

**FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS YARSI**

presentation

CYBER SECURITY OUTLOOK

Presented by Iswandi



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.



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.



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

The Cyber Information Security Primary Focus



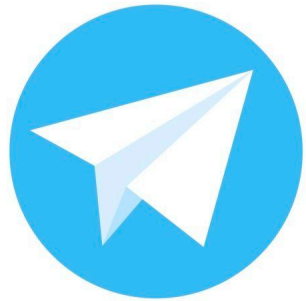
Confidentiality is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.

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.



Threat Landscape



Apple Store

Play Store





Personal Information

Social Networking

Browsing

Media files



Contacts

Chatting

Email messages

Documents



Personal Information

Social Networking

Browsing

Media files

Contacts

Chatting

Email messages

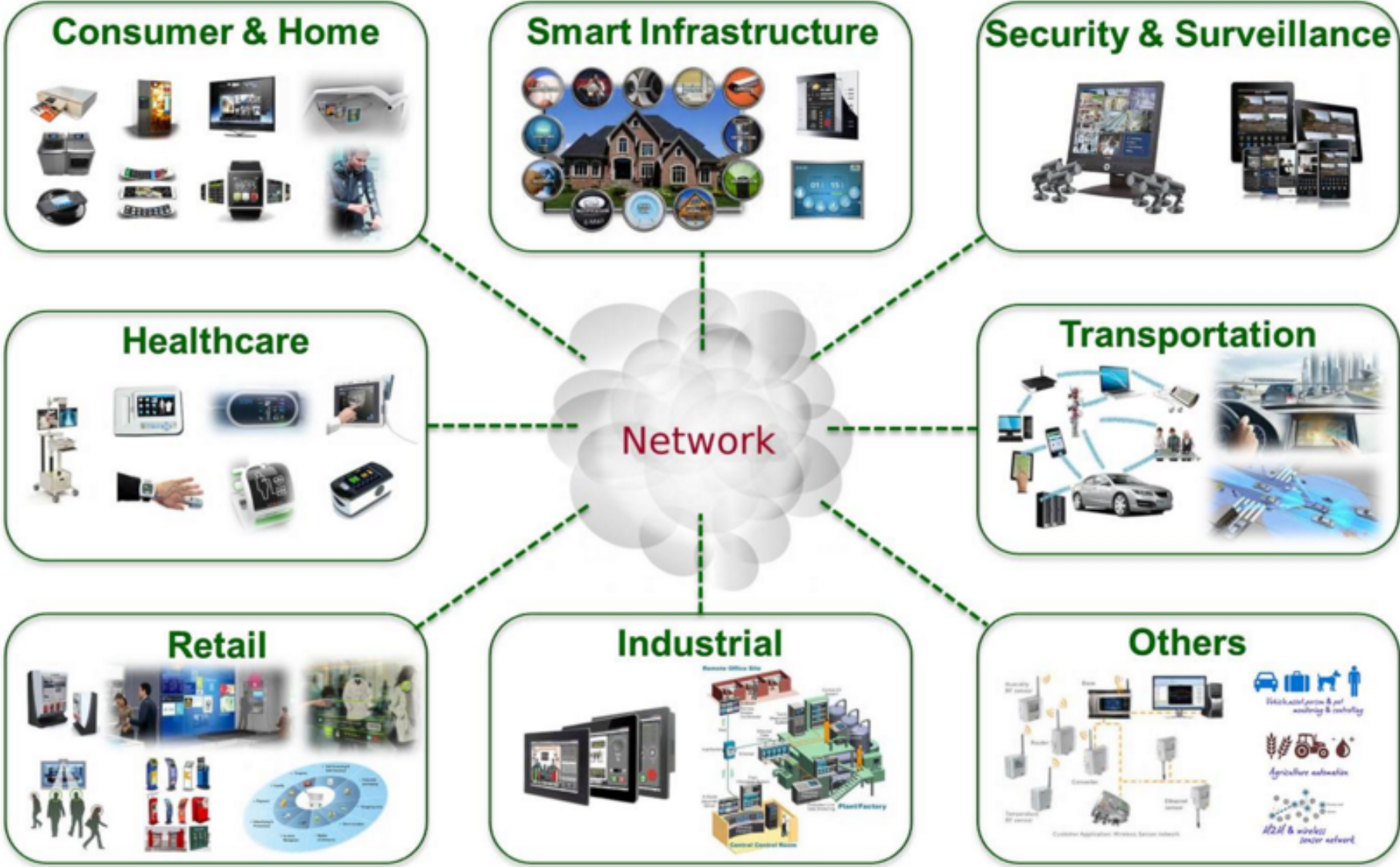
Documents



Identification of assets

Information Assets	Software Assets	Physical Assets	Services
 <p>Database :</p> <ul style="list-style-type: none">- customers- personnel- production- sales- marketing- finances  <p>Data files</p>	 <p>Application software</p> <p>System software</p>	   	<ul style="list-style-type: none">- Computing services- Communication services- Environmental conditioning services

IoT Ecosystem



Is the Internet of Things safe ?

INTERNET OF THINGS OR INTERNET OF THREATS?

What risks does the IoT brings to your life and how do you use new connected devices wisely

KASPERSKY
© 2015 Kaspersky Lab. All rights reserved.

USB-dongle for video streaming

Using the vulnerability in USB-dongle, the attacker could show false error messages to the user and urge them to reset their wi-fi network password.

Coffee maker

Coffee maker could contain a vulnerability that would expose user's Wi-Fi network credentials.

Baby monitor IP camera

Using credentials to the wi-fi network, criminal could exploit multiple vulnerabilities in Baby monitors and spy on its owners.

Home security system

Contact sensors that use magnetic fields could be bypassed by a burglar with a powerful enough magnet

How to make your life smarter with IoT and stay safe

Before buying an IoT device, search the Internet for news of any vulnerabilities.
The Internet of things is a very hot topic now, and a lot of researchers are doing great job finding security issues in products of this kind. From baby monitors to app-controlled rifles.
It is very possible that the device you are going to purchase has been already examined by security researchers and it is possible to find out whether the issues found in the device have been patched.

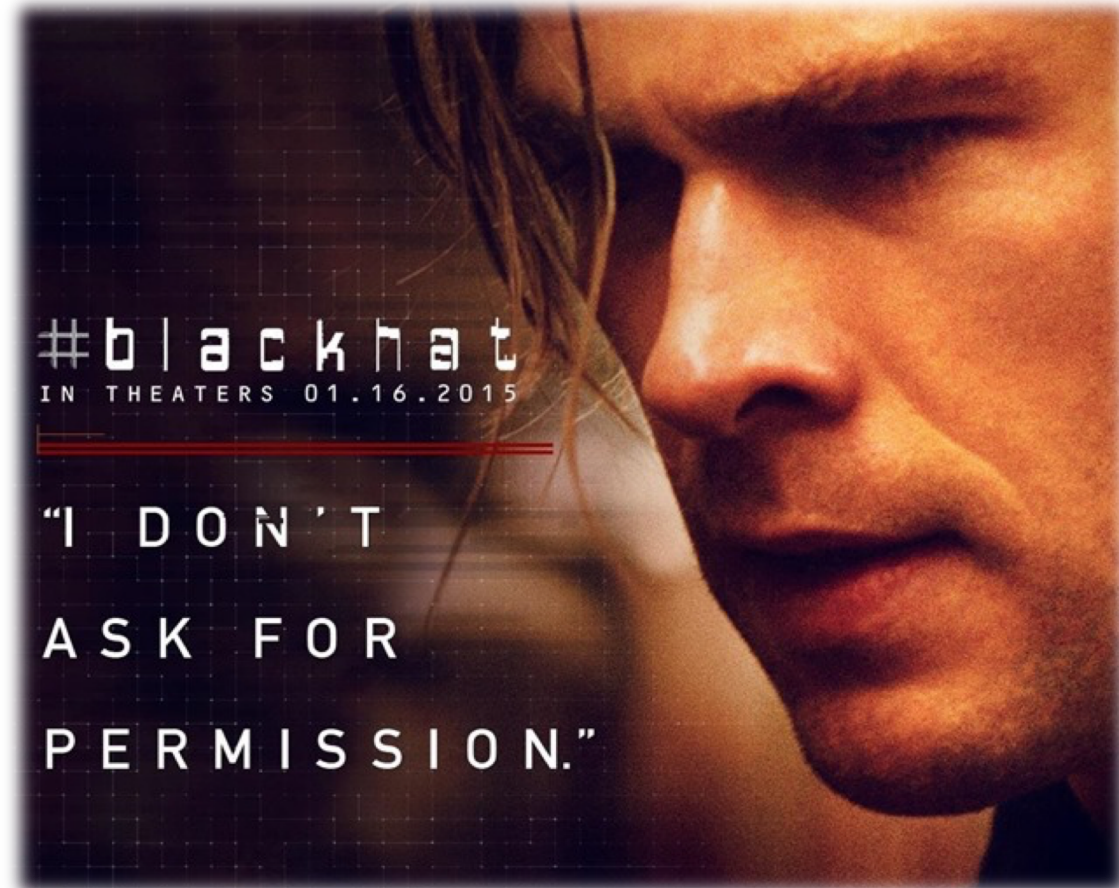
It is not always a great idea to buy the most recent products released on the market.
Along with the standard bugs you get in new products, recently-launched devices might contain security issues that haven't yet been discovered by security researchers.
The best choice here is buy products that have already experienced several software updates.

When choosing the device that will collect information about your personal life and the lives of your family, like a baby monitor, maybe it'd be wise to choose the simplest RF-model capable only of transmitting an audio signal, without Internet connectivity.
If that is not an option, than follow our 1st advice - choose wisely!



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)



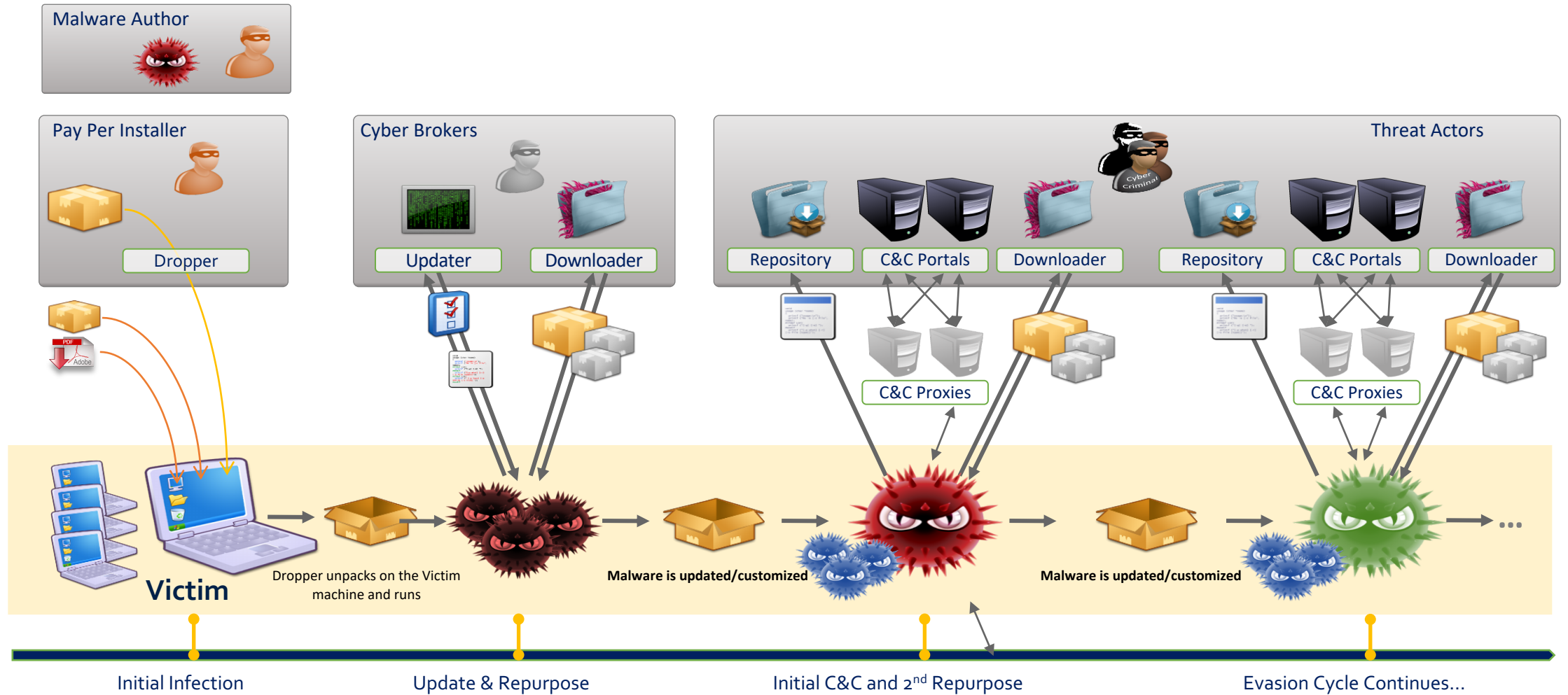
Advanced: APTs involve groups of attackers often working with governments and commercial entities. These groups are able to combine multiple targeting methods with a range of tools, technologies and techniques to reach, compromise, and maintain access to a target. Such groups usually have advanced technology 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.

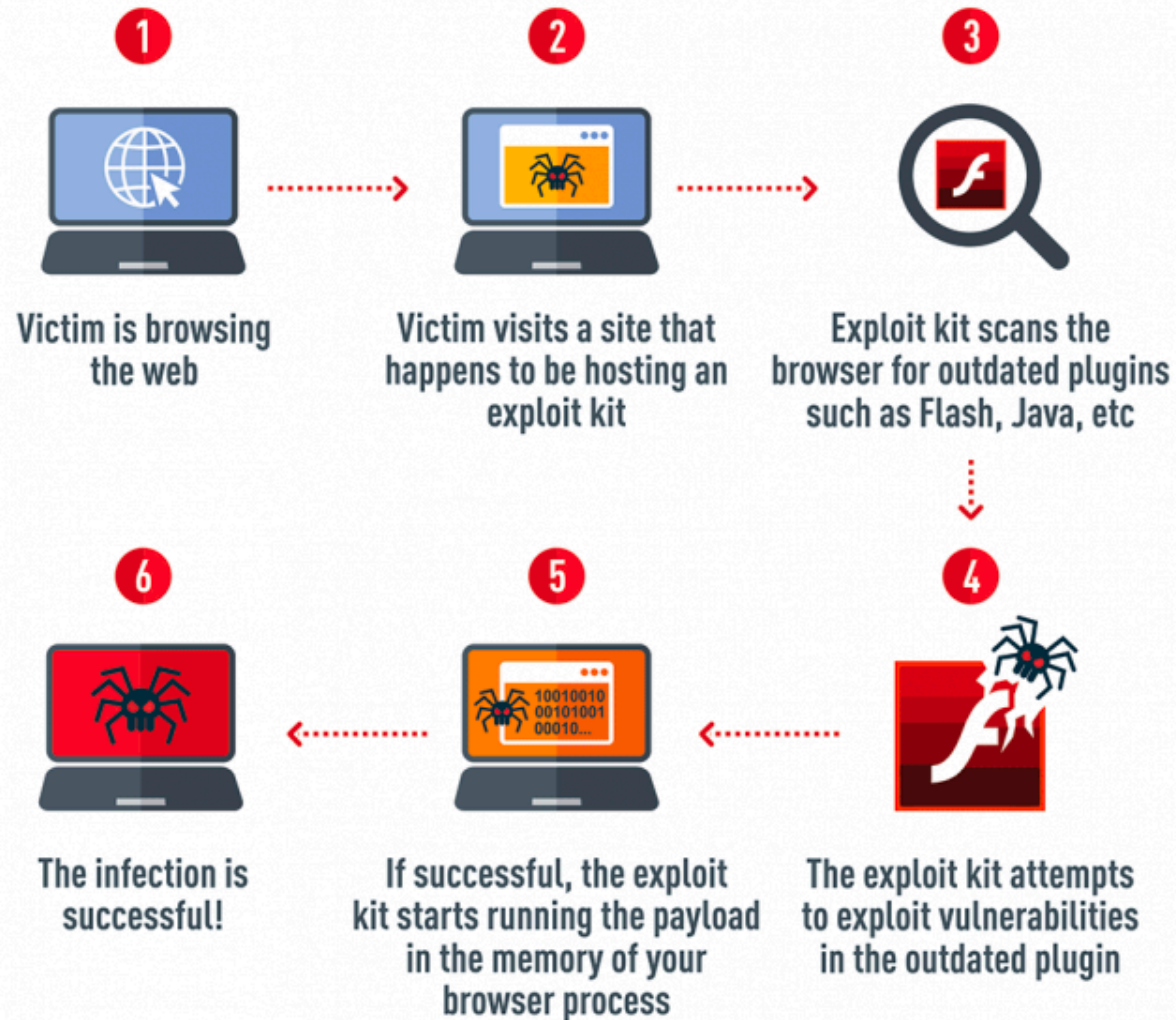
Threat: APTs require attackers who are skilled, motivated, organised and well-funded. They are executed by coordinated humans, rather than by mindless and automated pieces of code.

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

APT Life Cycle

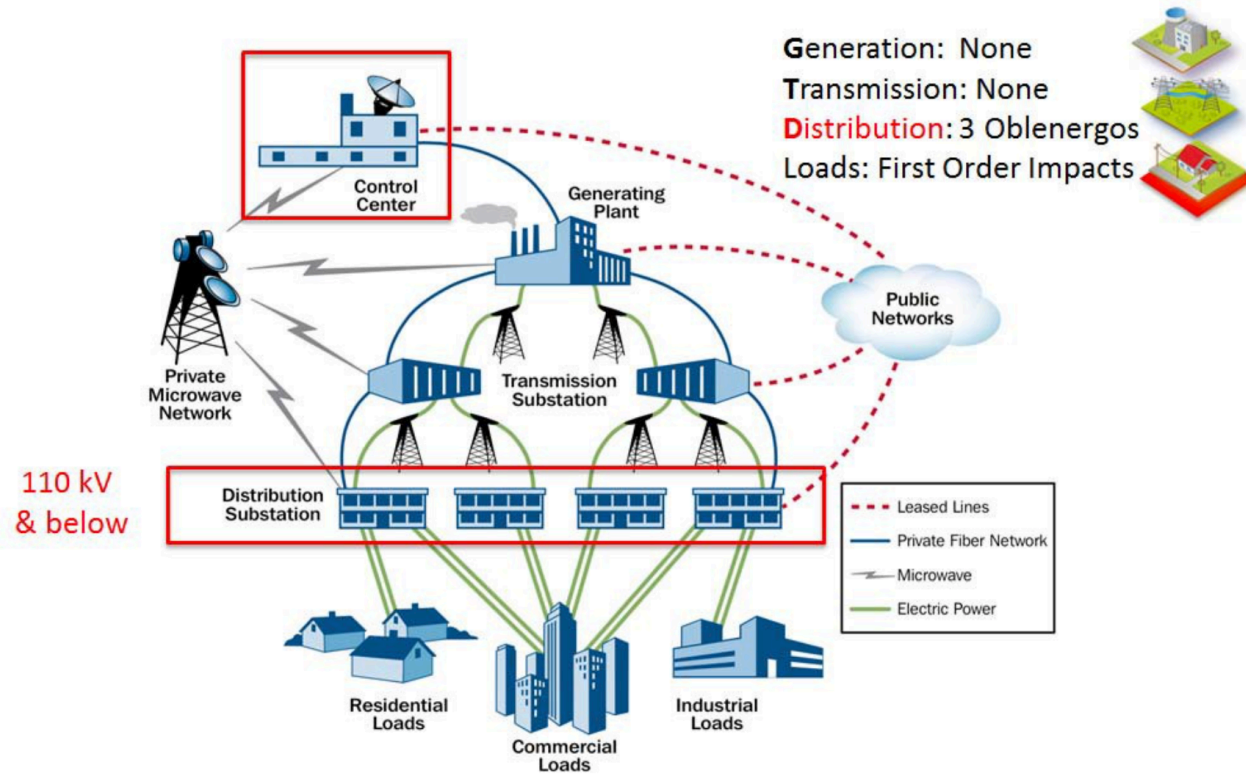


How fileless malware works



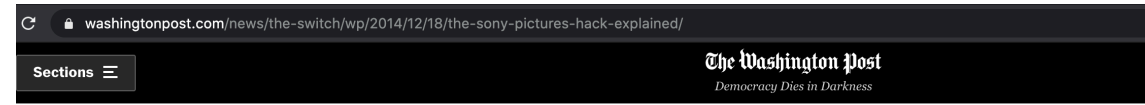
On **December 23, 2015**, the **Ukrainian Kyivoblenergo**,
The outages were due to a third party's illegal entry
into the company's computer and SCADA systems

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



Source: Modification to the DHS Energy Sector-Specific Plan 2010

Figure 1: Electric System Overview



The Switch

The Sony Pictures hack, explained



A scene from "The Interview." (Ed Araquel/Sony Pictures Entertainment)

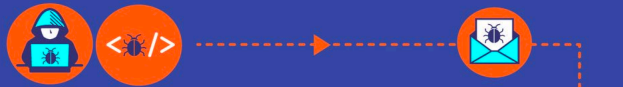


How it works

Carbanak / Cobalt

1 DEVELOPMENT
The cybercriminal is the brains of the operation and develops the malware

Spear-phishing emails are sent to bank employees to infect their machines



2 INFILTRATION AND INFECTION
The cybercriminal deploys the malware through the bank's internal network, infecting the servers and controlling ATMs



3 HOW THE MONEY IS STOLEN

MONEY TRANSFER
The criminal transfers the money into their account or foreign bank accounts

INFLATING ACCOUNT BALANCES
The criminal raises the balance of bank accounts and money mules withdraw the money at ATMs

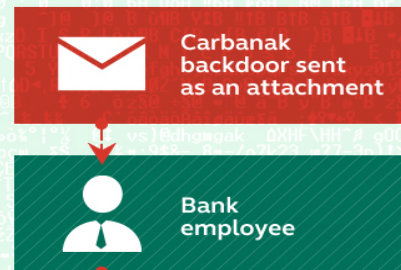
CONTROLLING ATMs
The criminal sends a specific ATMs to spit out cash and money mules collect the money

4 MONEY LAUNDERING

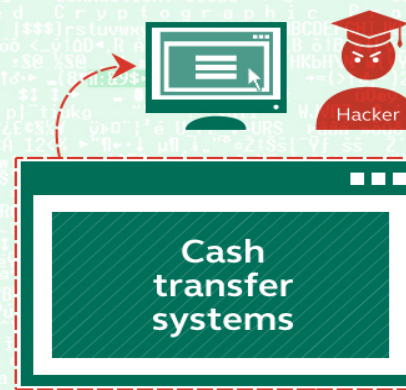


How the Carbanak cybergang stole \$1bn A targeted attack on a bank

1. Infection



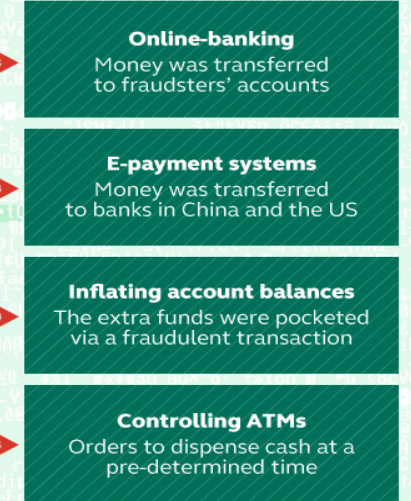
2. Harvesting Intelligence
Intercepting the clerks' screens



100s of machines infected in search of the admin PC



3. Mimicking the staff
How the money was stolen



© 2015 Kaspersky Lab



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

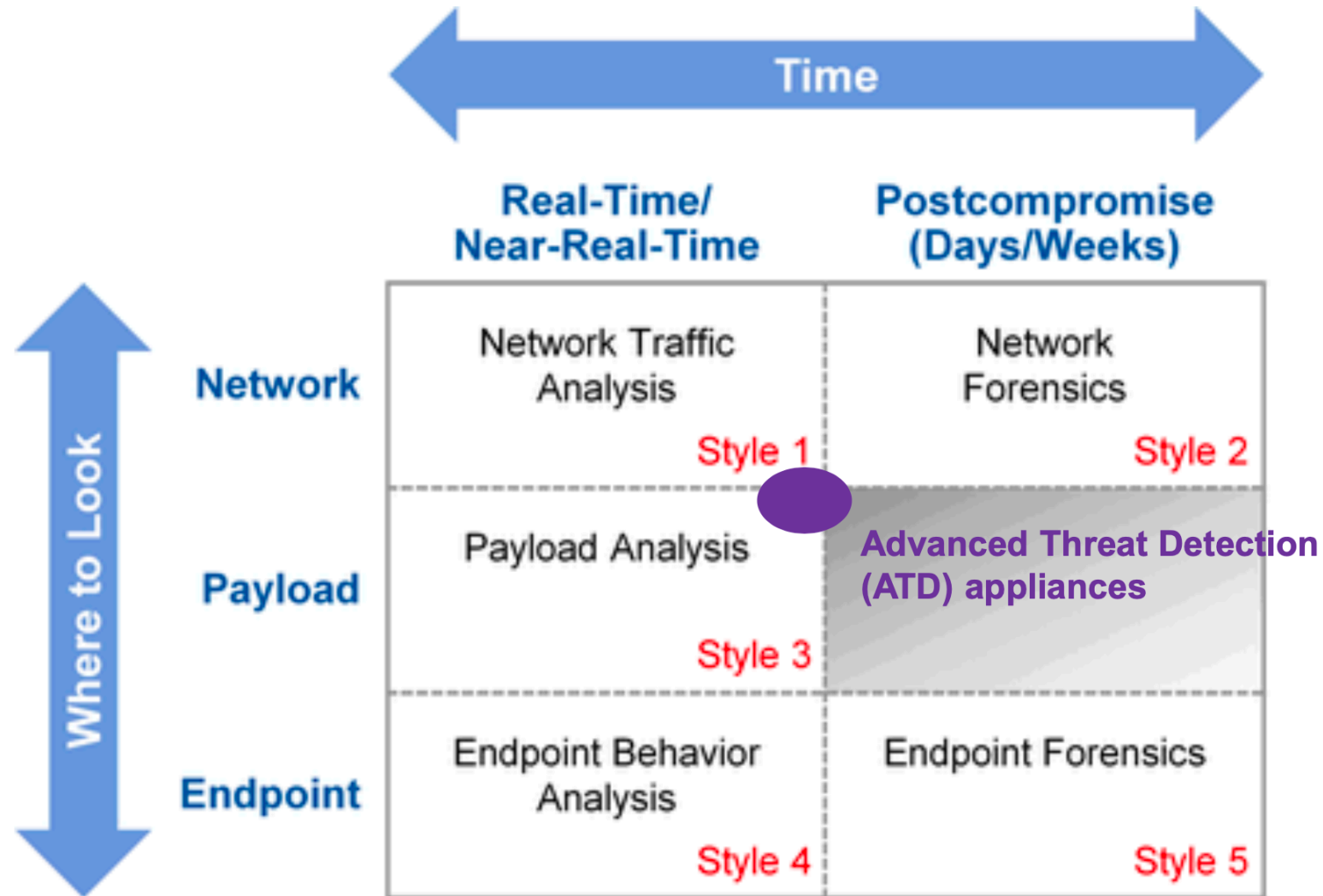
Source : <https://www.europol.europa.eu/publications-documents/carbanak/cobalt-infographic>

How we can protect from Cyber Threats?



- 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



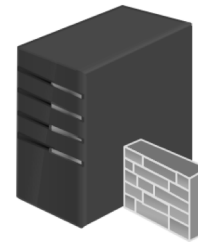
Traditional Anti Virus



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)

- 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...

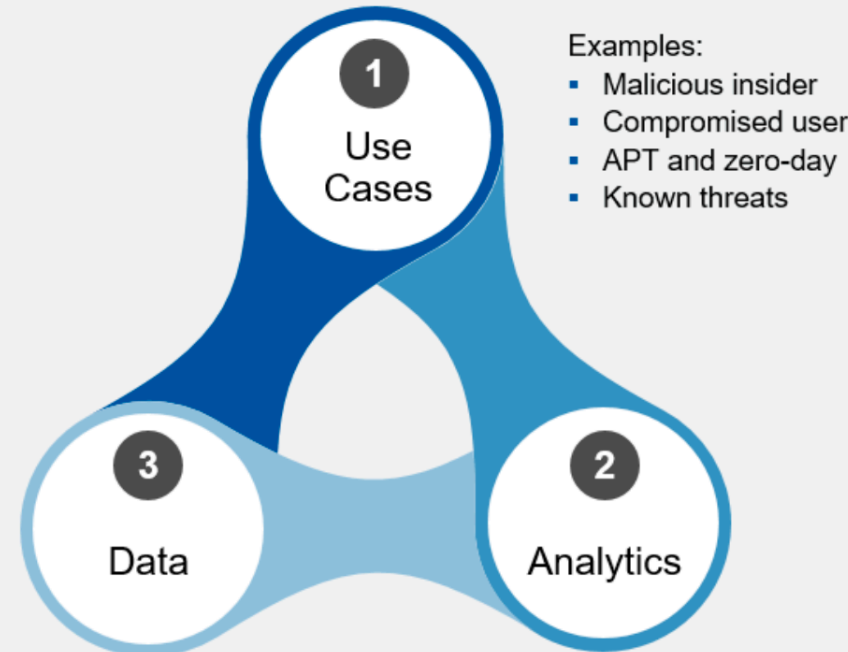


Source: Stellar Cyber



POWERED BY AI

The Three Pillars of UEBA



Examples:

- Malicious insider
- Compromised user
- APT and zero-day
- Known threats

Examples:

- Events and logs
- Network flows and packets
- Business context
- HR and user context
- External threat intelligence

Examples:

- **Future** Generative adversarial networks
- Ensemble networks
- Deep learning
- Supervised machine learning
- Unsupervised machine learning
- Statistical modeling
- Rule-based systems

The Rise of Machine Learning

Deep Learning

- Self-identification of features
- Intermediate representation discovery
- Can be effective at delivering security analyst automation for virtual alert triage and investigation

Ensemble Models

- Differing methodologies and models can run concurrently with each has a "vote" on the treatment
- Requires more-sophisticated computing capabilities than a single algorithm for real-time use

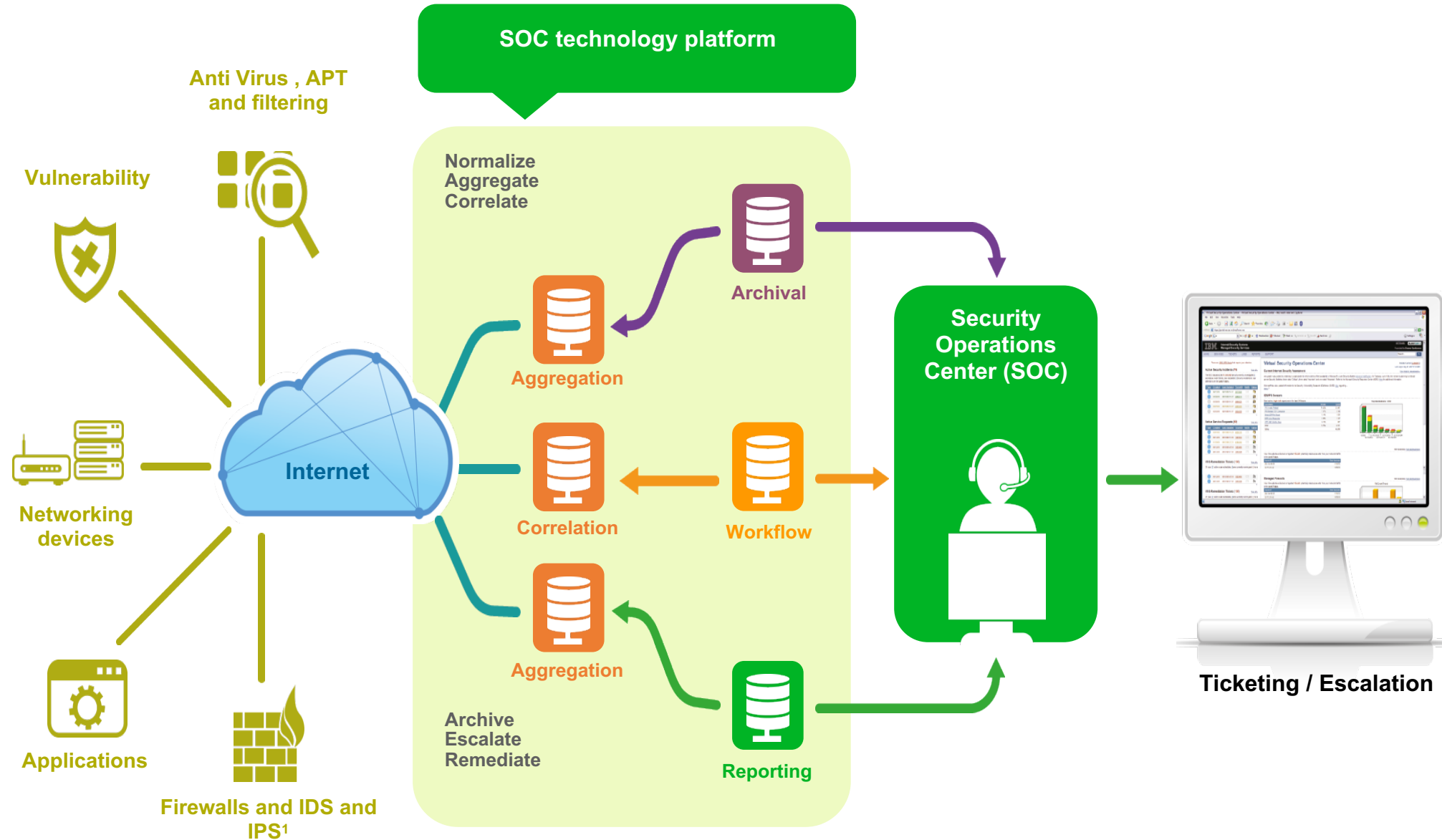
Unsupervised Machine Learning (Anomaly Detection)

- Anomaly detection
- Can use unstructured, unlabeled data
- Effective for cluster analysis and identification of outliers

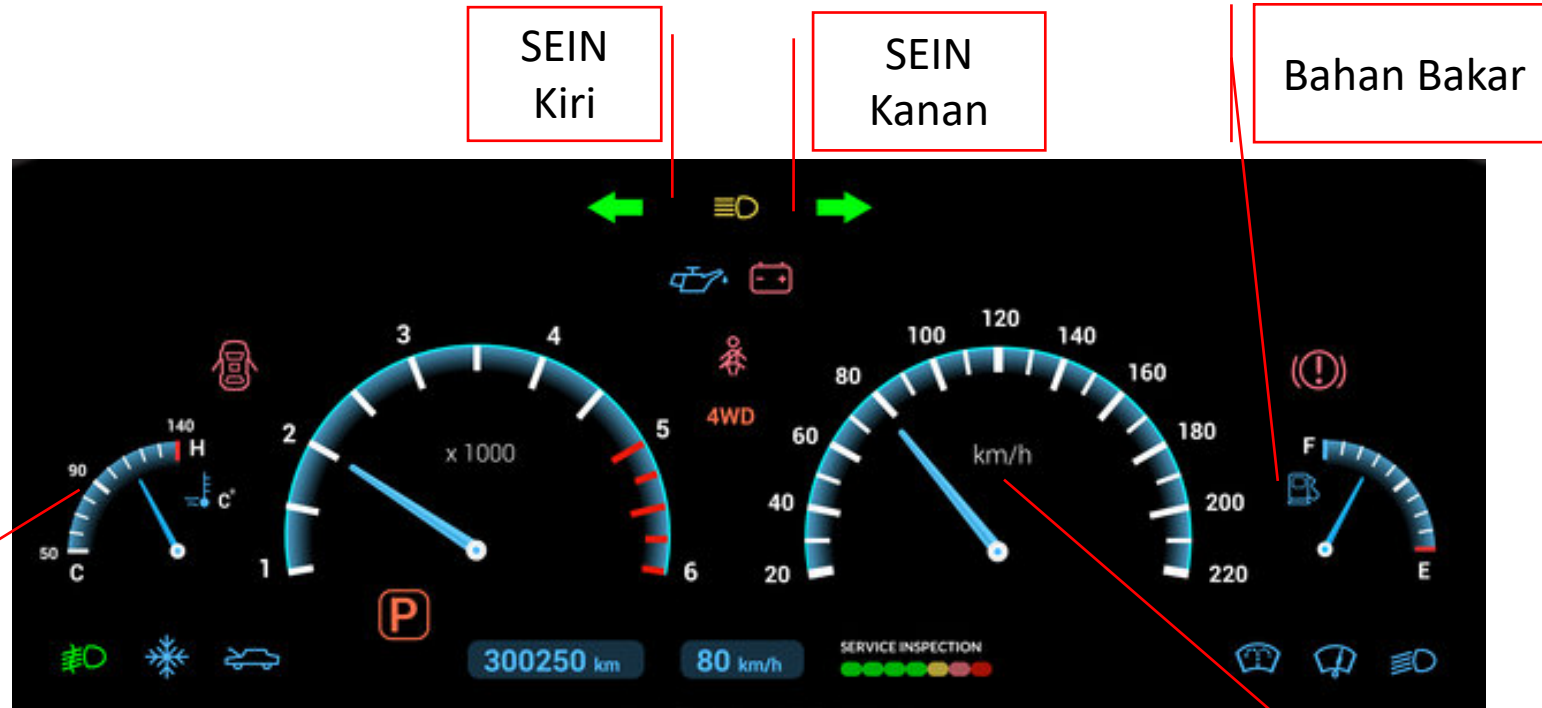
Supervised Machine Learning (Predictive Modeling)

- Neural networks; Bayesian modeling
- Discovering "known bad" and "known unknowns"

Security Operation Center/MDR Overview



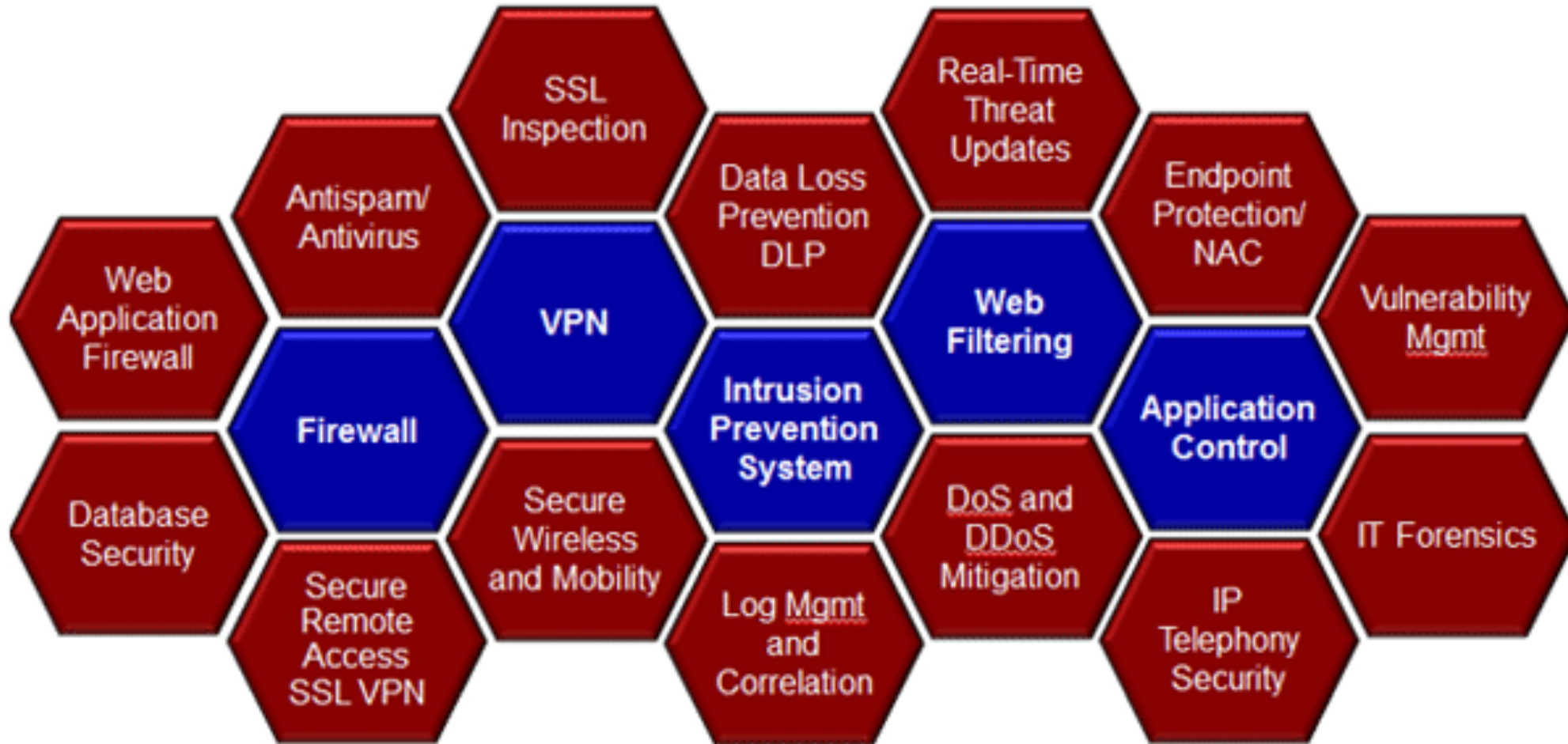
SOC is like a car dashboard



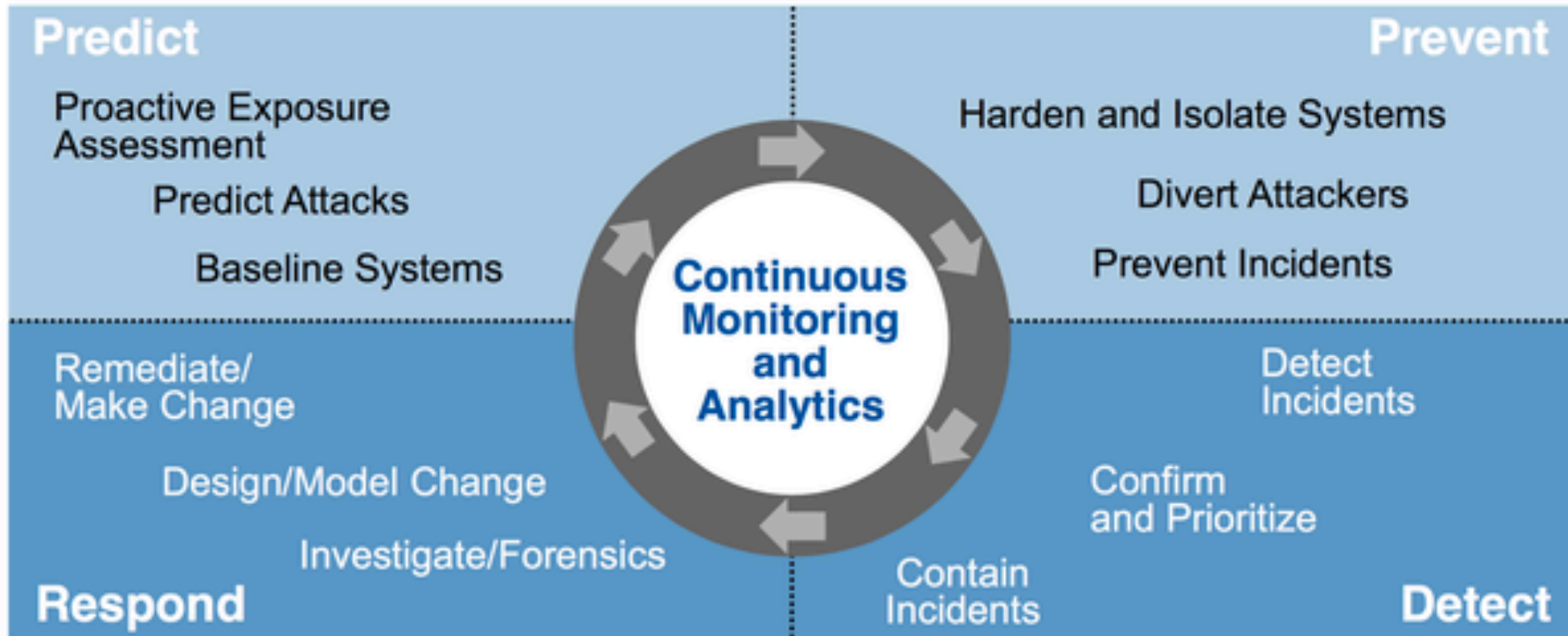
SOC Room



Why do we need SOC ?



The Adaptive Security Architecture



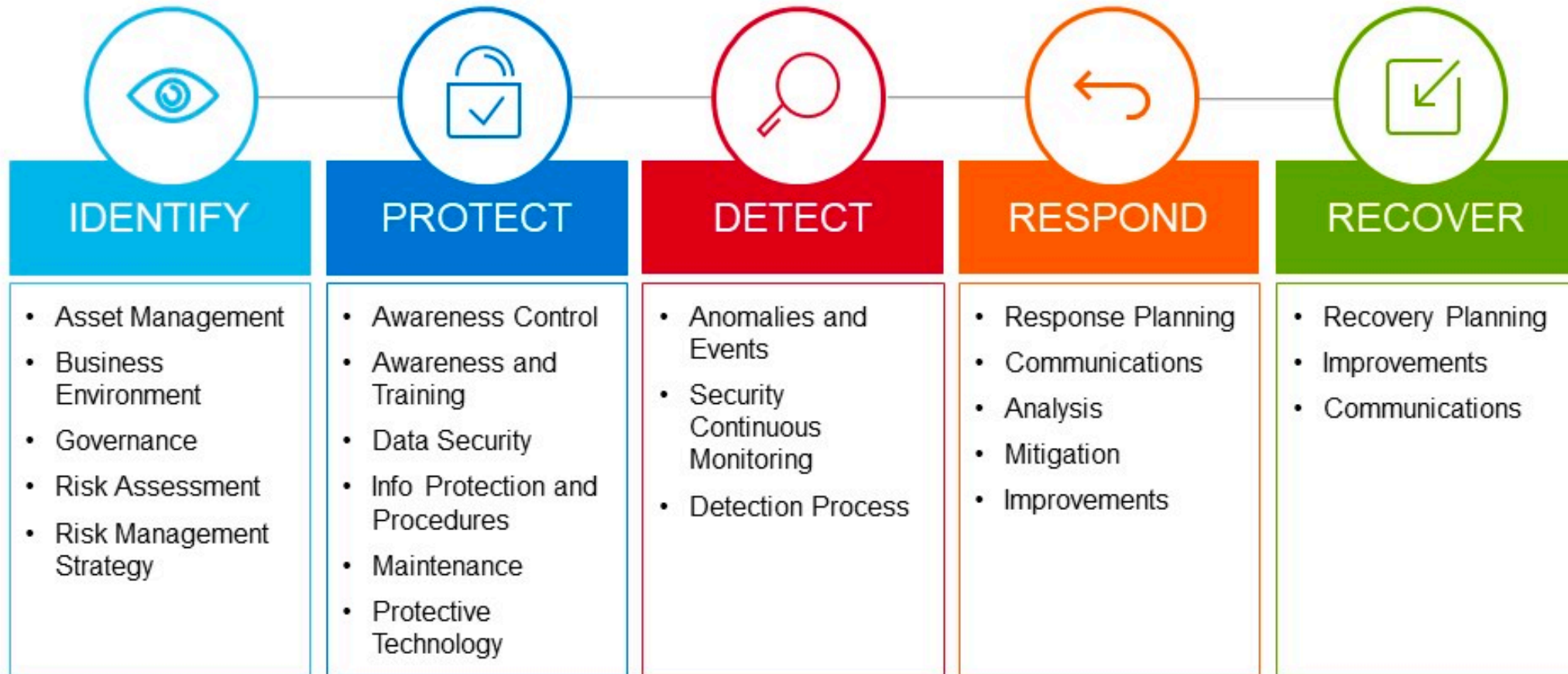
Source: Gartner (February 2014)

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%)

NIST Cybersecurity Framework Overview





Terima Kasih