FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS YARSI

presentation

CYBER SECURITY OUTLOOK

Presented by Iswandi

UNIVERSITAS YARSI

Jakarta, 15 Agustus 2020

What is Cyber Security ?

Cyber Security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Source : https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

What is Cyber Security ?

Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Information security protects the integrity and privacy of data, both in storage and in transit.

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Source : https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

The Cyber Threats Spectrum

Figure The Cyber Threat Spectrum (source: FBI Cyber Division)

The Cyber Information Security Primary Focus

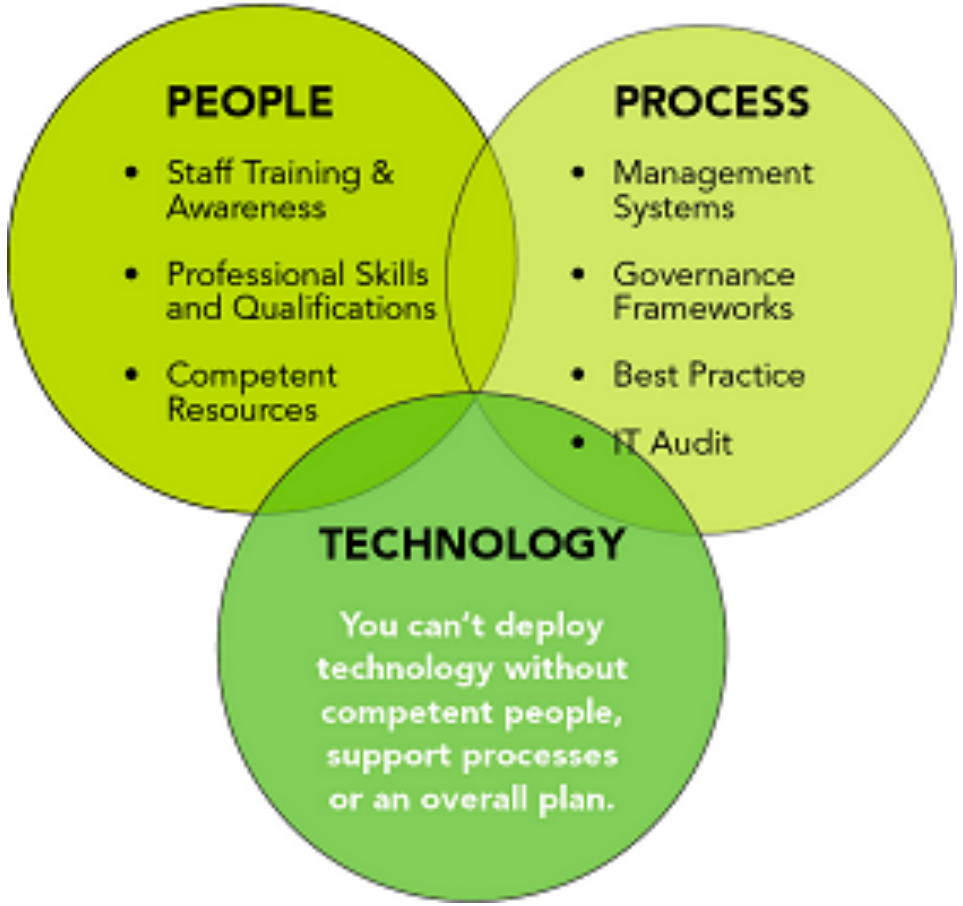
Confidentiality is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner.

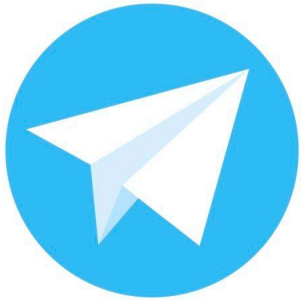
Availability for any information system to serve its purpose, the information must be available when it is needed.

Source : https://en.wikipedia.org/wiki/Information_security

Process in IT Security



Threat Landscape



Apple Store

Play Store

User Behavior

Contacts

Chatting

Email messages

Documents

Personal Information

Social Networking

Browsing

Media files

User Behavior

Personal Information

Social Networking

Browsing

Media files

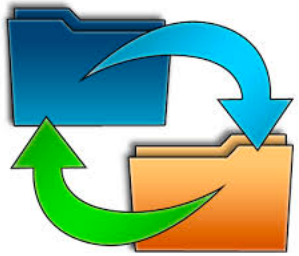
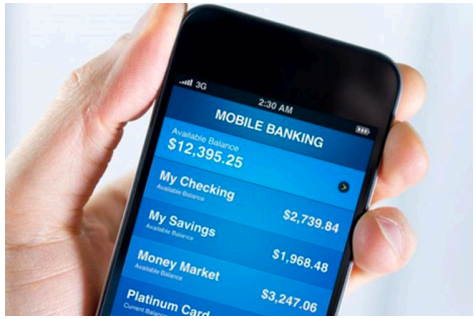
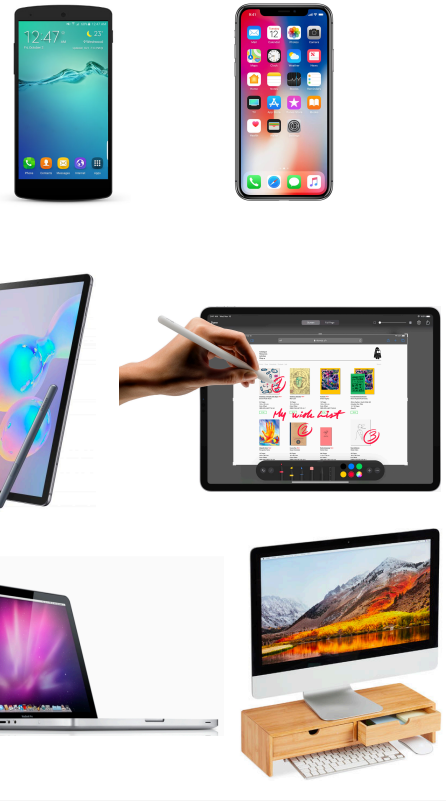
Contacts

Chatting

Email messages

Documents

Identification of assets

Information Assets	Software Assets	Physical Assets	Services
 Database : - customers - personnel - production - sales - marketing - finances  Data files	 Application software System software		- Computing services - Communication services - Environmental conditioning services

IoT Ecosystem

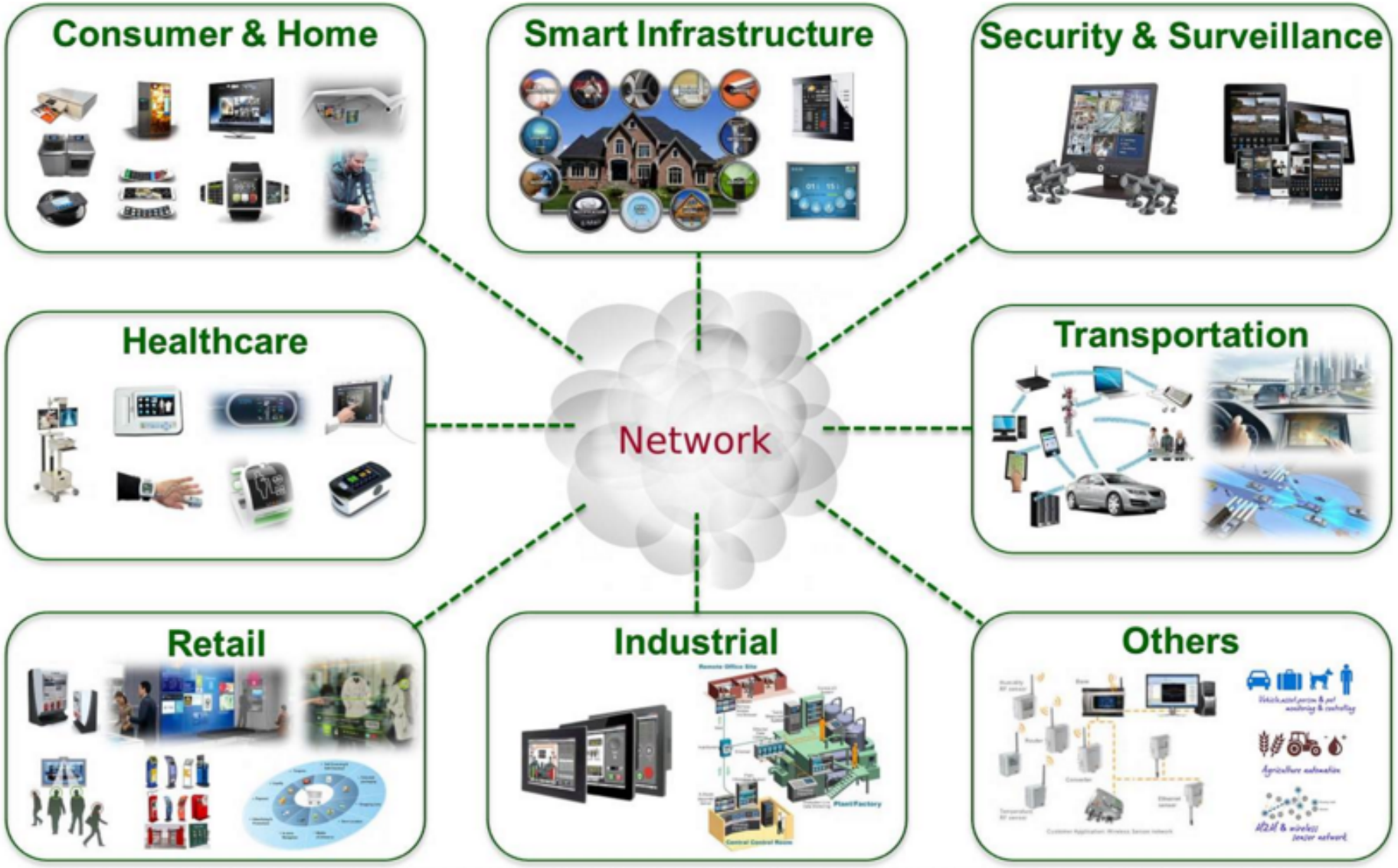


Image Courtesy of https://bensontao.files.wordpress.com/2013/10/vivante-iot-ecosystem.jpg

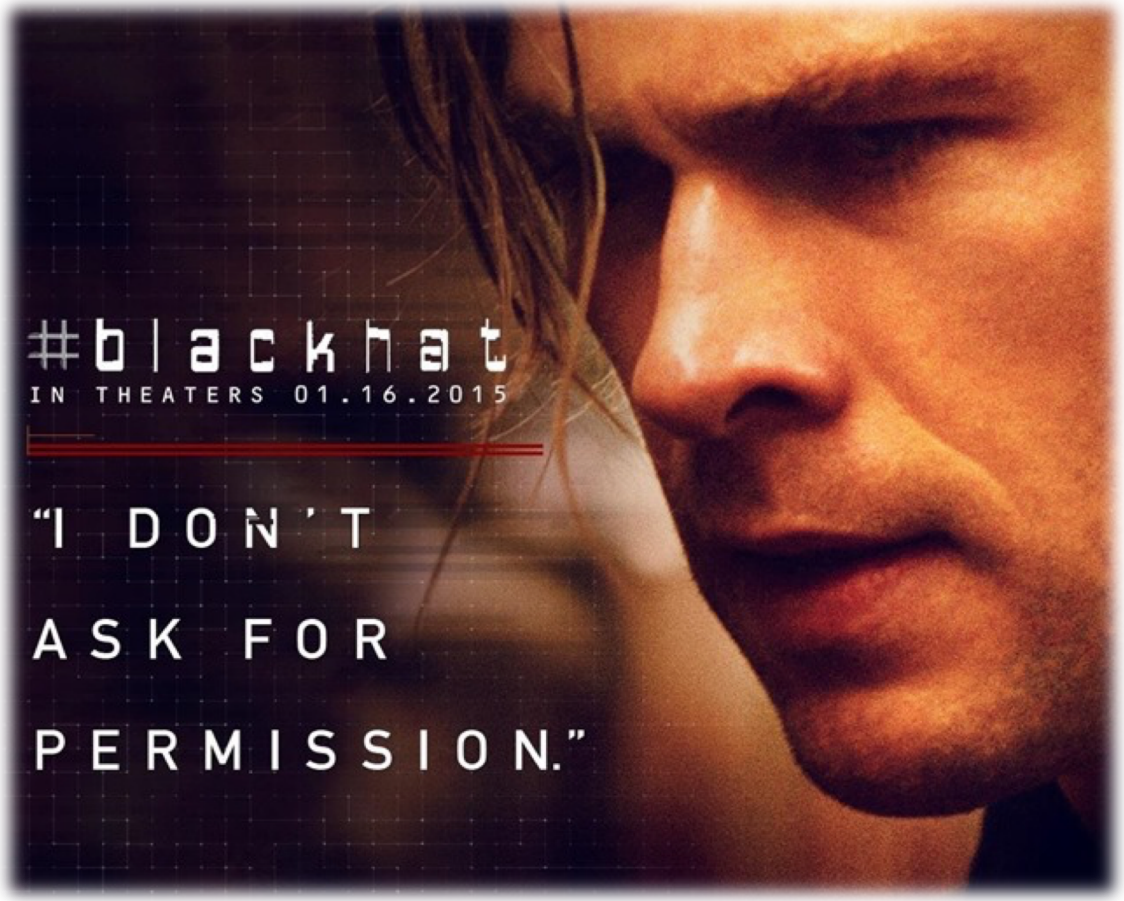
Is the Internet of Things safe ?

Cyber Threats

UNIVERSITAS YARSI

Backdoors	Backdoors allow remote access to computers or systems without users' knowledge.
Cryptojacking	Cryptojacking is the malicious installation of cryptocurrency mining – or 'cryptomining' – software. This software illicitly harnesses the victim's processing power to mine for cryptocurrency.
DDoS attacks	DDoS (distributed denial-of-service) attacks attempt to disrupt normal web traffic and take targeted websites offline by flooding systems, servers or networks with more requests than they can handle, causing them to crash.
DNS poisoning attacks	DNS (domain name system) poisoning attacks compromise DNS to redirect traffic to malicious sites. Affected sites are not 'hacked' themselves.
Formjacking	Formjacking is the process of inserting malicious JavaScript code into online payment forms in order to harvest customers' card details.
Malware	Malware is a broad term used to describe any file or program that is intended to harm or disrupt a computer.
MITM attacks	An MITM (man-in-the-middle) attack occurs when a hacker inserts themselves between a device and a server to intercept communications that can then be read and/or altered.
Phishing attacks	Phishing is a method of social engineering used to trick people into divulging sensitive or confidential information, often via email.
Social engineering	Social engineering is used to deceive and manipulate victims in order to obtain information or gain access to their computer.
SQL injection	A SQL (Structured Query Language) injection occurs when an attacker inserts malicious code into a server that uses SQL. SQL injections are only successful when a security vulnerability exists in an application's software. Successful SQL attacks will force a server to provide access to or modify data.
APT	APTs involve groups of attackers often working with governments and commercial entities.

Advanced Persistent Threats (APT)



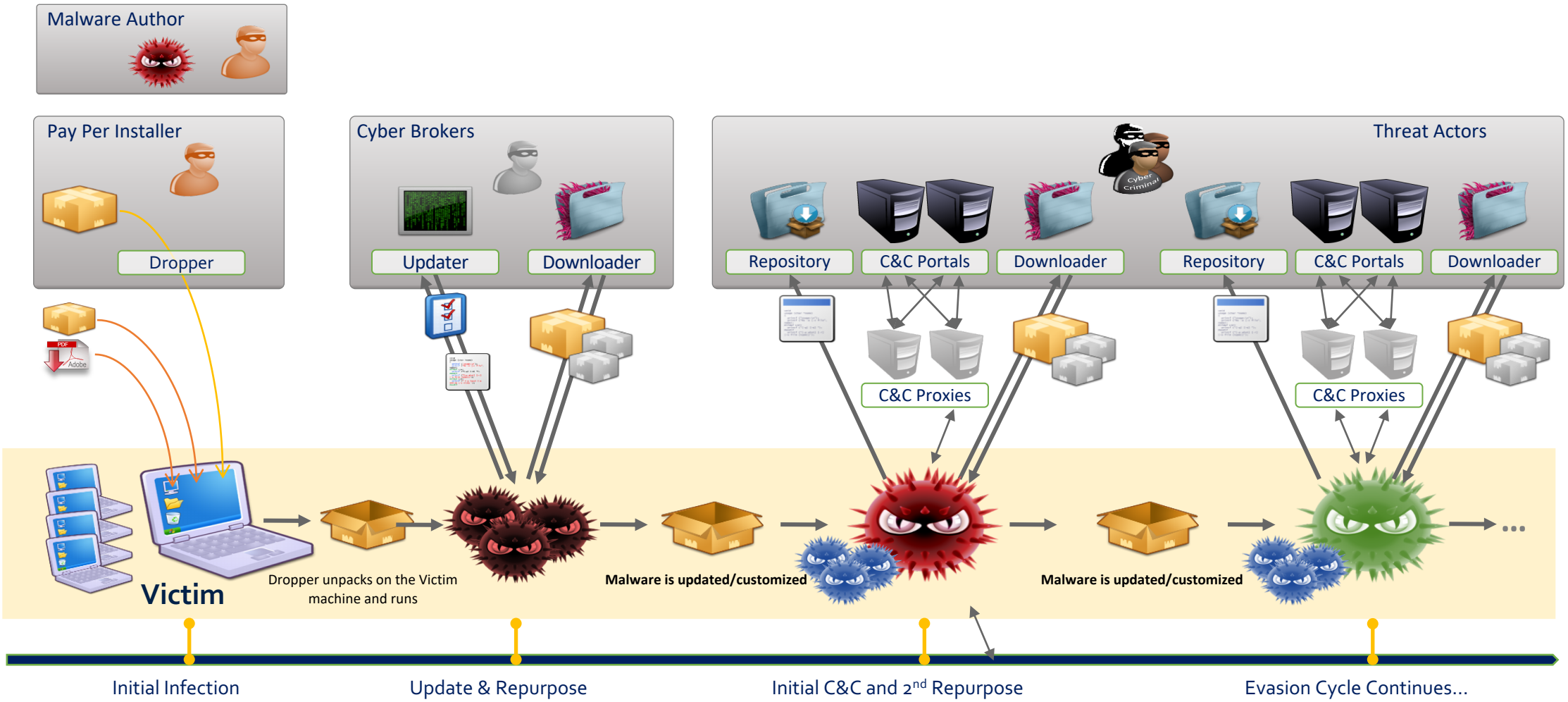
Advanced: APTs involve groups of attackers often working with governments and commercial entities. These groups are able to combine multiple targeting methods with a range of tools, technologies and techniques to reach, compromise, and maintain access to a target. Such groups usually have advanced technology skills, state protection, and a wide range of channels through which they can mount their attacks.

Persistent: APTs use a 'low and slow' approach, rather than a barrage of constant attacks and malware updates. The long-term access to a target provided by an APTs can be far more beneficial to the attacker, so remaining undetected is crucial to success.

Threat: APTs require attackers who are skilled, motivated, organised and well-funded. They are executed by coordinated humans, rather than by mindless and automated pieces of code.

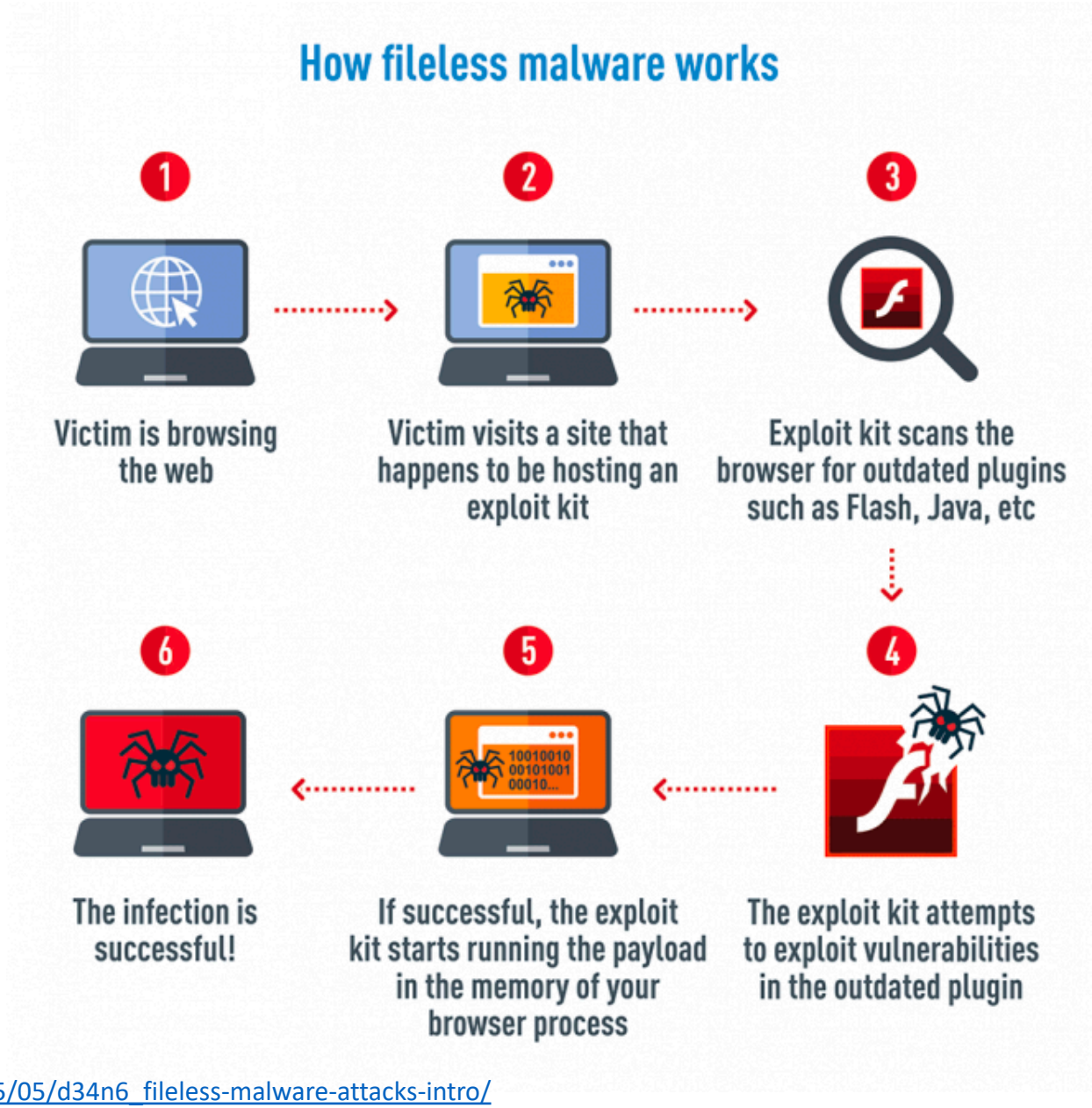
Source : https://www.itgovernance.co.uk/advanced-persistent-threats-apt

APT Life Cycle



Source: Core Security

APT Life Cycle



Source: https://d3pakblog.wordpress.com/2018/05/05/d34n6_fileless-malware-attacks-intro/

APT Case

On **December 23, 2015**, the **Ukrainian Kyivoblenergo**,
The outages were due to a third party's illegal entry into the company's computer and SCADA systems

Source: E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf (www.eisac.com)

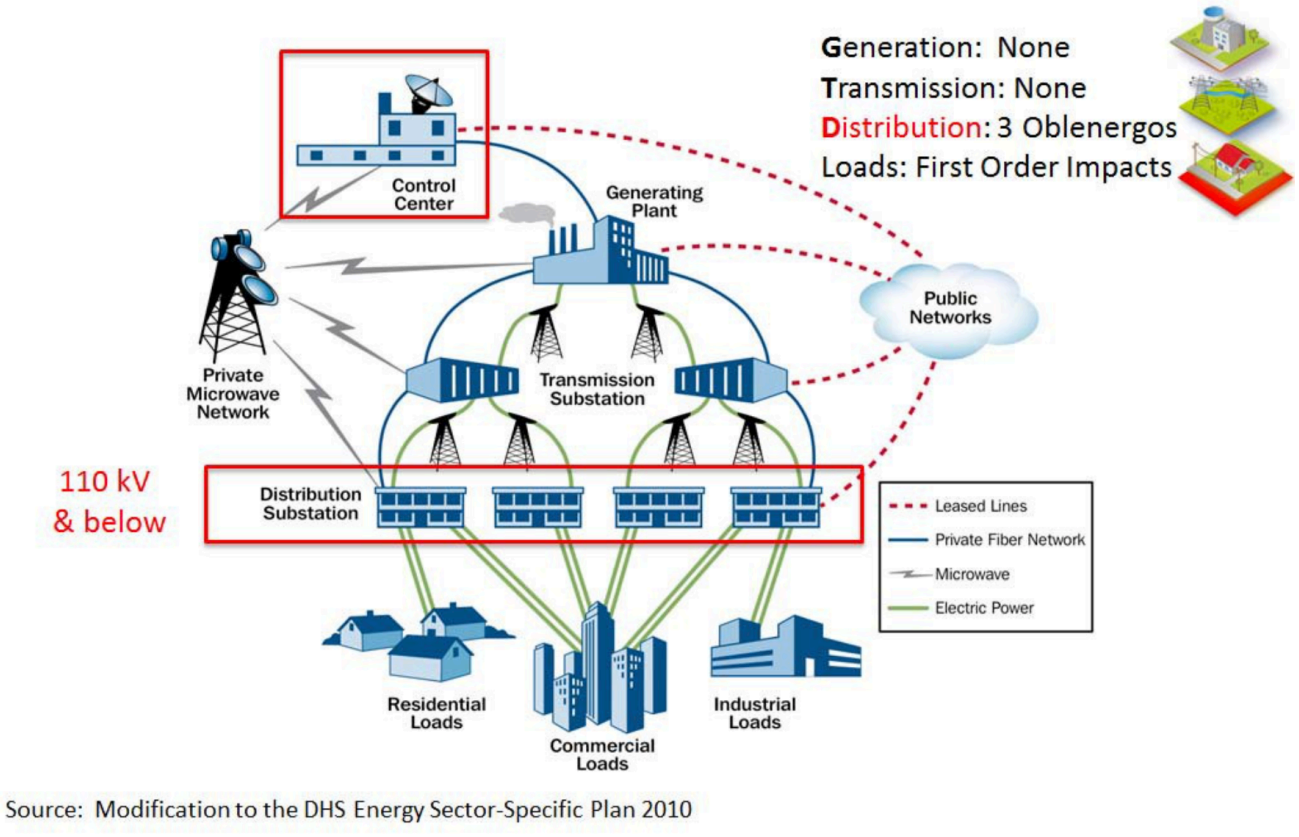
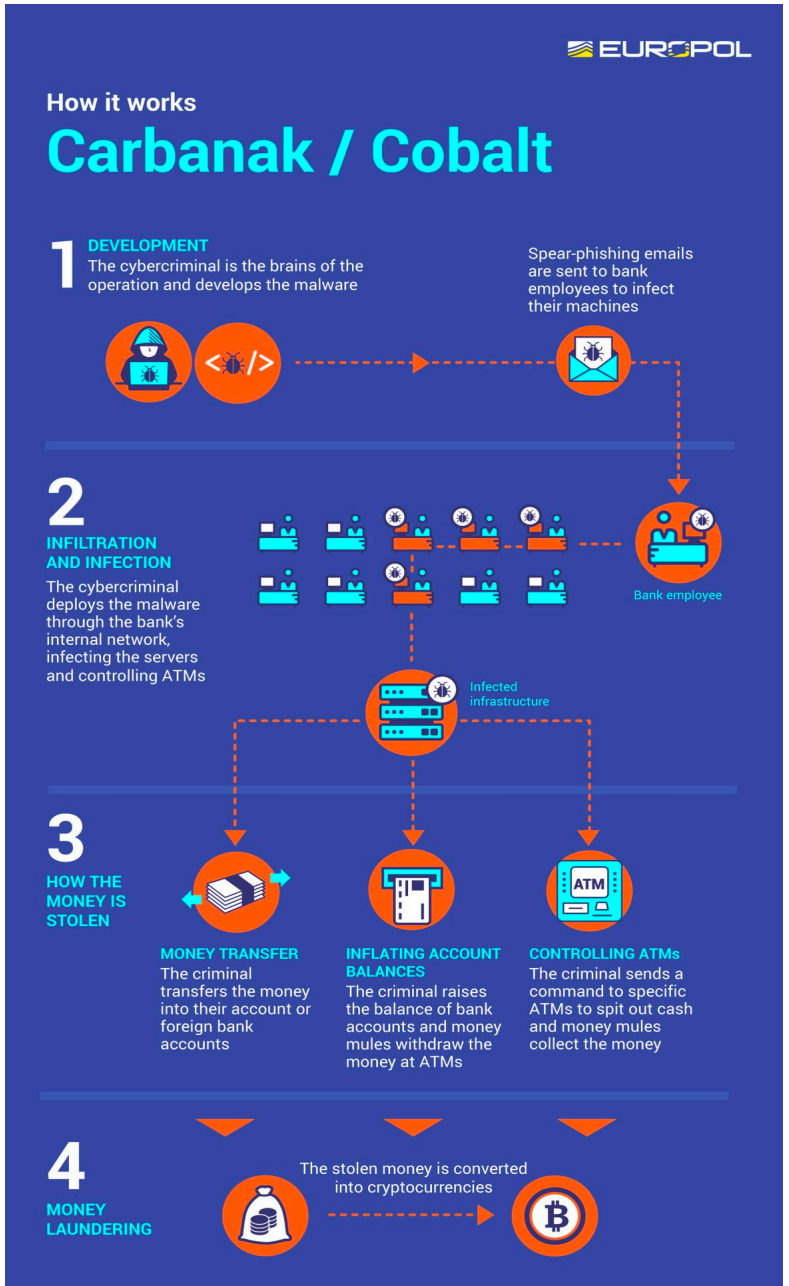
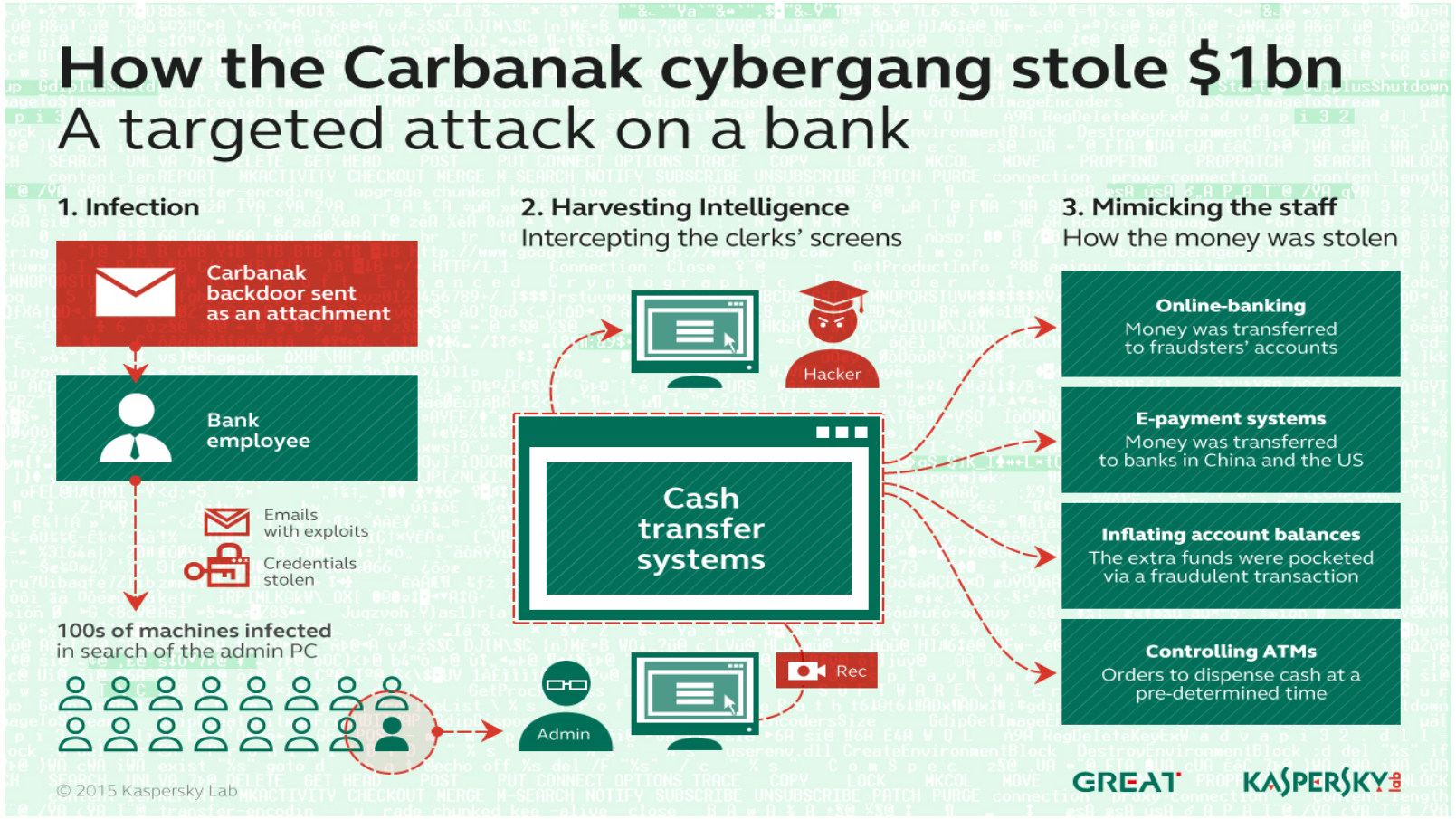


Figure 1: Electric System Overview

APT Case-Carbanak Malware





Source : https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

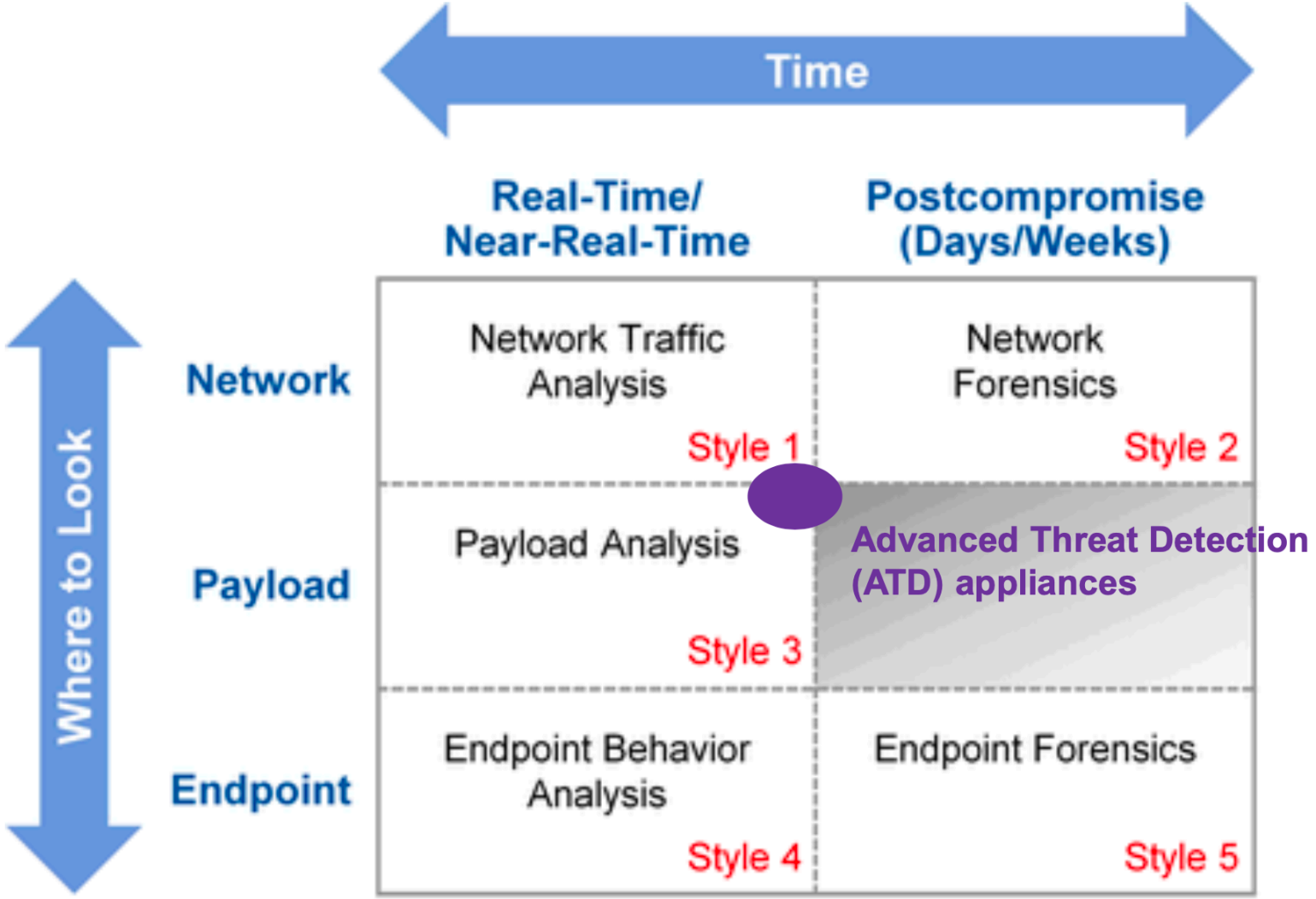
Source : https://www.europol.europa.eu/publications-documents/carbanak/cobalt-infographic

How we can protect from Cyber Threats?

Problem & Challenges

- Engines - Signatures Can’t Keep Up
- Need more time to develop signatures
- Must define the rule
- Humans are Required
- Can't detect the latest threat.

Five Styles of Advanced Threat Defense



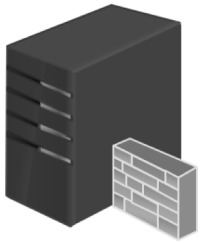
Source : Gartner (August 2013)

Perkembangan Prevention and Detection Tools

Traditional Anti Virus

Traditional Firewall

IPS/IDS



Proxy

Anti Spam

SIEM

NextGen
Anti Virus & EDR

NextGen
Firewall

NextGen
IPS/IDS

Advance
Threat Detection

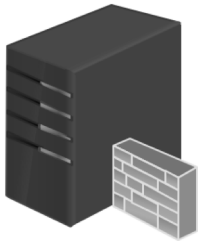
NextGen
SIEM

Perkembangan Prevention and Detection Tools

Traditional Anti Virus

Traditional Firewall

IPS/IDS



Proxy

Anti Spam

SIEM

NextGen
Anti Virus & EDR

NextGen
Firewall

NextGen
IPS/IDS

Advance
Threat Detection

NextGen
SIEM

XDR (Extended Detection and Response)

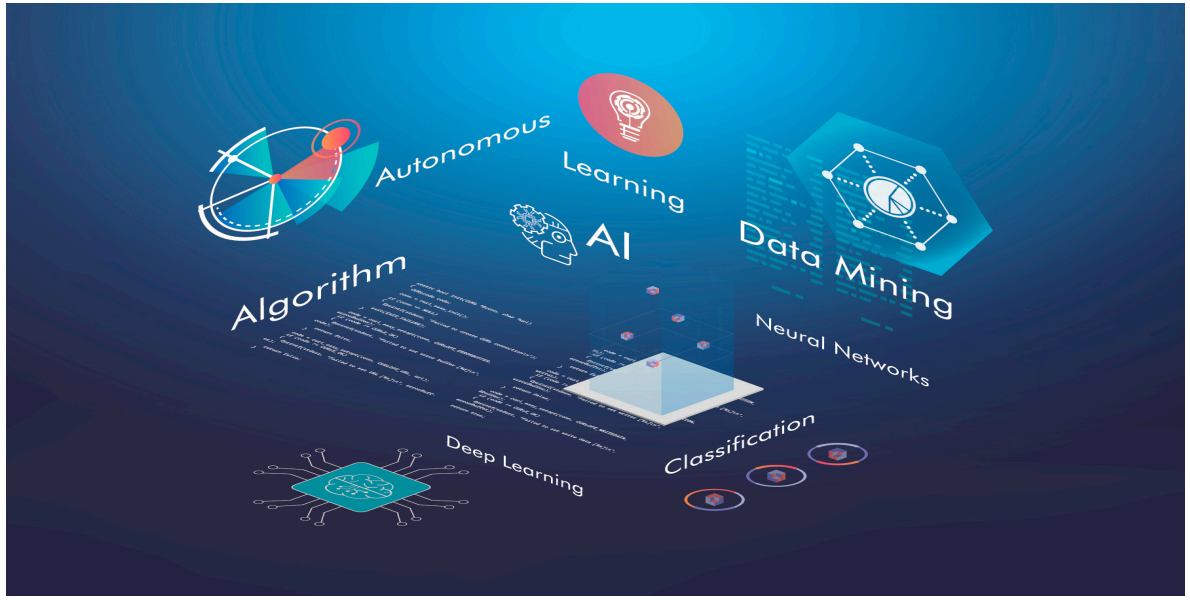
MDR (Managed Detection and Response)

XDR (Extended Detection and Response)

UNIVERSITAS YARSI

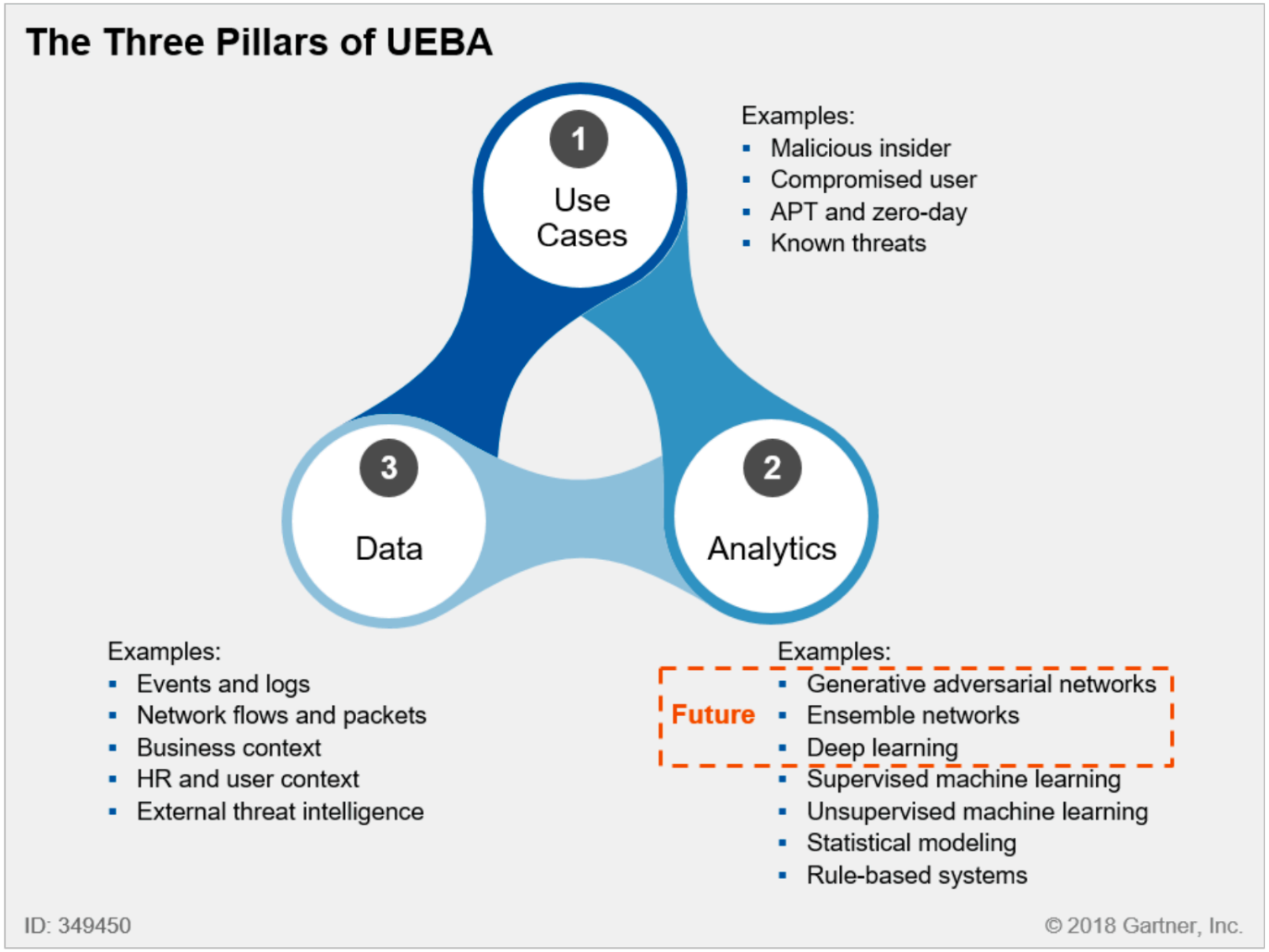
- Network Detection & Response (**NDR**)
- Automated Threat-Hunting (**ATH**)
- User Entity Behavior Analytics (**UEBA**)
- Cloud Detection & Response (**CDR**)
- Firewall Traffic Analysis (**FTA**)
- Next Gen SIEM
- Sandbox, etc…

Source: Stellar Cyber



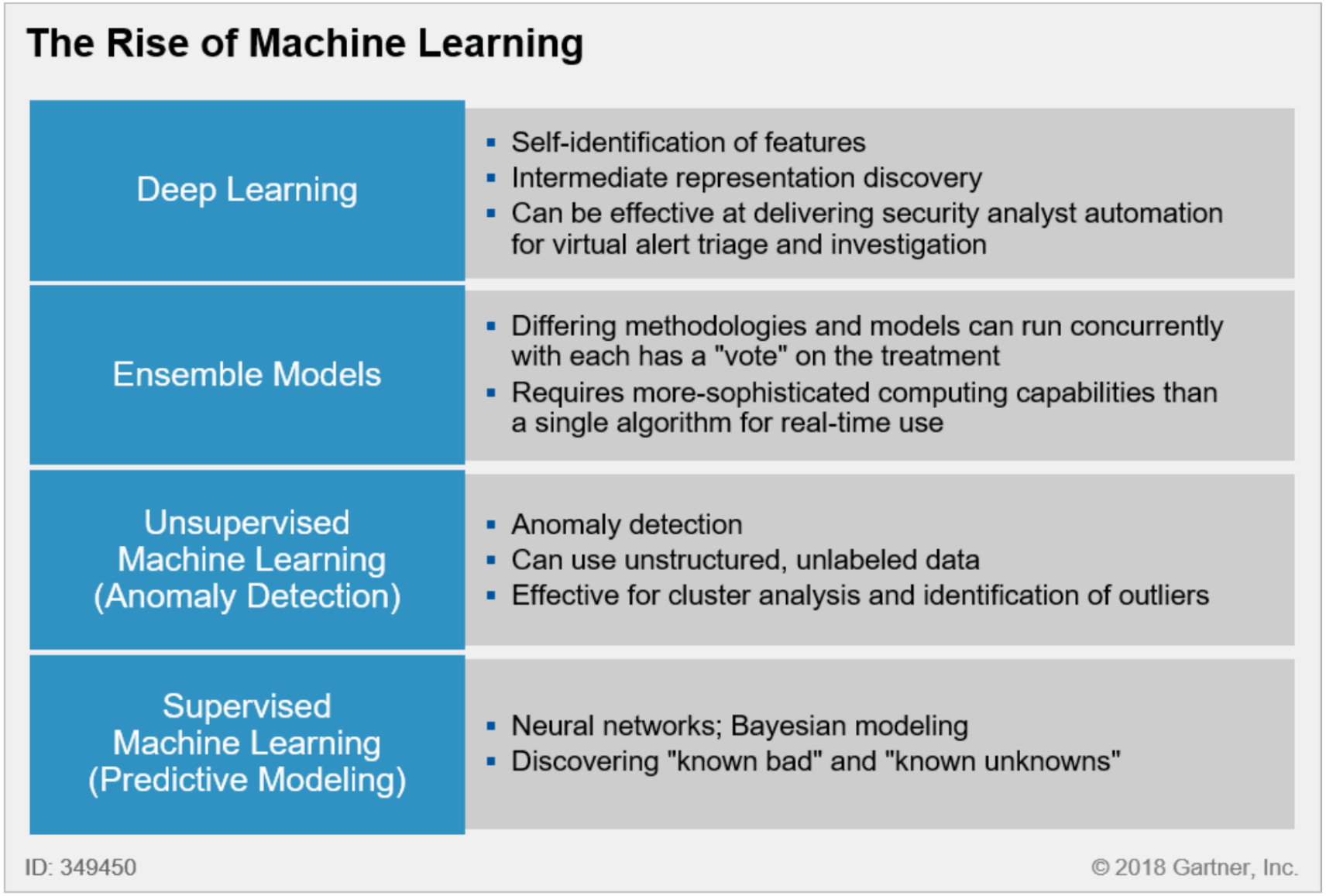
POWERED BY AI

The Three Pillars of UEBA



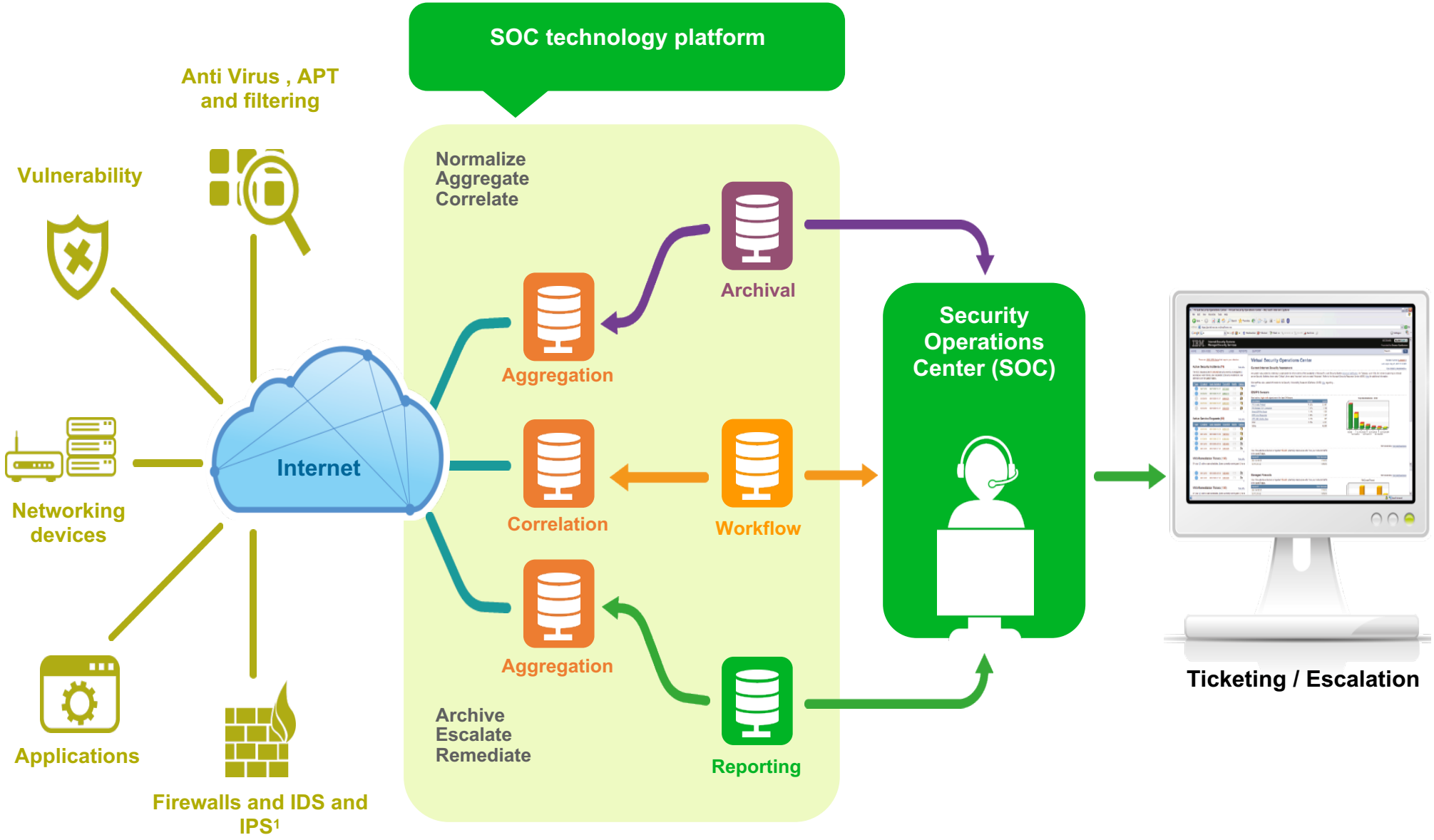
Source: Gartner (April 2018)

The Rise of Machine Learning



Source: Gartner (April 2018)

Security Operation Center/MDR Overview



SOC is like a car dashboard

SEIN Kiri

SEIN Kanan

Bahan Bakar

SUHU MESIN

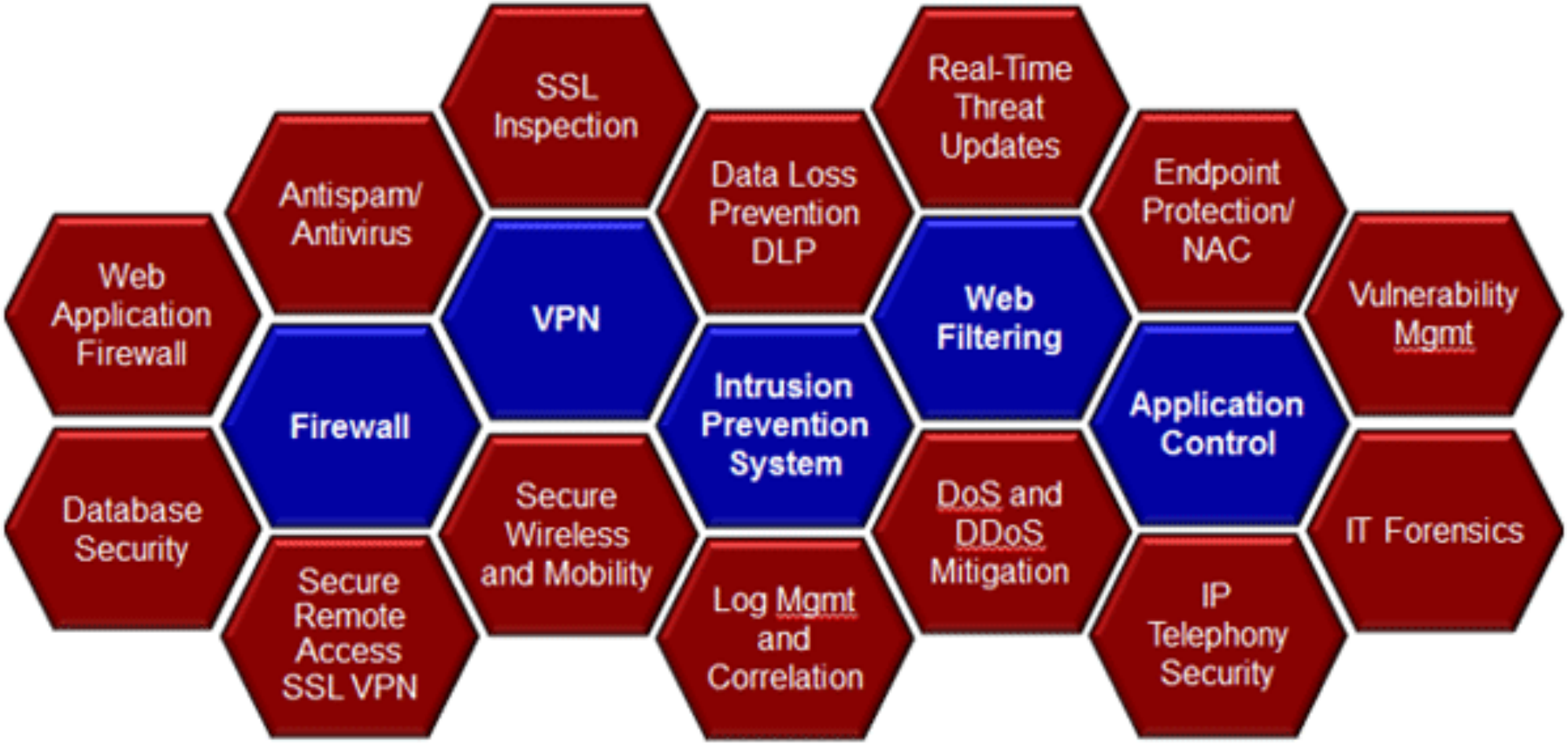
Kecepatan

SOC Room

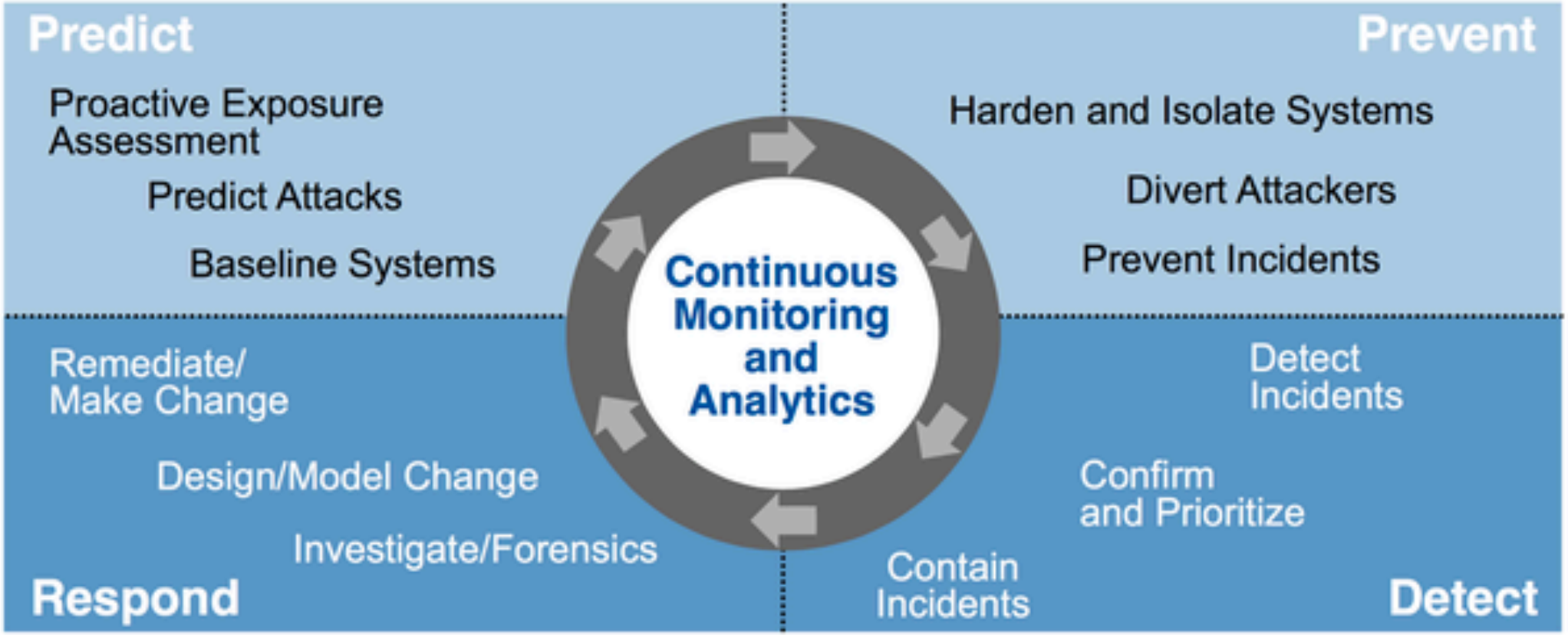
Source : https://www.bkav.com/en/top-news/-/view-content/78200/thai-binh-province-officially-opened-the-security-operations-center-soc

Why do we need SOC ?

UNIVERSITAS YARSI



The Adaptive Security Architecture



Source: Gartner (February 2014)

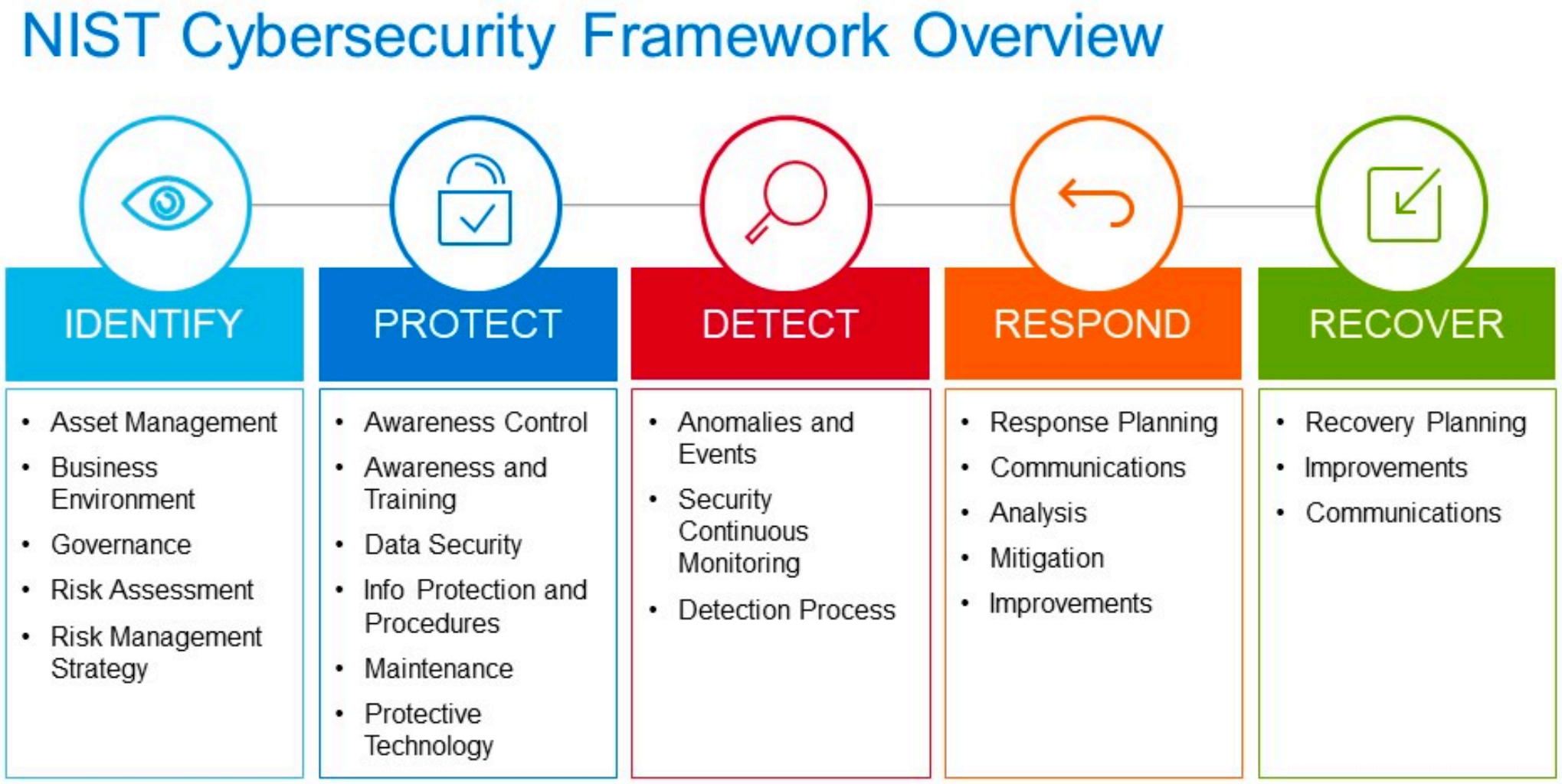
Top 4 Cyber Security Frameworks

The most frequently adopted frameworks should come as no surprise to security practitioners:

1. PCI DSS (47%)
2. ISO 27001/27002 (35%)
3. CIS Critical Security Controls (32%)
4. NIST Framework for Improving Critical Infrastructure Security (29%)

Source : https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks

IT Security Framework



Source : https://infocus.dellemc.com/michael_dulavitz/strengthen-security-of-your-data-center-with-the-nist-cybersecurity-framework/strengthen-security-with-nist-cybersecurity-framework-fig2/#main

Terima Kasih