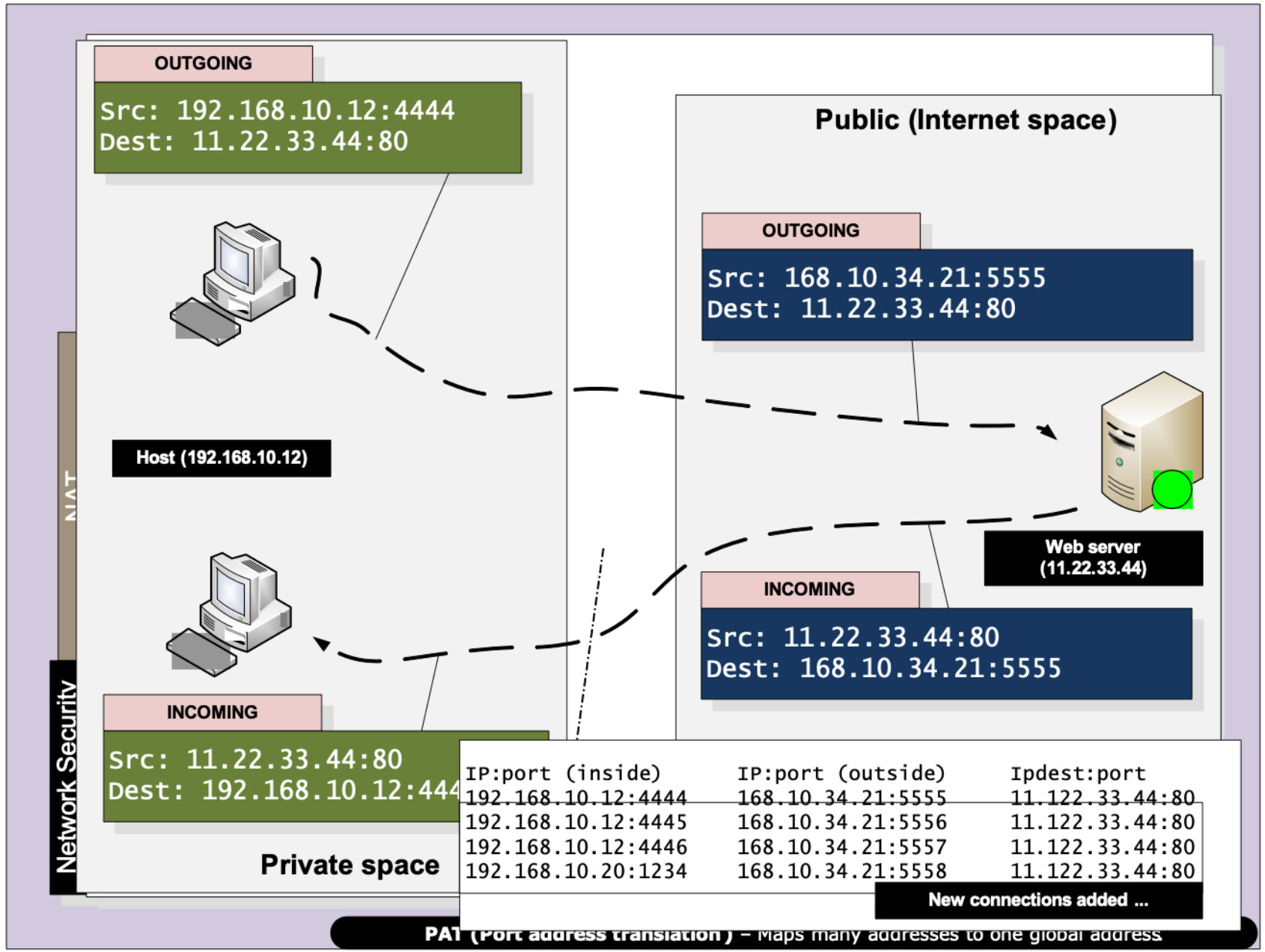
&cyber data

Layered Model



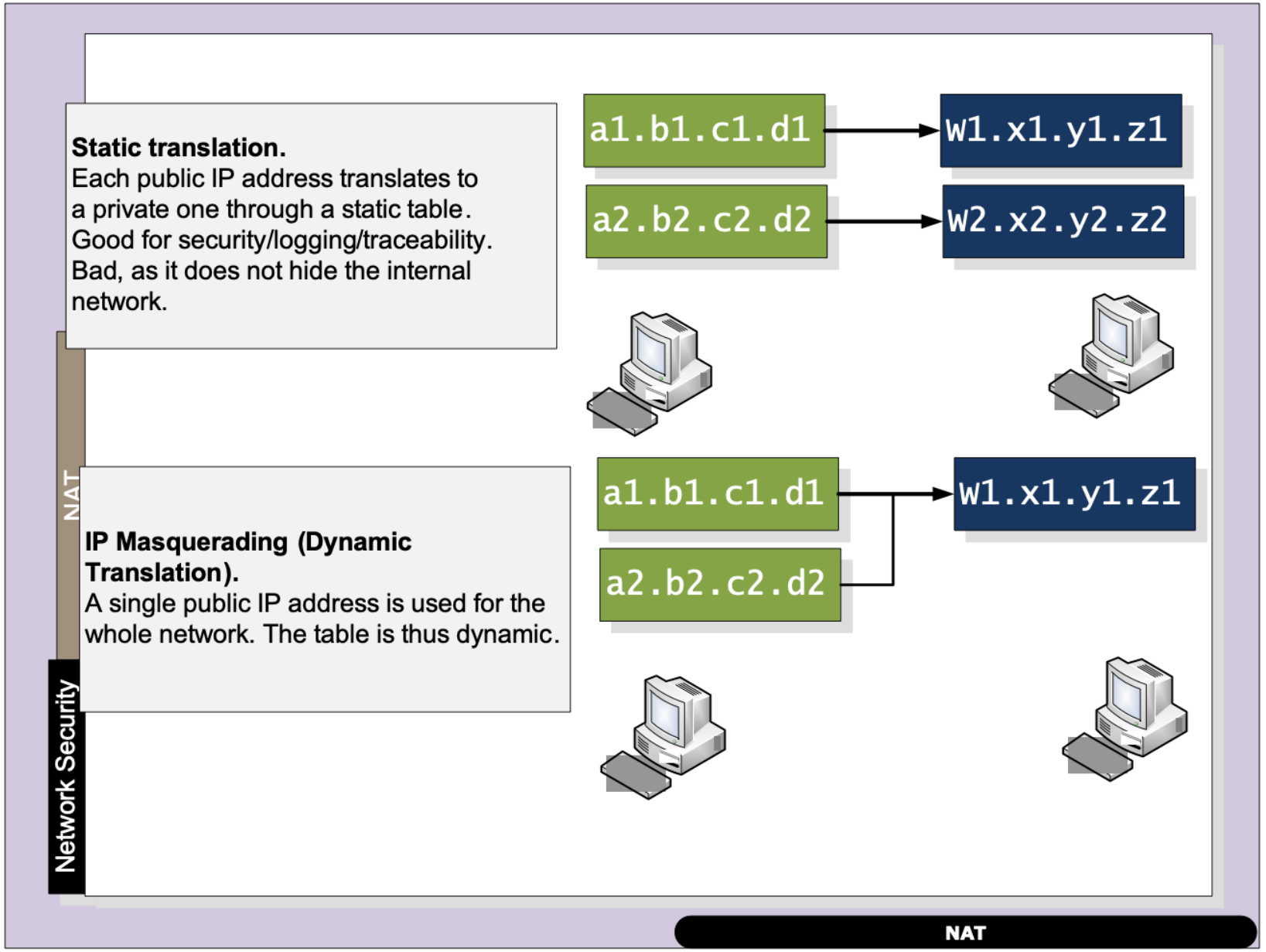
&cyber data

Layered Model



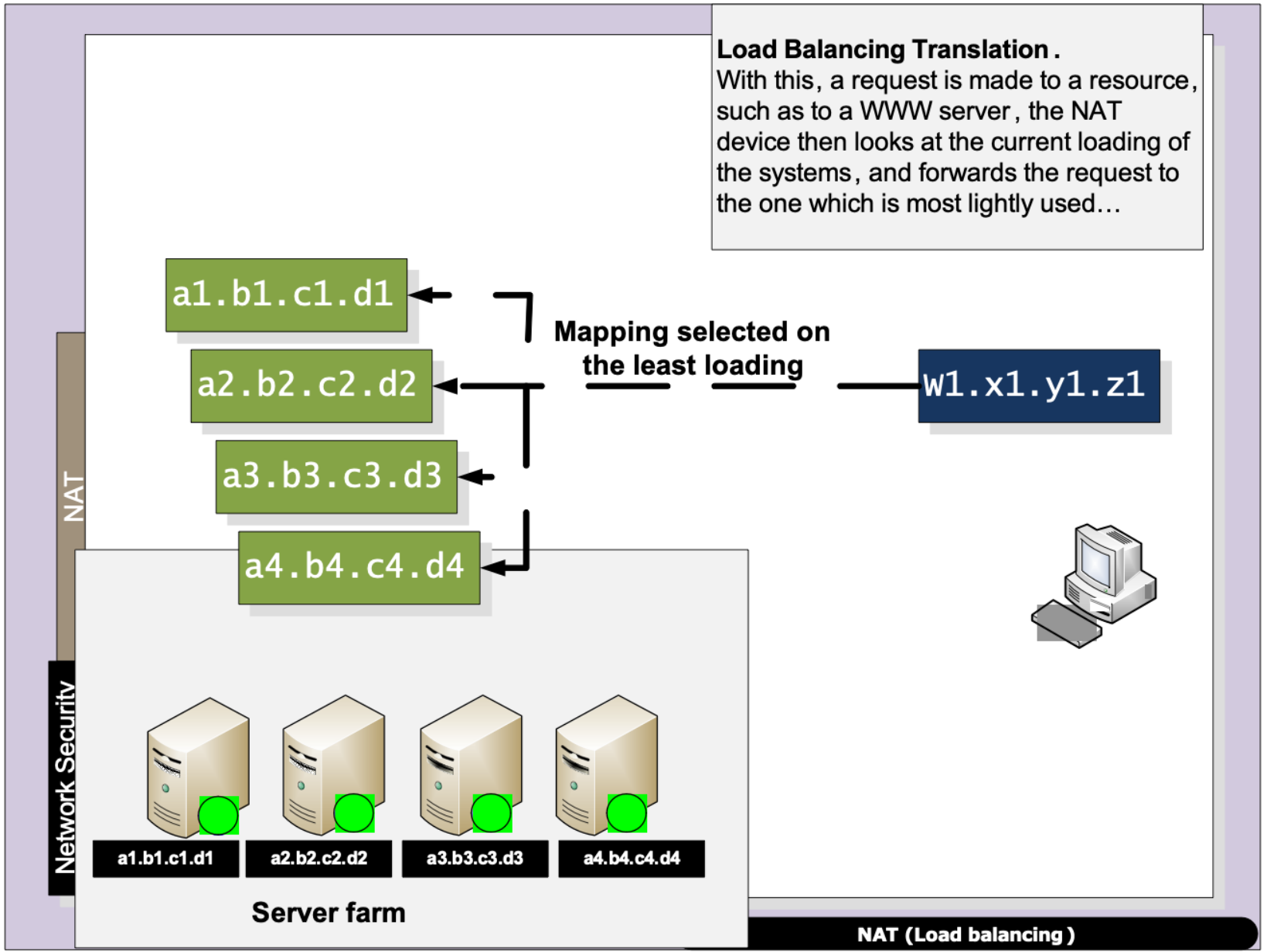
&cyber data

Layered Model



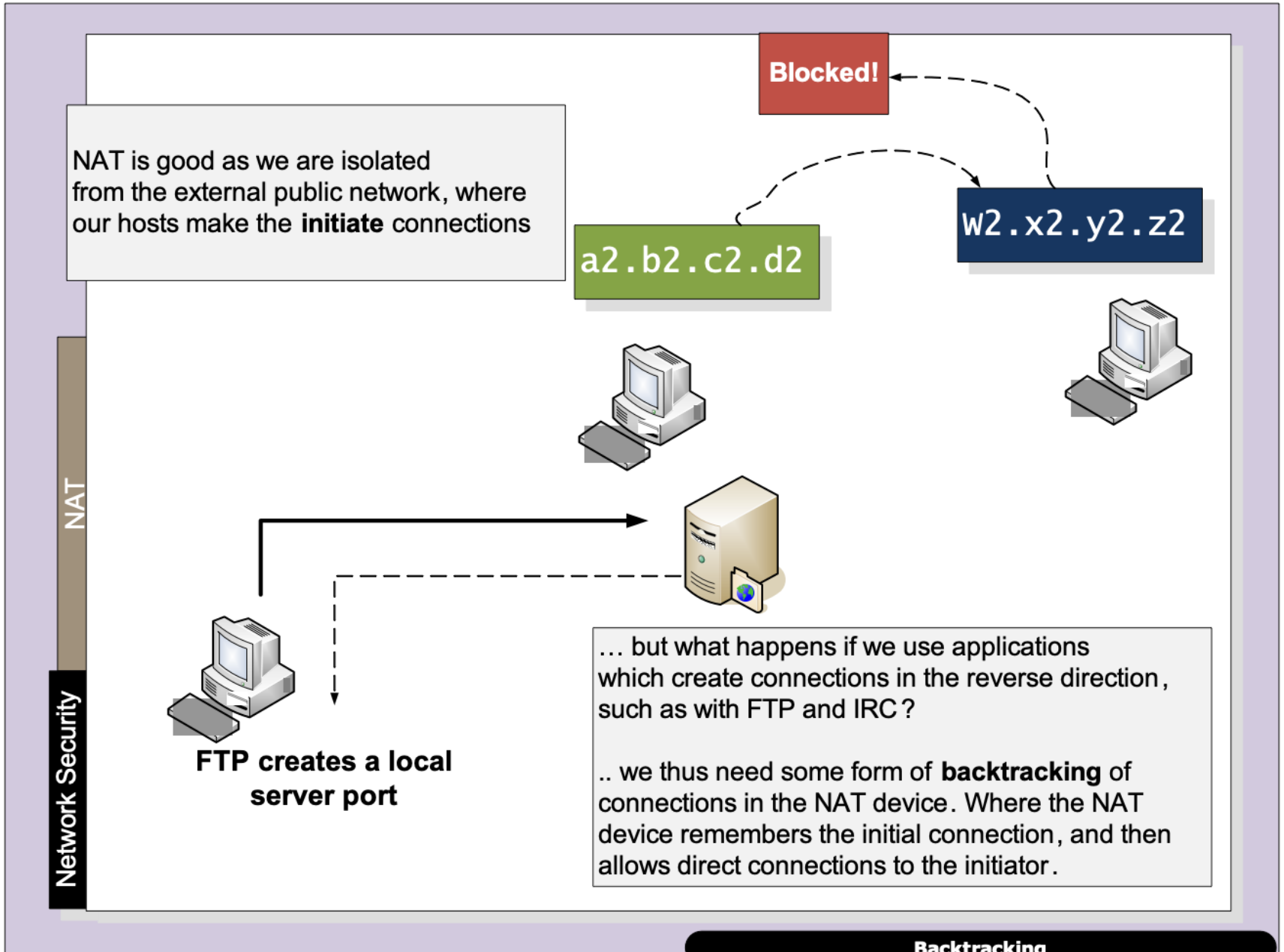
&cyber data

Layered Model



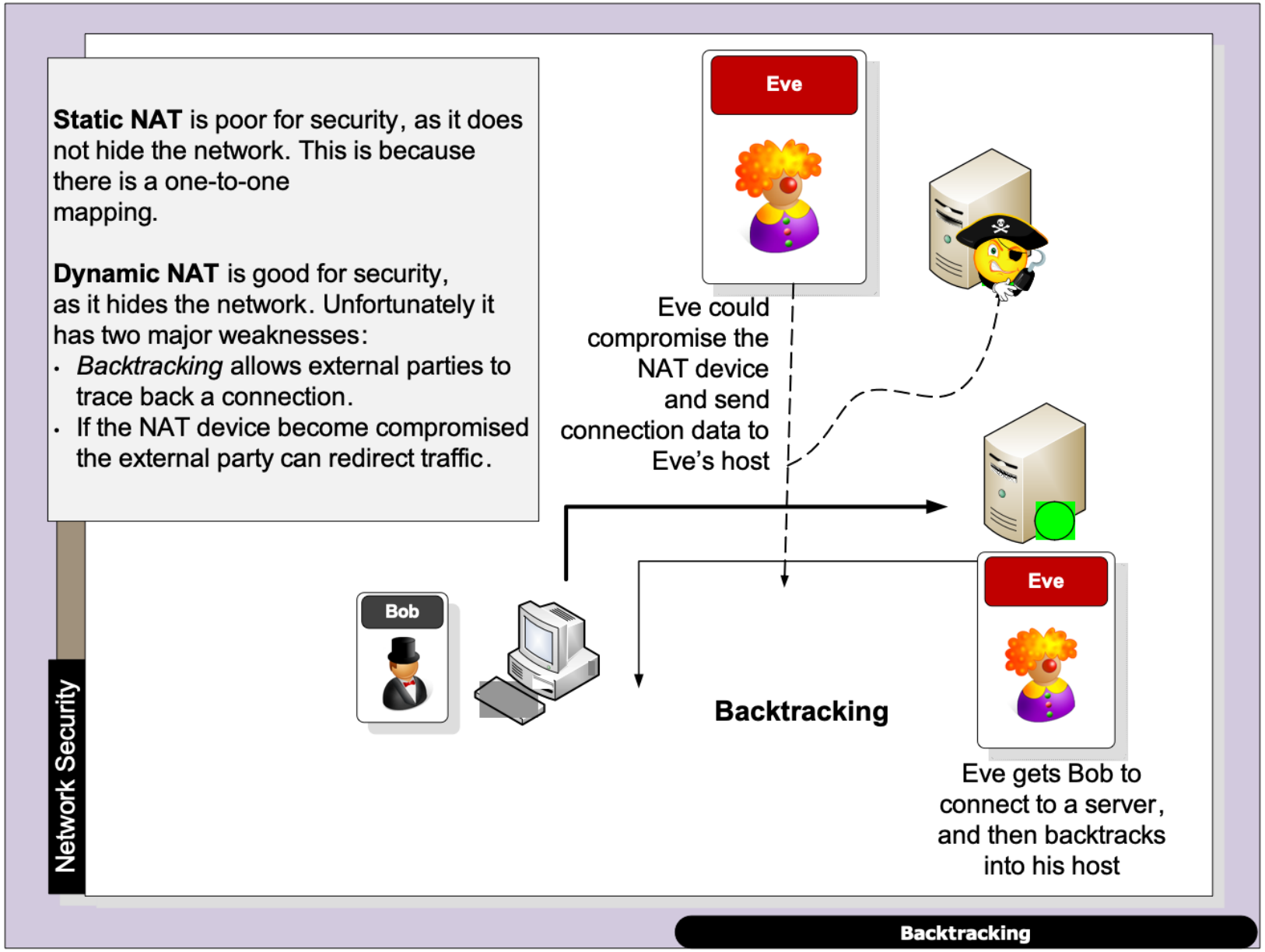
&cyber data

Layered Model



&cyber data

Layered Model



cyber & data

"From bits to information"

AI Threats and Opportunities

AI Threats

Attacking GenAI:

- Jailbreaks
- Reverse psychology
- Model escape
- Prompt injection.

Cyber Offense:

- Social engineering.
- Phishing emails
- Automated hacking
- Attack payload generation
- Malware code generation
- Polymorphic malware
- Reversing cryptography

Cyber Defence:

- Cyber Defence Automation.
- Cybersecurity Reporting.
- Threat Intelligence.
- Secure Code Generation and Detection.
- Developing Ethical guidelines
- Incident Response and Digital Forensics.
- Identification of Cyber attacks.
- Data set generation.

Social, Legal and Ethical:

- Pervasive role of ChatGPT
- Unauthorized access to conversations
- Personal information misuse
- Data ownership concerns
- Misuse by organisations
- Hallucinations

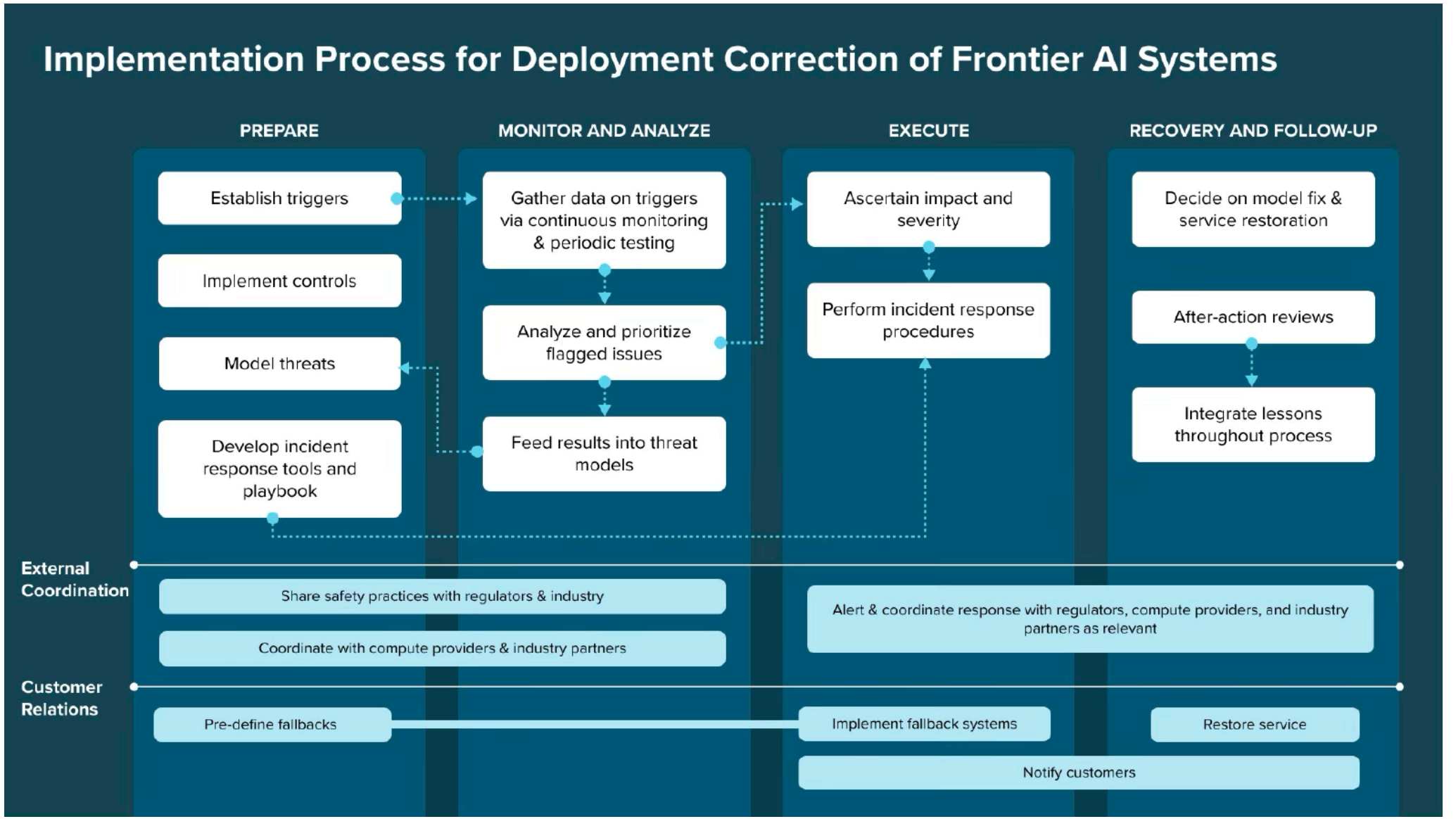
&cyber data

AI Threats

Drivers of cyber threat		Evidence	Potential impact
01. Vulnerability discovery	The deeper and more diverse the pool of vulnerabilities available to a threat actor, the more options they have for approaches, the lower the cost of creating exploits, and the lower the opportunity cost to execute a campaign.	High	Very high
02. Campaign planning and execution	Campaigns require the ability to specify and describe a target group, understand their technology usage, operational behaviours, security posture, and willingness to pay. Materials required for the execution of the campaign need to be created for the identified targets, taking time and resources for the threat actor.	High	High
03. Risk-reward analysis	All criminal activities which are not terrorism or war-like involve an assessment of risk and reward. Modifying the effectiveness of mechanisms for obtaining illicit gains or evading law enforcement can shift the equation in predictable ways.	Low	Low/Medium
04. Single points of failure	A fourth component underpinning the above three is the degree to which systems, services, technologies, and people are bound together (systemic coupling), giving rise to single points of failure. The greater the systemic coupling, the greater the unit-cost effectiveness of vulnerabilities, the larger the exposure footprint for any set of exploits, and the more extreme the risk-reward factors become. Examples of systemic coupling are cloud providers, DNS providers, and typically all services used by many businesses and provided by a small number of firms.	Low	Medium/High

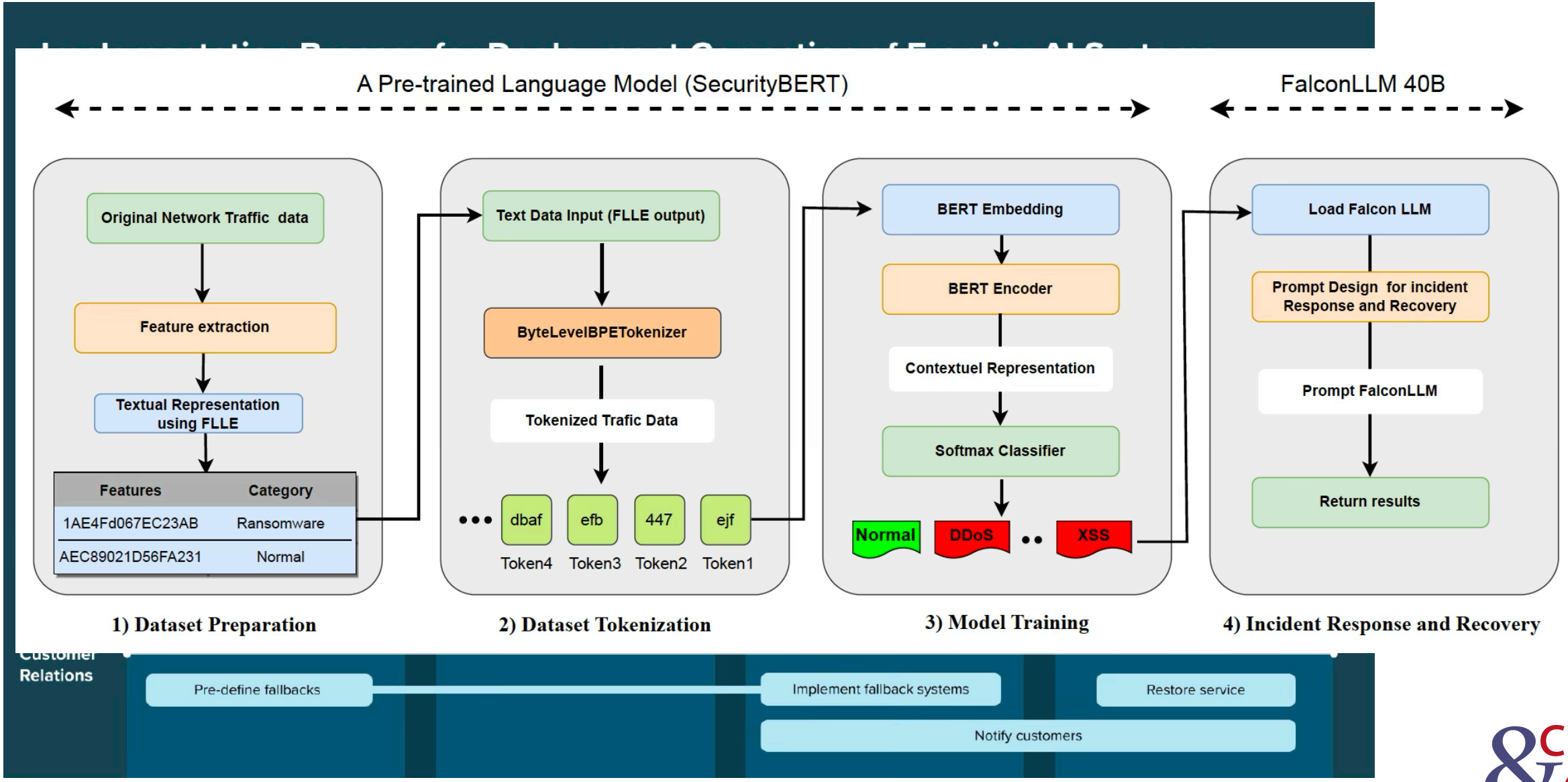
&cyber data

AI Security Frameworks



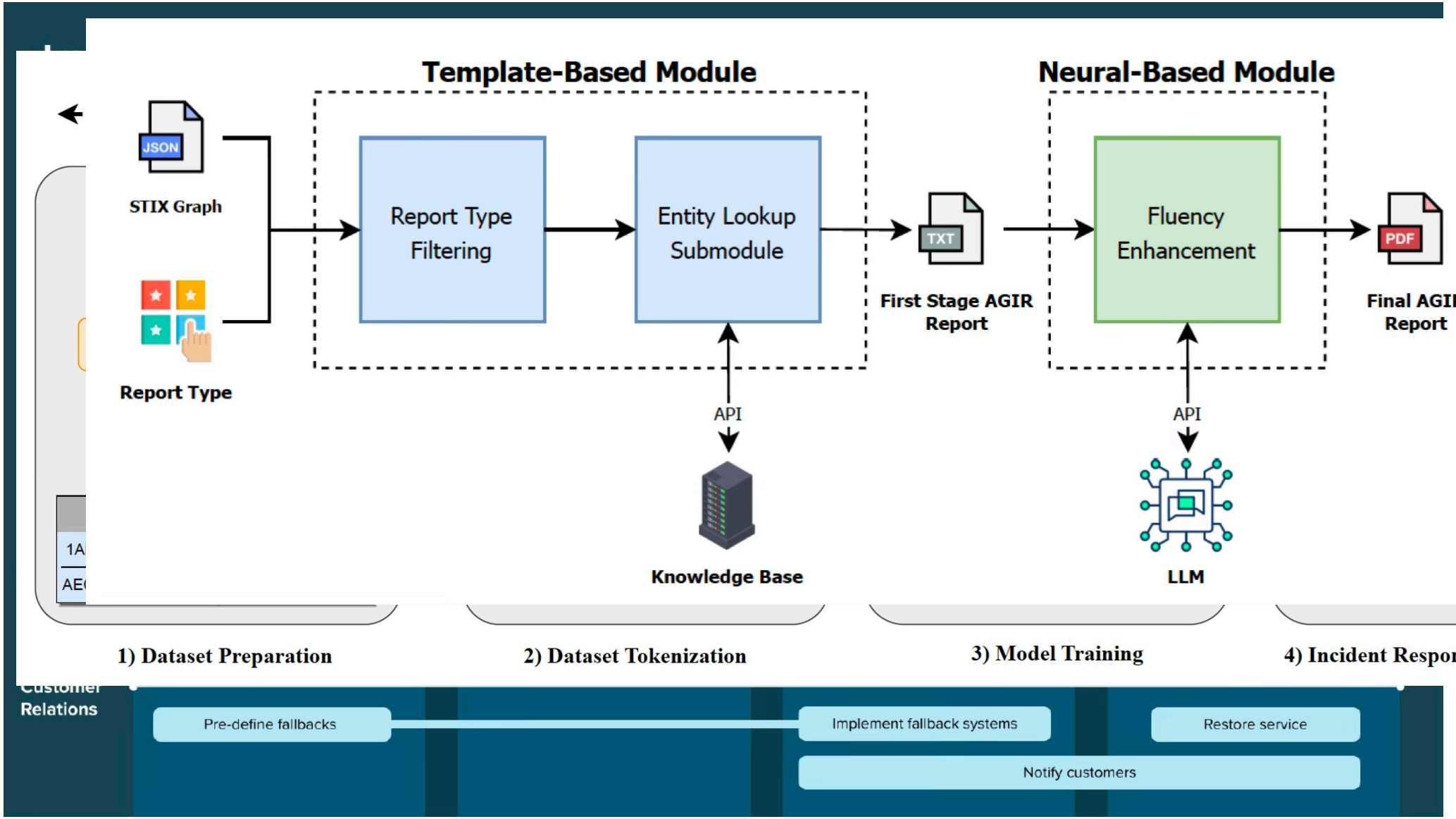
&cyber data

AI Security Frameworks

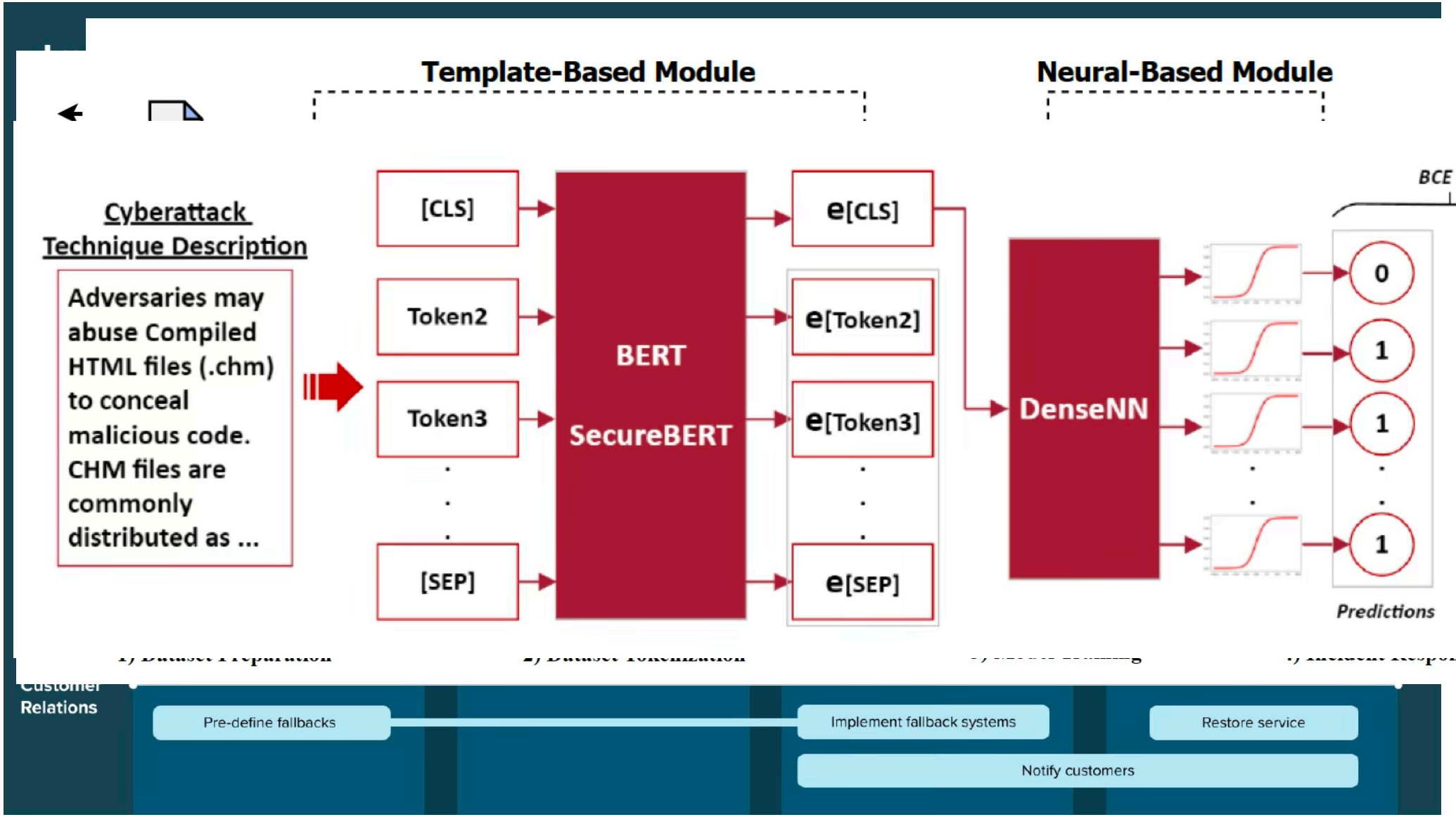


&cyber data

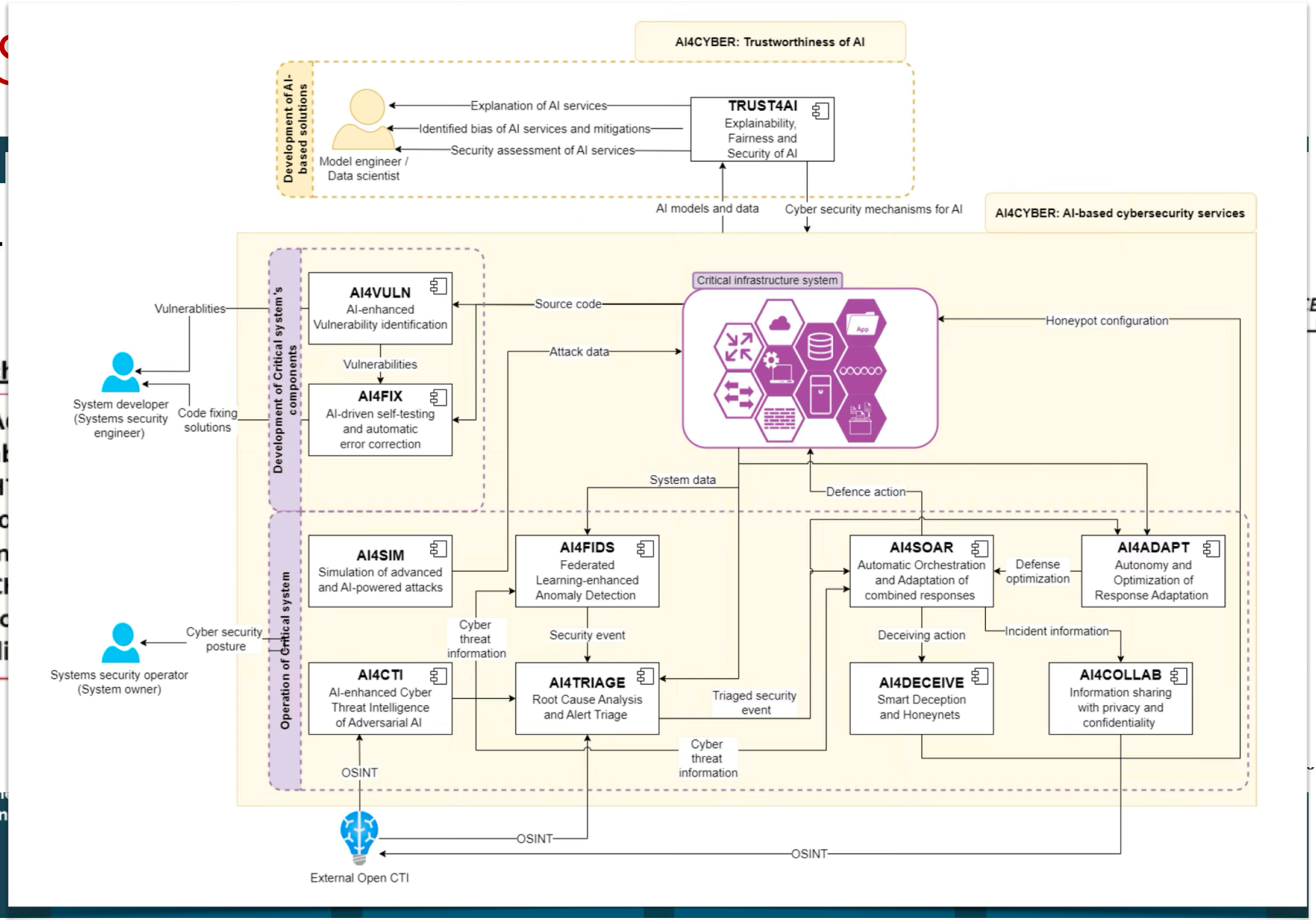
AI Security Frameworks



AI Security Frameworks

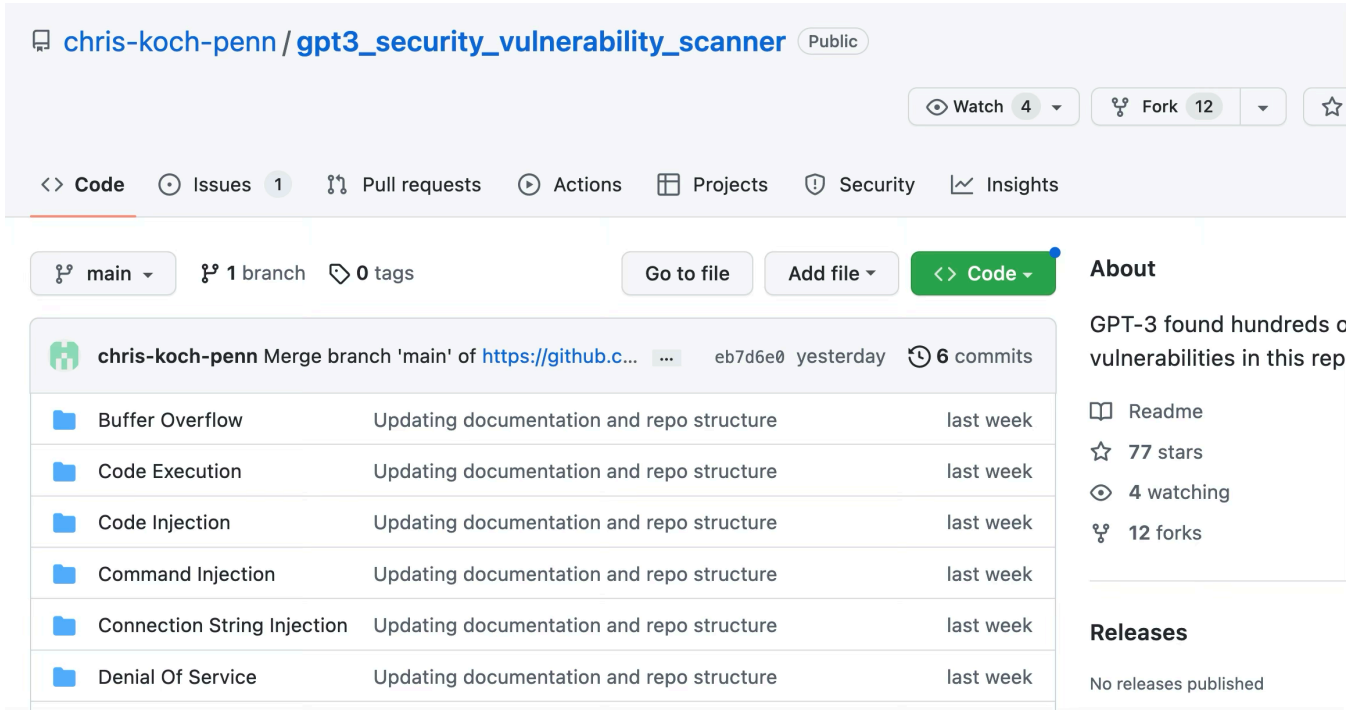


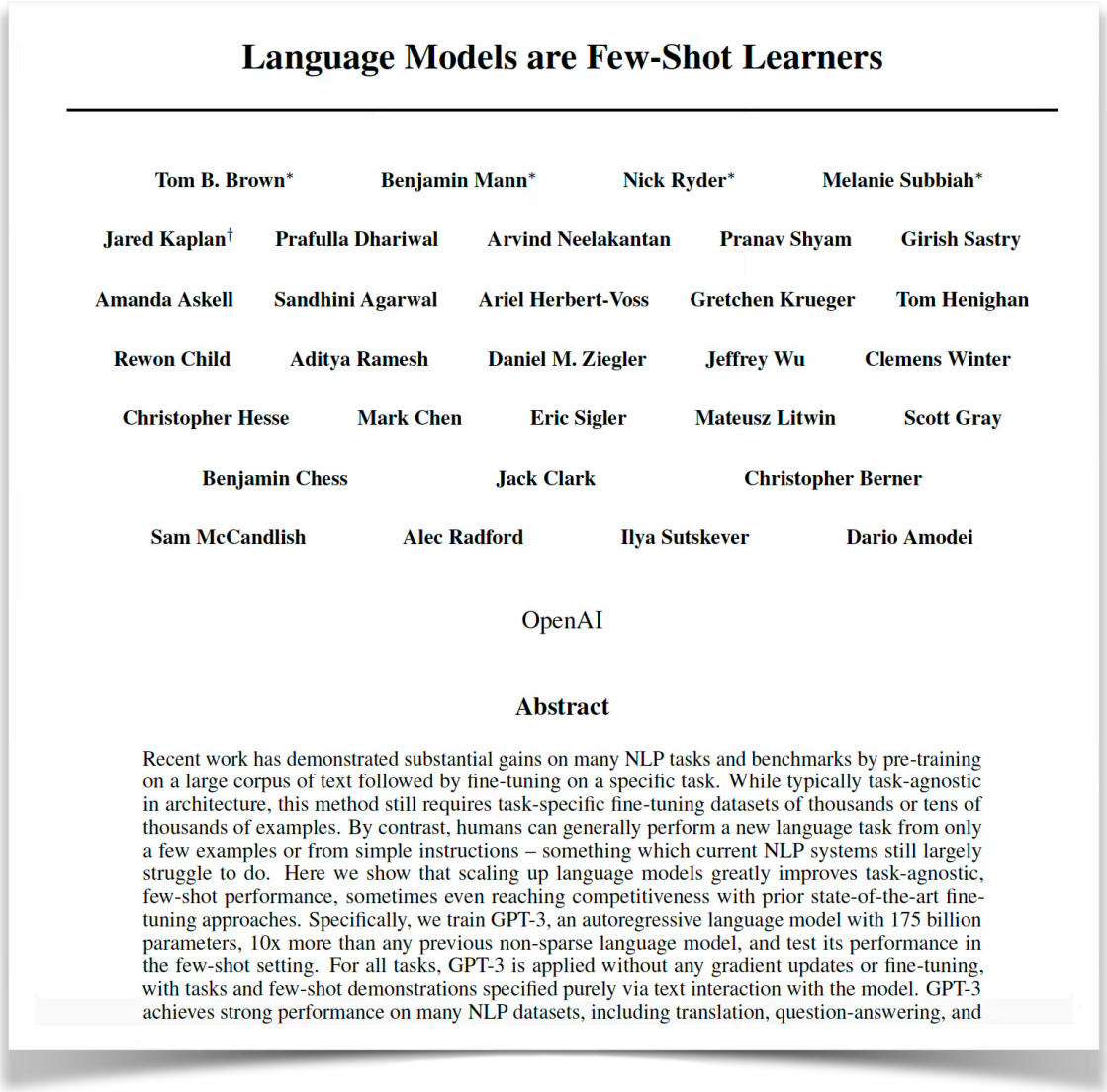
&cyber data


AI4CYBER: Trustworthiness of AI
Development of AI-based solutions
Model engineer / Data scientist
Explanation of AI services
Identified bias of AI services and mitigations
Security assessment of AI services
TRUST4AI
Explainability, Fairness and Security of AI
AI models and data
Cyber security mechanisms for AI
AI4CYBER: AI-based cybersecurity services
Development of Critical system's components
Vulnerablities
System developer (Systems security engineer)
Code fixing solutions
AI4VULN
AI-enhanced Vulnerability identification
Vulnerabilities
AI4FIX
AI-driven self-testing and automatic error correction
Source code
Attack data
Critical infrastructure system
Honeypot configuration
System data
Defence action
Operation of Critical system
Cyber security posture
Systems security operator (System owner)
AI4SIM
Simulation of advanced and AI-powered attacks
AI4FIDS
Federated Learning-enhanced Anomaly Detection
AI4SOAR
Automatic Orchestration and Adaptation of combined responses
Defense optimization
AI4ADAPT
Autonomy and Optimization of Response Adaptation
Cyber threat information
Security event
Deceiving action
Incident information
AI4CTI
AI-enhanced Cyber Threat Intelligence of Adversarial AI
AI4TRIAGE
Root Cause Analysis and Alert Triage
Triaged security event
AI4DECEIVE
Smart Deception and Honeynets
AI4COLLAB
Information sharing with privacy and confidentiality
Cyber threat information
OSINT
OSINT
OSINT
External Open CTI

Bug Detection

GPT-3 found 213 security vulnerabilities. One of the better commercial tools on the market found only found 99 issues - although their tool provides context in a more structured format. After manually reviewing a random sample of 50 / 213 of the vulnerabilities detected by GPT-3, only one was a false positive. Both tools had many false negatives.





Language Models are Few-Shot Learners

Tom B. Brown* Benjamin Mann* Nick Ryder* Melanie Subbiah*

Jared Kaplan† Prafulla Dhariwal Arvind Neelakantan Pranav Shyam Girish Sastry

Amanda Askell Sandhini Agarwal Ariel Herbert-Voss Gretchen Krueger Tom Henighan

Rewon Child Aditya Ramesh Daniel M. Ziegler Jeffrey Wu Clemens Winter

Christopher Hesse Mark Chen Eric Sigler Mateusz Litwin Scott Gray

Benjamin Chess Jack Clark Christopher Berner

Sam McCandlish Alec Radford Ilya Sutskever Dario Amodei

OpenAI

Abstract

Recent work has demonstrated substantial gains on many NLP tasks and benchmarks by pre-training on a large corpus of text followed by fine-tuning on a specific task. While typically task-agnostic in architecture, this method still requires task-specific fine-tuning datasets of thousands or tens of thousands of examples. By contrast, humans can generally perform a new language task from only a few examples or from simple instructions – something which current NLP systems still largely struggle to do. Here we show that scaling up language models greatly improves task-agnostic, few-shot performance, sometimes even reaching competitiveness with prior state-of-the-art fine-tuning approaches. Specifically, we train GPT-3, an autoregressive language model with 175 billion parameters, 10x more than any previous non-sparse language model, and test its performance in the few-shot setting. For all tasks, GPT-3 is applied without any gradient updates or fine-tuning, with tasks and few-shot demonstrations specified purely via text interaction with the model. GPT-3 achieves strong performance on many NLP datasets, including translation, question-answering, and

&cyber data

cyber & data

"From bits to information"

Defence Systems, Policies and Risks