UNIT-V

UNIT-V

- Threat Intelligence
- Investigating an Incident
- Recovery Process:
- Cyber-Physical Systems (CPS)

1. Threat Intelligence

- **Introduction to threat intelligence**
- **Open-source tools for threat intelligence**
- **Microsoft threat intelligence**
- **Leveraging threat intelligence to investigate suspicious activity**

Introduction to Threat intelligence

- **Intelligence is knowledge and foreknowledge** of the world around us – the prelude to decision and action…” - US Central Intelligence Agency (CIA)
- “Intelligence is **information that is received or collected to answer specific questions** on who, what, where, when, how and why…” - UK National Crime Agency (NCA).
- “**Threat intelligence is threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision making processes**.” - NIST SP 800-150
- **Intelligence Collection Disciplines: OSINT** (Open Source Intelligence), **HUMINT** (Human Intelligence) , **SIGINT** (Signal Intelligence) ,**GEOINT** (Geospatial Intelligence) and **IMINT** (Imaginary Intelligence)

Threat intelligence in other context

- **Military Context**: The term "**threat intelligence**" **from military**, which are mainly based on **HUMINT** (Human Intelligence) and **SIGINT** (Signals Intelligence).
- **Cyber Security Context**: In the context of **cybersecurity** as well as our subject, threat intelligence **refers to Cyber Threat Intelligence.**

Cyber threat intelligence

- Using threat intelligence towards the collected data can **bring more meaningful results and reveal actions** that are not detectable by traditional sensors.
- This enables an organization **to take proactive approach against known and unknown threat.**
- **The targeted attacks need the targeted defense!**

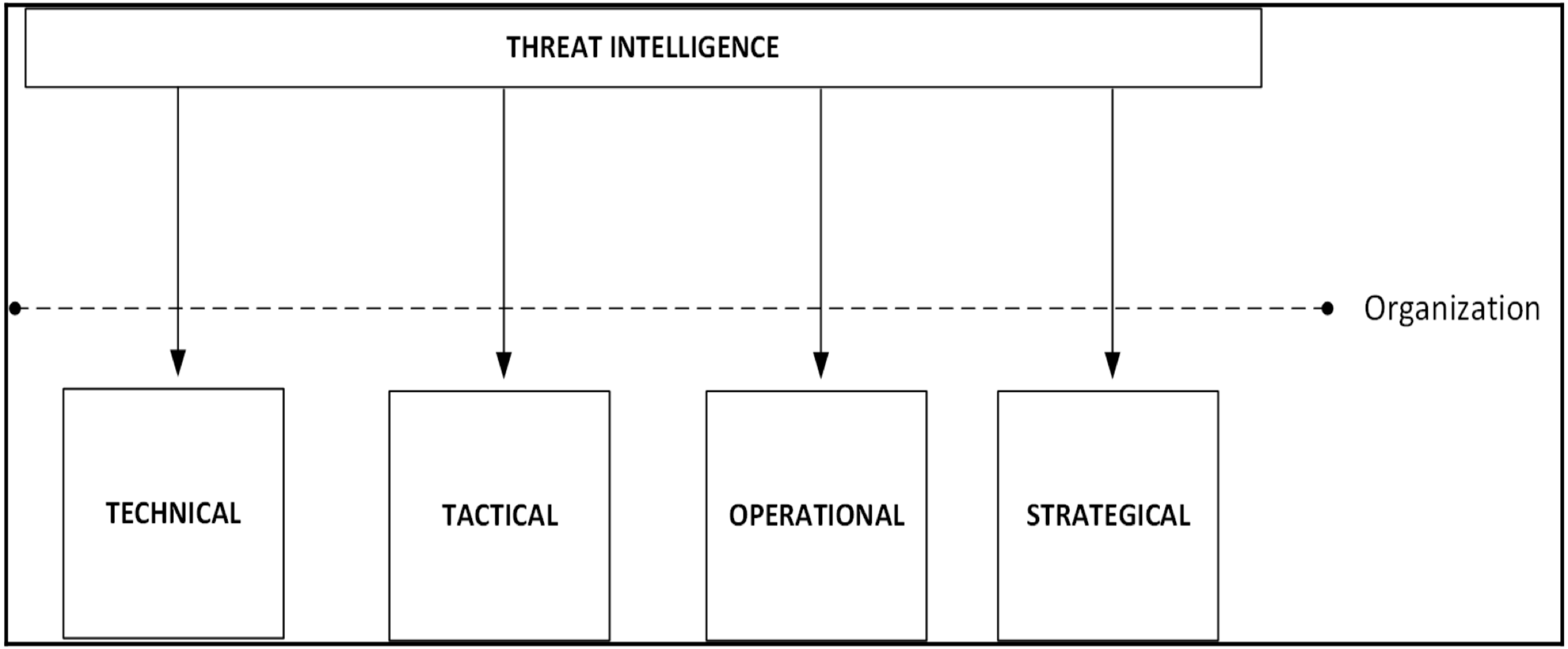
- **The areas where the information obtained from (cyber) threat intelligence can be used:**
  - ✓ **Profiling motivations**: cybercrime, hactivism, cyber espionage (more on next page)
  - ✓ **Analyzing attacker tactics**: attacker methodologies, tools and strategy
  - ✓ **Analyzing techniques (of attacks)**: indicators of specific malware
  - ✓ **Assessing operations**: assessment of an organisation's ability in determining future cyber-threats
- **Examples of profiling motivation:** Detection can be improved by learning more about the adversaries
  - ✓ **Cybercrime**: One of the main **motivations is to obtain financial gains**.
  - ✓ **Hacktivism**: This group has a broader scope of motivation—**it can range from an expression of political preference** to just an expression for a **particular cause.**
  - ✓ **Cyber espionage/state-sponsored**: There are a growing number of cyber spying cases as a **part of bigger state-sponsored campaigns**.

- **The question to ask**: **Which type of attacker among three is most likely to target our organization?**
- **Threat Intelligence could help scope data based on the adversary**.
  - ✓ For example, if we are responsible for the defense of a financial institution, we want to obtain **threat intelligence from adversaries that are actively attacking the financial industry.**
- **Scoping the adversary**
  - ✓ Using an intelligence-led approach has long been accepted as **best practice in the realm of conventional security.**
  - ✓ **Without it, organisations will invariably defend against too little**, because they don't understand the threats they face, or try to defend against all potential threats – an unsustainable approach that may also impair the organization's ability to operate effectively.

- The cyber threat intelligence ensures that organizations have their **ability to prevent, detect and respon**d to realistic, contemporary and accurate attacks.
- The **Bank of England's CBEST was the first intelligence-led cyber security testing frameworks,** which ensures that organizations are tested on their ability of cyber threat intelligence.
- **The CBEST framework ensures that security testers and threat intelligence providers work together, replicating very real attacks from sophisticated adversaries.**

- The principle has since expanded, both internationally to other financial sectors. These schemes include:
    - ✓ **TIBER-NL** (Threat Intelligence Based Ethical Red-teaming Netherlands) for the Dutc financial sector
    - ✓ **TBEST** for the UK telecoms sector
    - ✓ **TIBER-EU** for the European financial sector
    - ✓ **iCAST** (Intelligence-led Cyber Attack Simulation Testing) for Hong Kong’s financia sector
    - ✓ **GBEST** for UK government departments
    - ✓ **ATTEST** for the UK aviation industry

- There are **different areas that cyber threat intelligence can be used**: Each area differs in the nature and format of the material conveyed, its intended audience and its a



Operational threat intelligence:

- Operational threat intelligence **uses the collection of data and information to respond to a threat or attack as it is in progress**.
- It is meant to be used immediately **and provides real-time alerts that can help your security team understand the scope of an attack and defend against it**. It is a critical part of detecting active threats and responding to them quickly, so that your organization suffers minimal harm
- **Operational threat intelligence** often **relates** to details of potential impending **operations against an organization.**
- Although it is not always easy to obtain, by using an all-source approach an intelligence provider will be able to detect.
- **Operational threat intelligence e.g.: A conversation** from **cyber activists - "discussing potential targets for an upcoming campaign, or data leaked or sold on a dark web forum" that could be used in an operation against the company**.

Tactical threat intelligence:

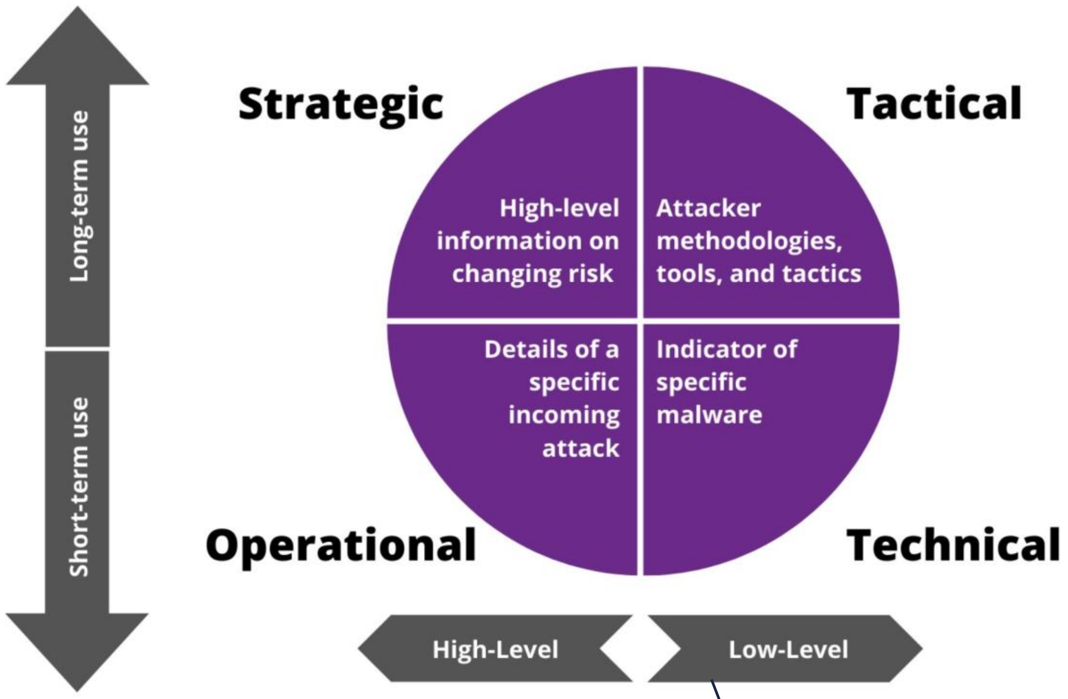
- It **consists of material relating to the techniques, tactics and procedures (TTP's)** used by threat actors.
- **Indicators of compromise (IOCs)** are the main deliverable for tactical threat intelligence providers.
- These are particularly **useful for updating signature-based defense systems** to defend against known attack types, but can **also prove useful** for more proactive measures, such as **threat hunting exercises**.
- It is therefore particularly useful to network defenders such as **Network Operations Centers (NOCs).**
- **CTI (Cyber Threat Intelligence)** providers will generally **supply IOCs In machine readable** formats, whereas intelligence on TTPs will be in human-readable formats and will require human assimilation and action.

Technical threat intelligence :

- focuses on **specific clues or evidence of an attack** and creates a base to analyse such attacks, like scanning for the IoCs of an attack.

Strategic threat intelligence

- exists to inform senior decision makers **of broader changes in the threat landscape**.


Long-term use
Short-term use
Strategic
Tactical
High-level information on changing risk
Attacker methodologies, tools, and tactics
Details of a specific incoming attack
Indicator of specific malware
Operational
Technical
High-Level
Low-Level

Technical Knowledge

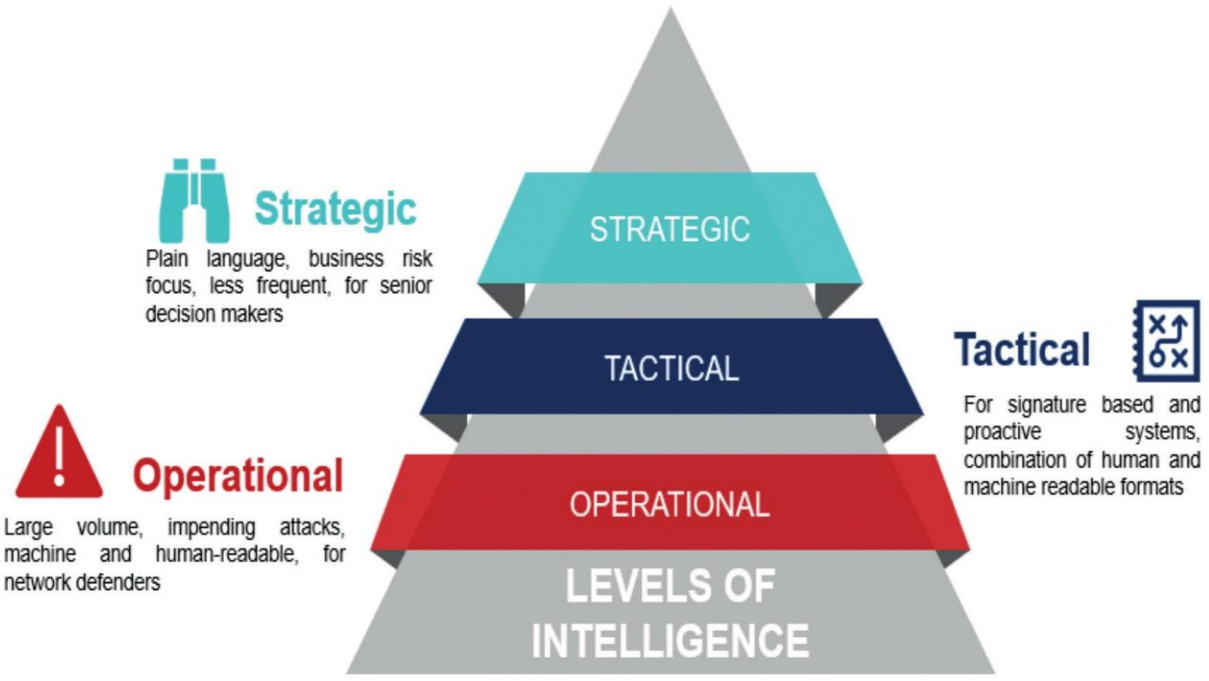

Strategic
Plain language, business risk focus, less frequent, for senior decision makers
STRATEGIC
TACTICAL
Tactical
For signature based and proactive systems, combination of human and machine readable formats
Operational
Large volume, impending attacks, machine and human-readable, for network defenders
OPERATIONAL
LEVELS OF INTELLIGENCE

Figure 5: The three levels of cyber threat intelligence

Some Reference for Levels of TI

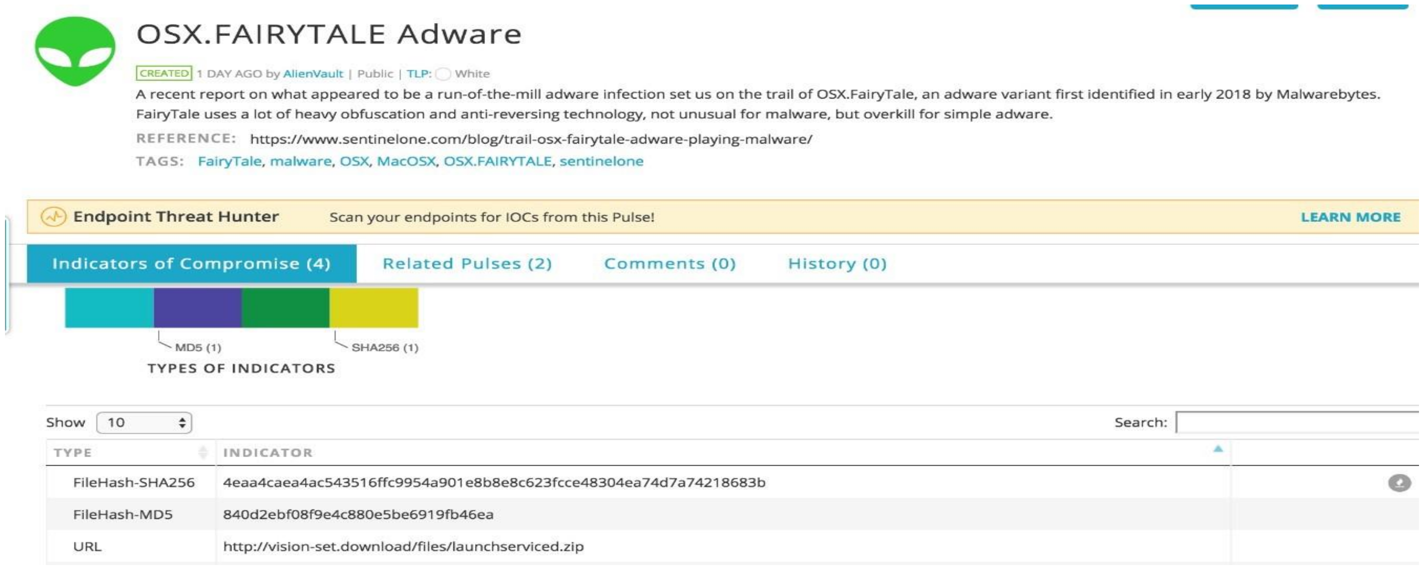
1. https://www.crest-approved.org/wp-content/uploads/2022/04/CREST-Cyber-Threat-Intelligence.pdf
2. https://www.wallarm.com/what/threat-intelligence

Microsoft Threat Intelligence

- **Microsoft consumes threat intelligence through different channels, such a**s:
  - ✓ **The Microsoft Threat Intelligence Center**, which aggregates data from:
    - ➢ **Honeypots**, **malicious IP addresses, botnets, and malware detonation feeds**
    - ➢ **Third-party** sources (threat intelligence feeds)
    - ➢ **Human-based** observation and intelligence collection
  - ✓ **Intelligence coming from consumption of their service**
  - ✓ **Intelligence feeds generated by Microsoft and third parties**

Open-source tools for threat intelligence

- Various open source tools (for tactical threat Intelligences):
  - ✓ **Quick IP validation**: https://fraudguard.io/
  - ✓ **Malware inspection**: https://vms.drweb.com
  - ✓ **Threat intelligence exchange**: https://otx.alienvault.com/



OSX.FAIRYTALE Adware

CREATED 1 DAY AGO by AlienVault | Public | TLP: ○ White

A recent report on what appeared to be a run-of-the-mill adware infection set us on the trail of OSX.FairyTale, an adware variant first identified in early 2018 by Malwarebytes. FairyTale uses a lot of heavy obfuscation and anti-reversing technology, not unusual for malware, but overkill for simple adware.

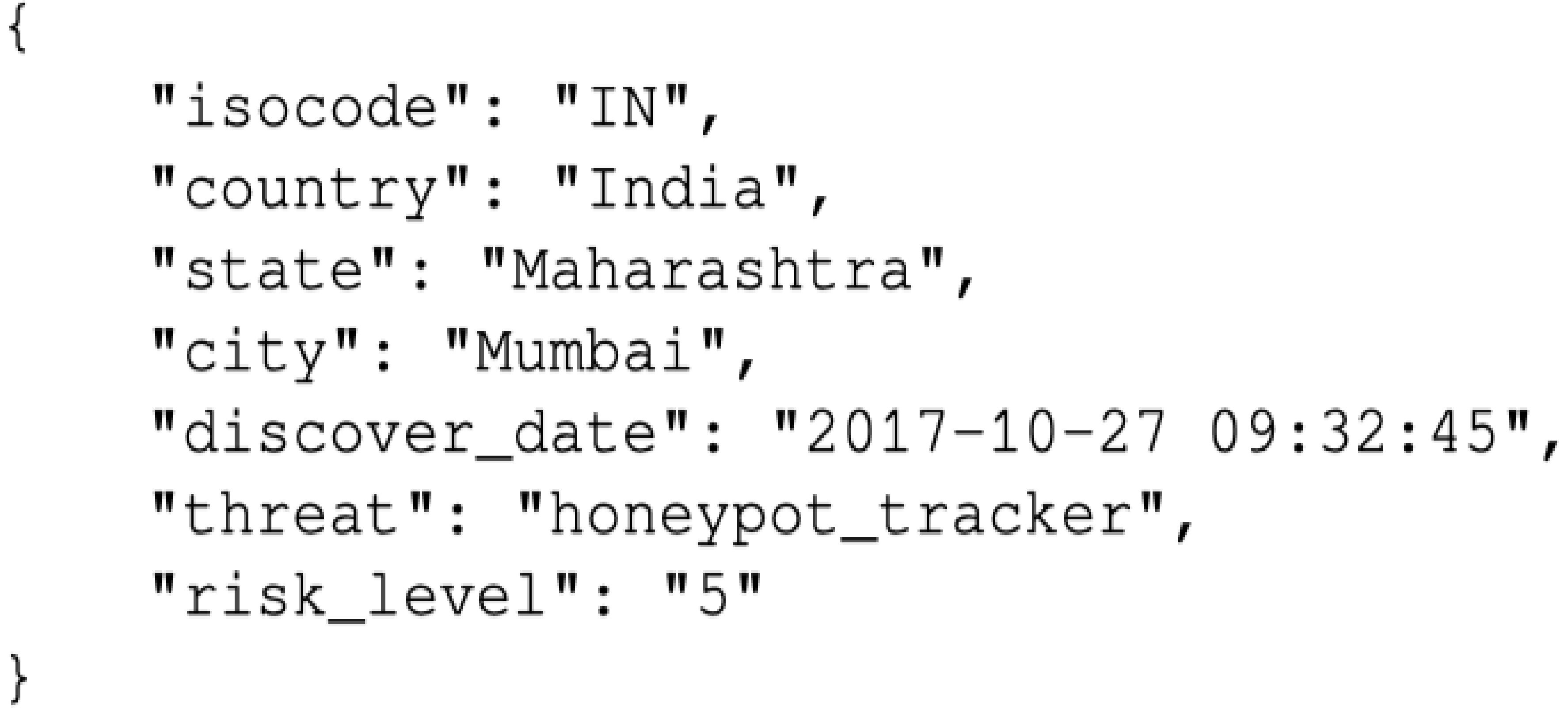
REFERENCE: https://www.sentinelone.com/blog/trail-osx-fairytale-adware-playing-malware/

TAGS: FairyTale, malware, OSX, MacOSX, OSX.FAIRYTALE, sentinelone

Endpoint Threat Hunter Scan your endpoints for IOCs from this Pulse! LEARN MORE

TYPE	INDICATOR
FileHash-SHA256	4eaa4caea4ac543516ffc9954a901e8b8e8c623fcce48304ea74d7a74218683b
FileHash-MD5	840d2ebf08f9e4c880e5be6919fb46ea
URL	http://vision-set.download/files/launchserviced.zip

- For instance, test IP “220.227.71.226” on 10/27/2017, the result was



```
{
    "isocode": "IN",
    "country": "India",
    "state": "Maharashtra",
    "city": "Mumbai",
    "discover_date": "2017-10-27 09:32:45",
    "threat": "honeypot_tracker",
    "risk_level": "5"
}
```

Leveraging Threat Intelligence To Investigate Suspicious Activity

- **Challenges of interpreting many security alerts**
  - ✓ **According to Microsoft's Lean** on the Machine report, **an average large organization has to look through 17,000 malware alerts each week**, taking on **average 99 days for an organization to discover a security breach.**
  - ✓ **End up randomly prioritizing**, and in some cases **even ignoring, future alerts**.
- **Threat intelligence assisting incident response**
  - ✓ The **Blue Team works primarily on the defense system**, they do collaborate with the incident response team by providing the right data that can lead them to find the root cause of the issue.
  - ✓ **Other teams in cyber security**: Red Team: Conducts offensive security testing , Purple Team: Acts as a bridge between the Red and Blue Teams, Green Team: Focuses on developing security solutions and processes , Yellow Team: Sometimes involved in specialized technical tasks like creating security policies, compliance, and governance. White Team: Manages and oversees the security testing exercises, ensuring that Red, Blue, and Purple teams follow agreed upon protocols.

- **Alert triage**
  - ✓ The **process of determining the most important threat** that must be alerted.
  - ✓ Failing/delaying this process can **lead to a domino effect**, because if triage fails at this level, the operation will also fail.
  - ✓ The **domino effect** in cybersecurity refers to a **chain reaction of adverse events triggered by a single initial failure or oversight**. When a critical threat is not identified, prioritized, or alerted in a timely manner, it can lead to a sequence of security vulnerabilities and compromises.

- **The alert triage usually happens at Network Operations Center (NOC)**. Questions at the end of threat intelligence
  - ✓ Which systems were compromised?
  - ✓ Where did the attack start?
  - ✓ Which user account was used to start the attack?
  - ✓ Did it move laterally? If it did, what were the systems involved in this movement?
  - ✓ Did it escalate privilege? If it did, which privilege account was compromised?
  - ✓ Did it try to communicate with command and control?
    - ✓ If it did, was it successful?
      - ➢ If it was, did it download anything from there?
      - ➢ If it was, did it send anything to there?
  - ✓ Did it try to clear evidence? If it did, was it successful?
  - ✓ What is Cyber Threat Intelligence and how is it used?

2. Investigating An Incident

- Scoping the issue
- Case study: On-premises compromised system
- Case study: Cloud-based compromised system
- Lessons learned

Scoping the issue

- **Scoping in the incident investigation**
  - ✓ A process to determine a given incident is security-related.
  - **Reasons for scoping**
    - ✓ **Not every incident is a security-related incident** and, for this reason, it is vital to scope the issue prior to start an investigation.
    - ✓ Sometimes, the **symptoms** may lead the investigator to **initially think they are security-related,** but as the investigator ask more questions and **collect more data,** it turns out that the **problem was not really related to security.**

- Scoping example
  - ✓ Users reporting systems running “slow”: Rather than dispatching a security responder to initiate an investigation, **basic performance troubleshooting should be conducted**.
  - ✓ During this initial scoping stage, it is also **important to determine the frequency of the issue.** - If the issue is not currently happening, the investigator may need to configure the environment to collect data when the user is able to reproduce the problem.
  - ✓ Make sure to **document all the steps** and provide an accurate action plan for the end use.

Key Artifacts

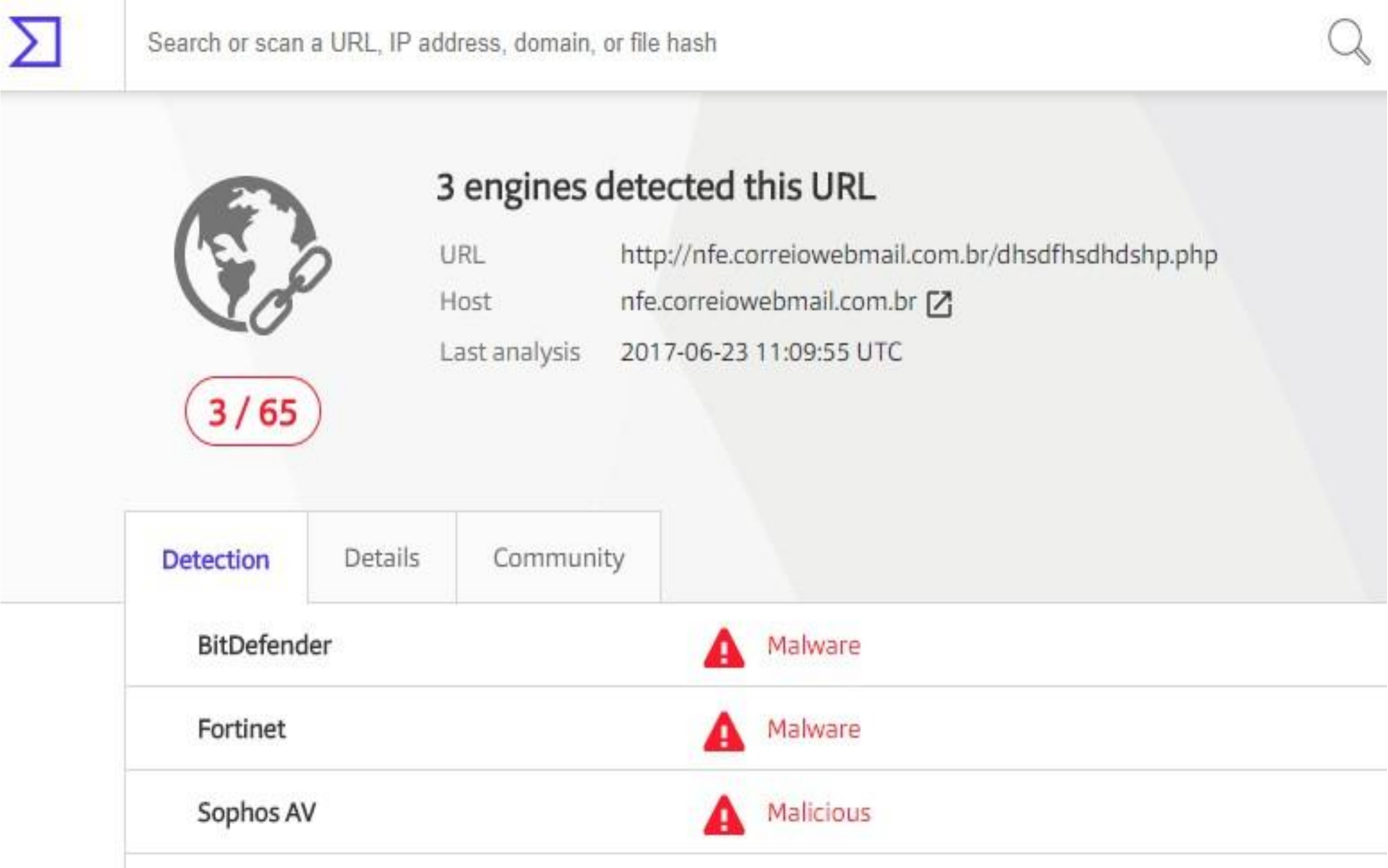
- **More data doesn't necessarily mean better investigation**.
- Data collection should focus on obtaining just **the vital and relevant artifacts** from the target system.
  - ✓ **Too much data can deviate security team from the root cause of the problem**.
- It is important to make sure **you know the information of your system**
- In a **Windows** system, the **information** is usually located in the **registry key.**
- It can be **retrieved** by **PowerShell command** (e.g., Get- ItemProperty).
- **Key artifacts in Windows system**
  - ✓ The **location** (time zone) of the machine
  - ✓ The **networks** the machine visited
  - ✓ **USB** usage
  - ✓ If there is any **malicious software** configured to start when Windows starts
- In addition**, traffics and processes dumps can be collected**, if this is live investigation.

- All **security events** can be captured :
  - ✓ The **audit log** was cleared.
  - ✓ **Logging-on success or failure.**
  - ✓ A **registry value was modified**.
  - ✓ An attempt was made to access an object (e.g. unauthorized access to the file system): This log can be used to drill down who performed this change.
  - ✓ **A new process has been created**: The **malware and ransomware** have a **cmd.exe** [command]. This will create a new process.
  - ✓ A **scheduled task** was **enabled or updated**.
  - ✓ **The user account: enabled**, **created**, or **locked-out account**, **password reset**, **denied remote access.**
  - ✓ **Policies:** Log policy changed, Domain policy changed, Changes in security-enabled global (or local) group.
  - ✓ A **change** has been made to **Windows Firewall exception list**.

Case study : Investigating A Compromised System On-premises

- Compromised by phishing email
  - ✓ The end user (victim) was received the content of the email, which triggered the victim to click the image in the email.
  - ✓ The victim tried to download it but couldn’t and only had a glimpse of a quickly opening and disappearing window.
  - ✓ Then, the victim ignored the email.
- Detection
  - ✓ A couple of days later, he receiving an automated report from IT saying that he accessed a suspicious site and he should call support to follow up on this ticket.
  - ✓ The victim submitted the suspicious mail as an evidence.

- Investigation steps
  - ✓ The URL which was linked in the image was investigated.



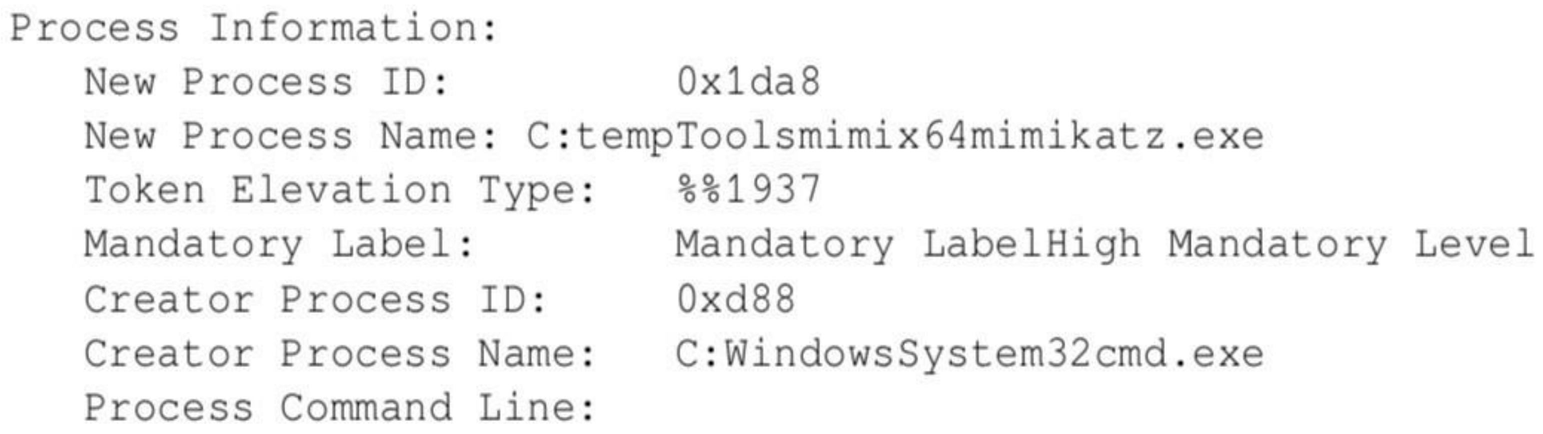
3 engines detected this URL

URL http://nfe.correiowebmail.com.br/dhsdfhsdhdshp.php
Host nfe.correiowebmail.com.br
Last analysis 2017-06-23 11:09:55 UTC

BitDefender	Malware
Fortinet	Malware
Sophos AV	Malicious

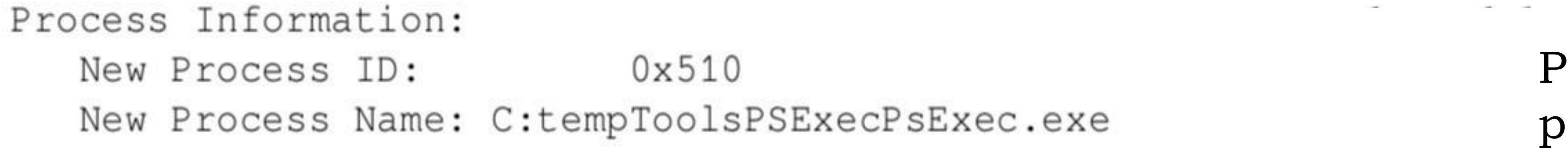
This was already a strong indication that this site was malicious .

- The next step is to review the event logs. The meaningful logs are:



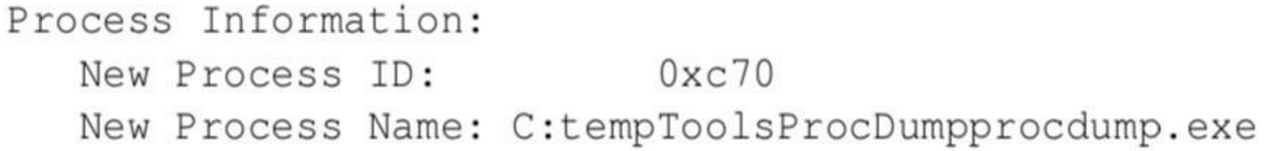
```
Process Information:
   New Process ID:          0x1da8
   New Process Name: C:tempToolsmimix64mimikatz.exe
   Token Elevation Type:    %%1937
   Mandatory Label:         Mandatory LabelHigh Mandatory Level
   Creator Process ID:      0xd88
   Creator Process Name:    C:WindowsSystem32cmd.exe
   Process Command Line:
```

mimikatz: Used to perform pass-the-hash attack



```
Process Information:
   New Process ID:          0x510
   New Process Name: C:tempToolsPSExecPsExec.exe
```

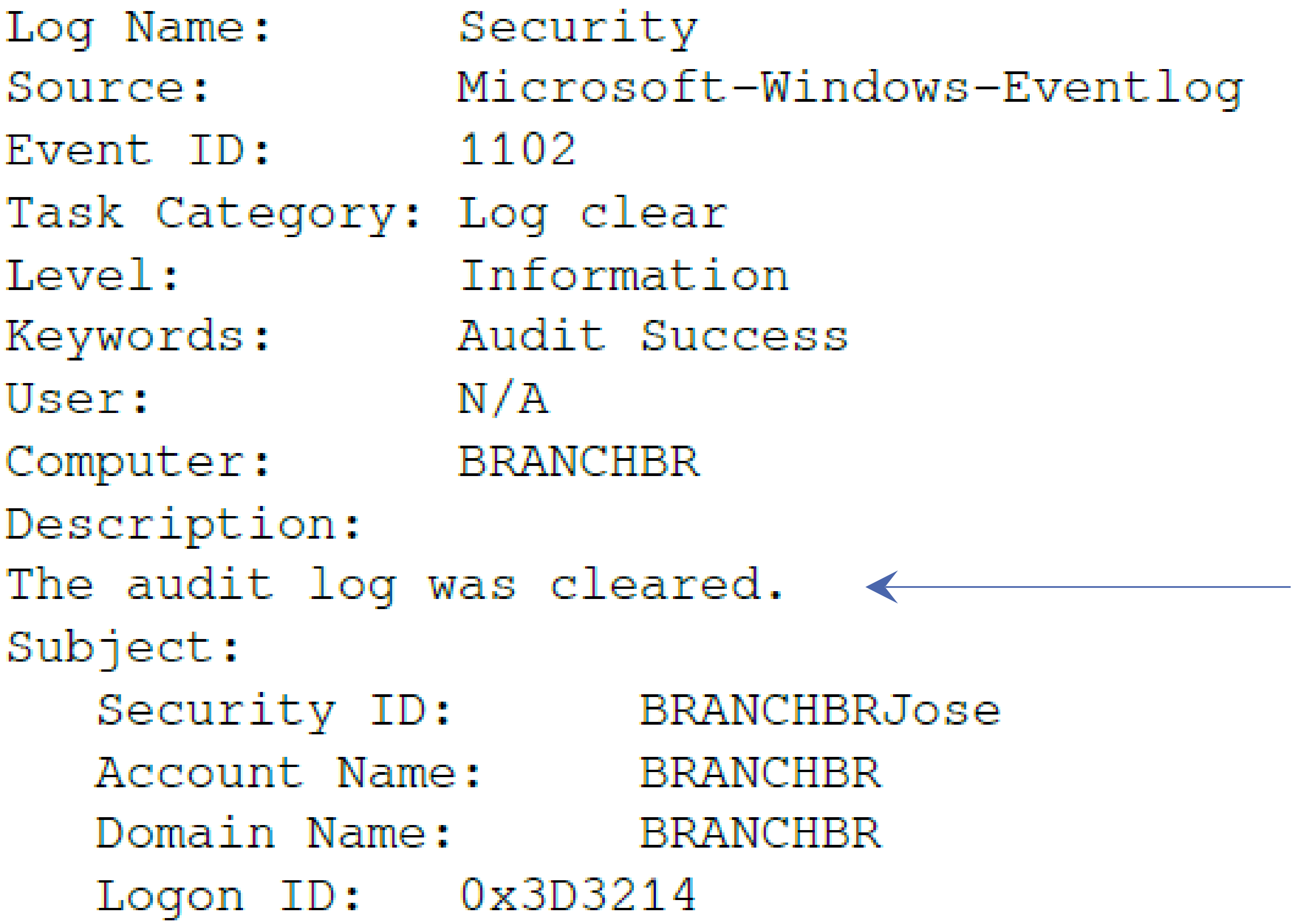
PsExec: Used to perform privileges escalation



```
Process Information:
   New Process ID:          0xc70
   New Process Name: C:tempToolsProcDumpprocdump.exe
```

procdump: Used to dump the credentials

- The meaningful logs are:



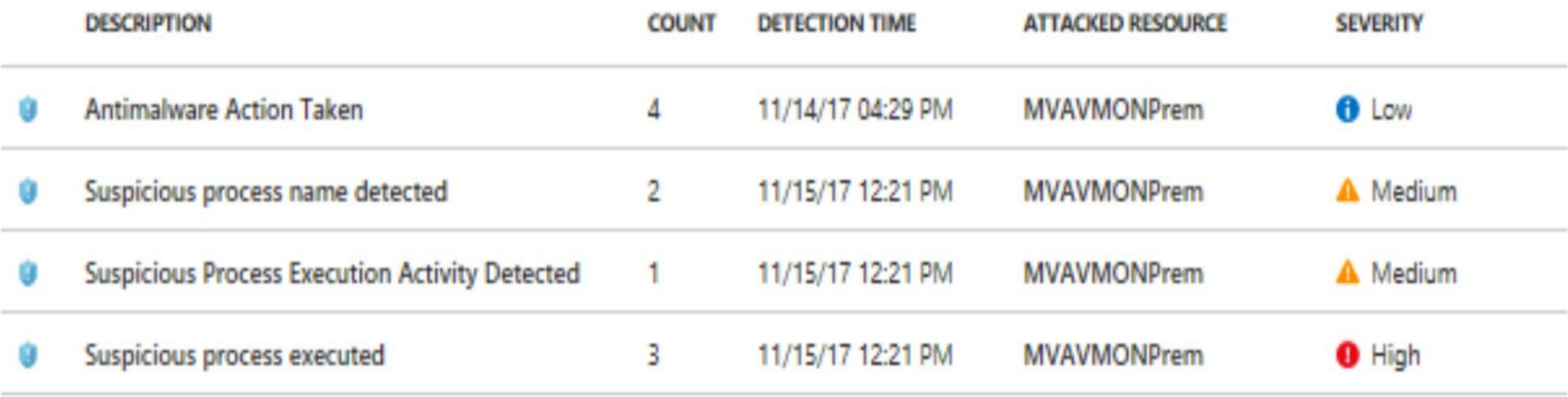
```
Log Name:      Security
Source:        Microsoft-Windows-Eventlog
Event ID:      1102
Task Category: Log clear
Level:         Information
Keywords:      Audit Success
User:          N/A
Computer:      BRANCHBR
Description:
The audit log was cleared.
Subject:
   Security ID:      BRANCHBRJose
   Account Name:     BRANCHBR
   Domain Name:      BRANCHBR
   Logon ID:   0x3D3214
```

The attacker cleared logs. It hid how the attacker achieved privilege escalation.

- Summary of the case
  - ✓ Everything started with a phishing email.
  - ✓ This email had an embedded image that had a hyperlink to a site that was compromised.
  - ✓ A package was downloaded an extracted in the local system, this package contained many tools, such as mimikatz, procdump, and PsExec.
  - ✓ This computer was not part of the domain, so only local credentials were compromised.

Case Study : Investigating A Compromised System In A Hybrid Cloud

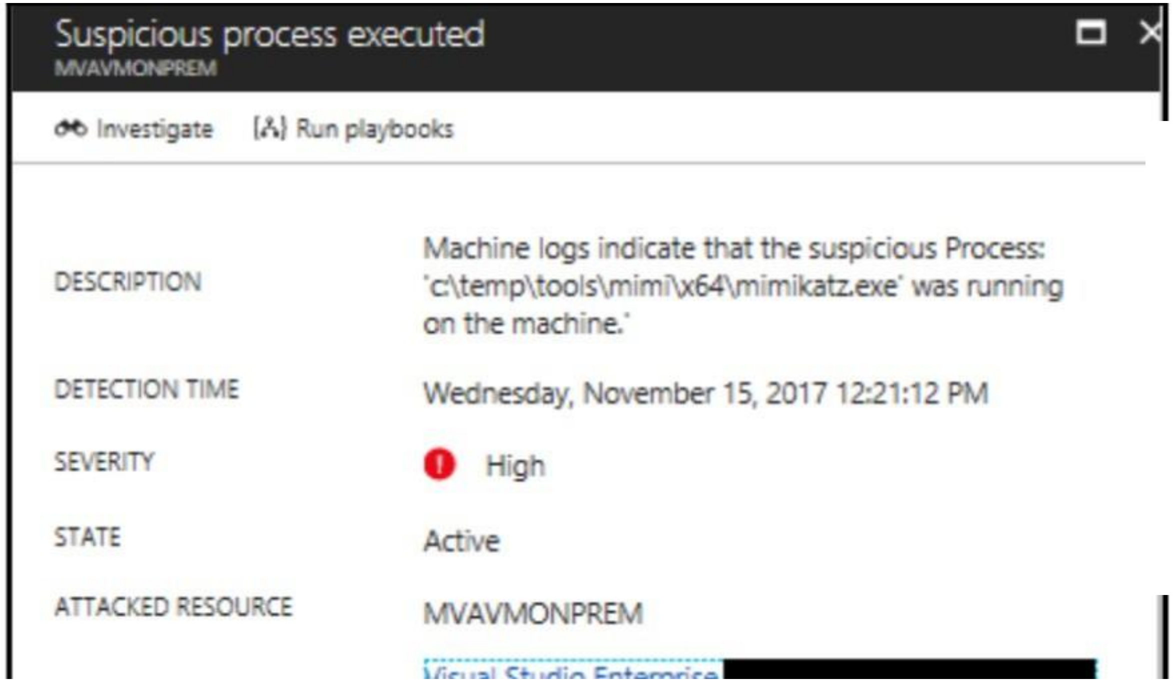
- Compromised by phishing email – Cloud version
  - ✓ In this hybrid scenario, the compromised system is located on-premises and the company has a cloud-based monitoring system.
  - ✓ Again, a user received a phishing email, clicked on the hyperlink, and got compromised.
  - ✓ **The difference now is that there is an active sensor monitoring the system**, which will **trigger an alert to SecOps**, and **the user will be contacted.** The **users don't need to wait days to realize they were compromised;** the response is faster and more accurate.
  - ✓ The **example of the active sensor is Azure Security Center** and four events were recorded.



DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE	SEVERITY
Antimalware Action Taken	4	11/14/17 04:29 PM	MVAVMONPrem	Low
Suspicious process name detected	2	11/15/17 12:21 PM	MVAVMONPrem	Medium
Suspicious Process Execution Activity Detected	1	11/15/17 12:21 PM	MVAVMONPrem	Medium
Suspicious process executed	3	11/15/17 12:21 PM	MVAVMONPrem	High

- Although the antimalware software captured the malware, the attacker kept going and succeeded as the last three events show.
- The last three events are related to the serious mimikatz process.

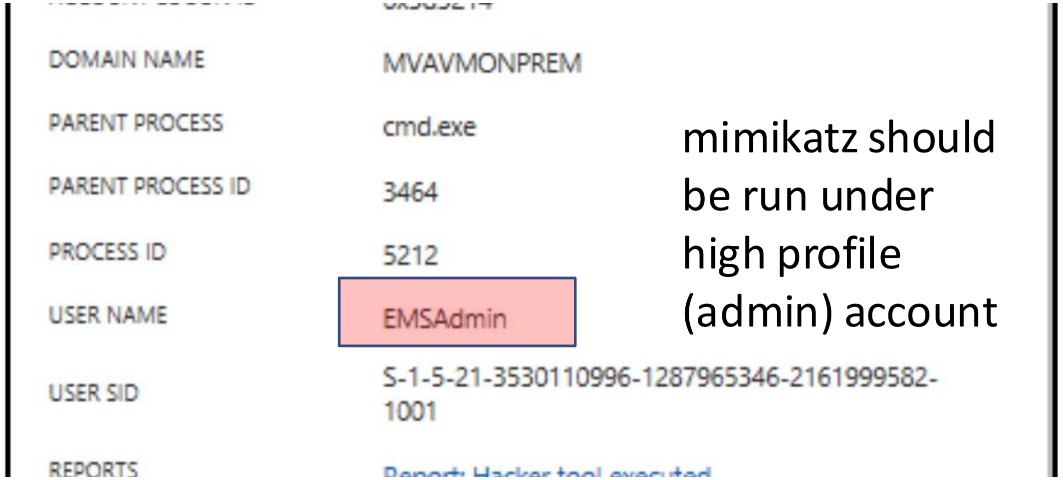
- The following figure shows the mimikatz process, which was executed.



Suspicious process executed

MVAVMONPREM

DESCRIPTION	Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe' was running on the machine.'
DETECTION TIME	Wednesday, November 15, 2017 12:21:12 PM
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	MVAVMONPREM
	Visual Studio Enterprise [redacted]



DOMAIN NAME	MVAVMONPREM
PARENT PROCESS	cmd.exe
PARENT PROCESS ID	3464
PROCESS ID	5212
USER NAME	EMSAdmin
USER SID	S-1-5-21-3530110996-1287965346-2161999582-1001
REPORTS	Report: Hacker tool executed

mimikatz should be run under high profile (admin) account

SEARCH AND YOU SHALL FIND IT

- **In a real-world scenario**, the **amount of data that gets collected by sensors and monitoring systems can be overwhelming.**
  - ✓ A **security monitoring system that can aggregate all these logs, digest them, and rationalize the result.**
  - ✓ **You also need searching capabilities to be able to keep digging up more important information.**
  - ✓ It is **important to be used to those search capability of the platform that you are using and familiar with commands to further analysis.**
  - ✓ Also, the **platform should provide efficient visualizing and searching interfaces**.

LESSONS LEARNED

- Every time an incident comes to its closure,
  - ✓ Each step that was done during the investigation should be documented.
  - ✓ Key aspects of the investigation that need to be either reviewed to improve or fix should be identified.
- The lessons learned are crucial for the continuous improvement of the process and to avoid making the same mistakes again.
- the Blue Team should create an extensive report to document the lessons learned and how this will be used to improve the defense controls.

- Lessons learned from the examples: Attacks against a user's credential are a growing threat and the solution is not based on a silver bullet product, instead, it is a combination of tasks, such as:
  - ✓ Reducing the number of administrative level accounts and eliminating administrative accounts in local computers. (Regular users shouldn't be administrators on their own workstation.)
  - ✓ Using multifactor authentication as much as possible. Adjusting the organization’s security policies to restrict login rights.
  - ✓ Having a plan to periodically reset the Kerberos TGT (KRBTGT) account. This account is used to perform a golden ticket attack.

RECOVERY PROCESS

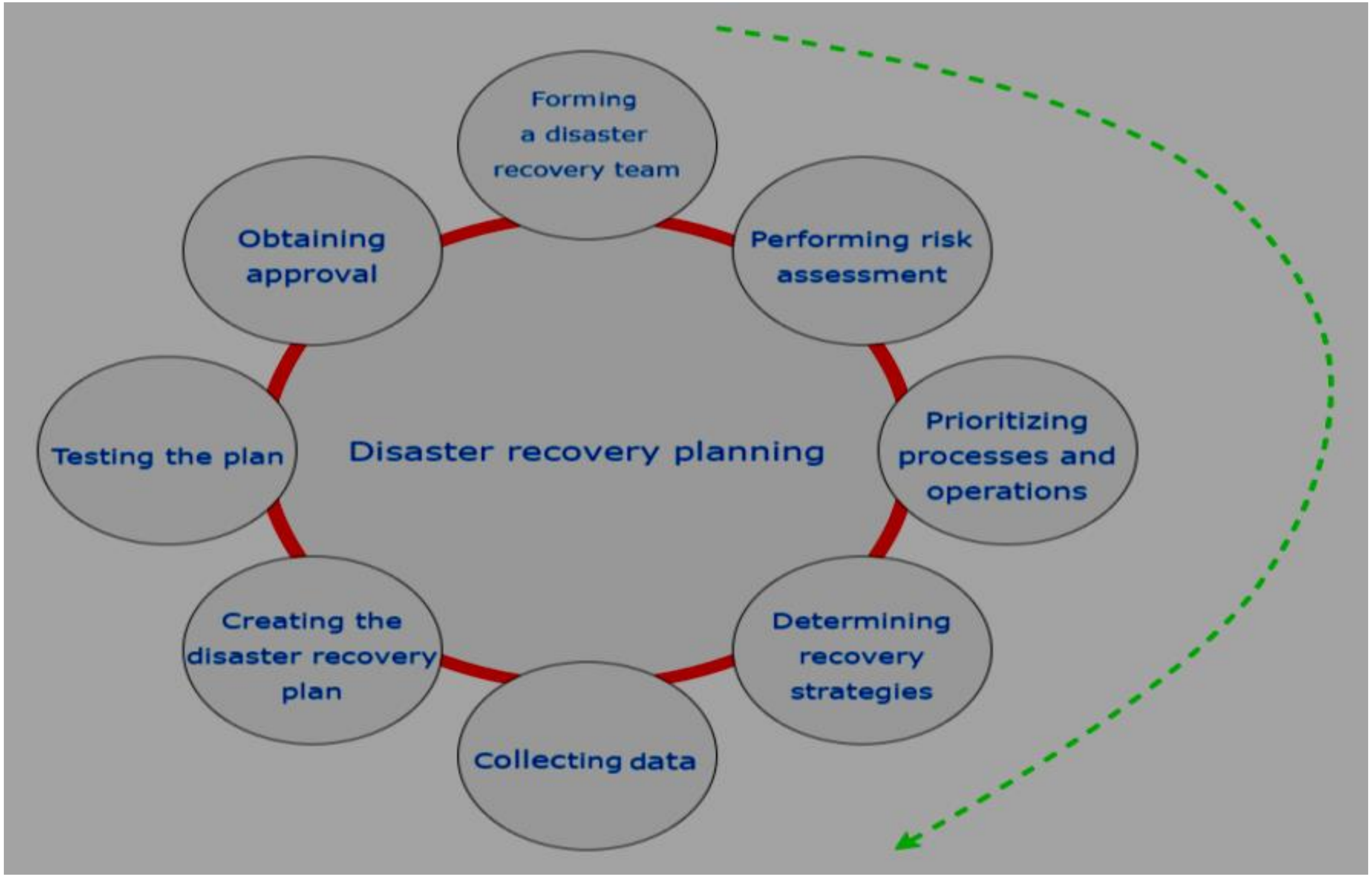
- The recovery process refers to how an organization deals with disruptions to its IT infrastructure, which may be caused by both natural and man-made disasters.
- Natural disasters include events like earthquakes, floods, and hurricanes, while man-made disasters may include cyberattacks, power surges, and accidental damages.
- Organizations must have well-planned disaster recovery mechanisms to survive and recover from these events.
- Key Elements of Recovery Process:
  - ✓ **Disaster Recovery Plan:** A documented set of procedures to recover IT infrastructure.
  - ✓ **Live Recovery:** Recovering systems that are still in use without taking them offline.
  - ✓ **Contingency Plan:** Interim measures to reduce the impact of failures and facilitate quick recovery.

DISASTER RECOVERY PLAN

- The disaster recovery plan **is a documented set of processes** and **procedures** that are carried out in **the effort to recover the IT infrastructure in the event of a disaster.**
- Because of many organizations' dependency on IT, it has become **mandatory** for organizations to have a **comprehensive and well-formulated disaster recovery plan**.
- **Organizations are not able to avoid all disasters**; the best they can do is plan ahead how they will recover when disasters happen.
- The **objective** of the plan is **to protect the continuity of business operations** when IT operations have been partially or fully stopped.

- **There are several benefits of having a sound disaster recovery plan:**
  - ✓ The **organization has a sense of security**. The recovery plan assures it of its continued ability to function in the face of a disaster.
  - ✓ The organization **reduces delays in the recovery process**. Without a sound plan, it is easy for the disaster recovery process to be done in an uncoordinated way, thereby leading to needless delays.
  - ✓ There is **guaranteed reliability of standby systems**. A part of the disaster recovery plan is to restore business operations using standby systems. The plan ensures that these systems are always prepped and ready to take over during disasters.
  - ✓ The **provision of a standard test plan** for all business operations.
  - ✓ The **minimization of the time taken to make decisions** during disasters.
  - ✓ The **mitigation of legal liabilities** that the organization could develop during a disaster.

The disaster recovery planning process


Forming a disaster recovery team
Performing risk assessment
Prioritizing processes and operations
Determining recovery strategies
Collecting data
Creating the disaster recovery plan
Testing the plan
Obtaining approval
Disaster recovery planning

The disaster recovery planning process

The disaster recovery plan (DRP) outlines the steps that an organization takes to restore IT infrastructure after a disaster. The planning process includes several critical steps.

Steps in the Disaster Recovery Planning Process:

- **Forming a Disaster Recovery Team:** This team should include representatives from all departments and top management. Their responsibility is to assist in recovery operations and oversee the creation and implementation of the plan.
- **Performing Risk Assessment:** The disaster recovery team identifies risks that could impact the organization’s operations, especially those tied to IT infrastructure. Both natural and man-made risks are considered.

- **Prioritizing Processes and Operations:** This involves identifying critical operations that need to be prioritized during a disaster. Since resources may be limited, it is essential to focus on critical systems that support the business. Operations are ranked based on priority levels: essential, important, and non-essential.
- **Determining Recovery Strategies:** Practical strategies to restore operations are created at this stage. The strategies should cover all aspects of the organization’s IT systems, such as hardware, software, databases, and customer services.
- **Collecting Data:** The disaster recovery team collects and documents critical information, such as contact lists, backup schedules, hardware/software inventories, and communication protocols.

- **Creating the Disaster Recovery Plan:** Using the information from previous steps, the team creates a comprehensive and practical disaster recovery plan. This plan should clearly detail the actions required to restore operations.
- **Testing the Plan:** The disaster recovery plan must be tested regularly using methods such as simulations and full-interruption tests. Testing ensures that the plan is effective and reveals any weaknesses.
- **Obtaining Approval:** Once the plan is tested, it must be approved by top management to ensure it aligns with the organization’s policies and goals.
- ·**Maintaining the Plan:** The recovery plan should be regularly updated to reflect changes in the organization’s IT infrastructure or new threats. The plan should be dynamic and adaptable to ensure it remains relevant.

- While disaster recovery planning is essential, organizations face several challenges that can affect the success of the recovery process.
- **Key Challenges:**
  - ✓ **Lack of Top Management Support:** Disaster recovery plans may be viewed as **unnecessary drills for hypothetical events that are unlikely to occur**. As a result, they may not receive sufficient support or funding from management.
  - ✓ **Inaccurate Recovery Time Objectives (RTOs):** RTOs determine the **acceptable downtime for an organization.** It can be difficult for the disaster recovery team to create a plan that meets the RTO while also being cost-effective.
  - ✓ **Outdated Plans:** The **IT threat landscape is constantly changing**, and a disaster recovery plan can become outdated quickly. Organizations must continuously update their plans to account for new threats.

LIVE RECOVERY

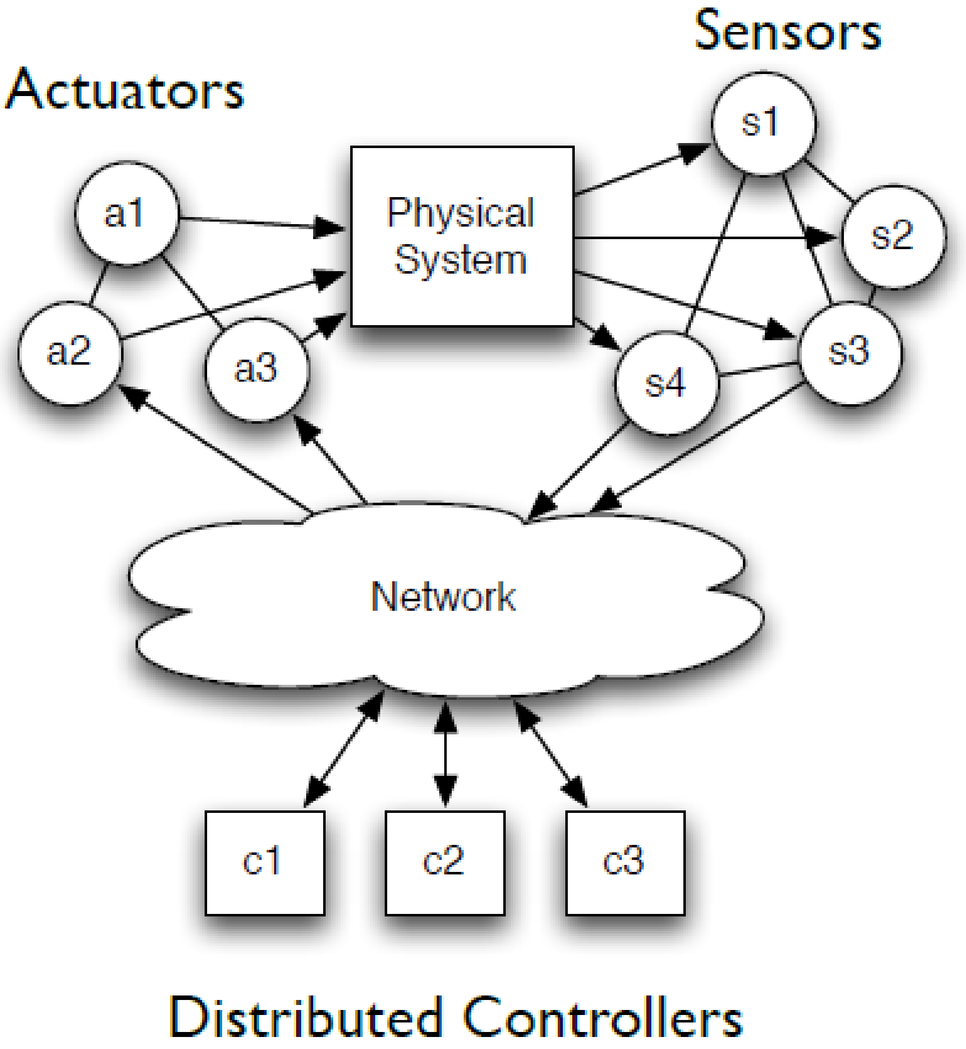
- Live recovery involves **restoring systems that are still in use without taking them offline**.
- There are two primary types of live recovery:
  - ✓ **System Replacement:** Installing a clean system over the faulty one without taking the system offline.
  - ✓ **Data Recovery Tools:** Using tools to restore data and configurations without affecting the overall system.
- A common example of live recovery is using a Linux live CD to recover a Windows system.

CONTINGENCY PLANNING

- Contingency planning is **essential for maintaining operations when critical systems fail**. It involves **identifying potential risks and setting up recovery mechanisms to minimize damage.**
- Key elements of contingency planning include:
  - ✓ **Identifying risks:** Natural and man-made threats.
  - ✓ **Developing recovery strategies:** Creating plans to recover IT infrastructure.
  - ✓ **Maintaining backup systems:** Ensuring offsite or cloud backups are available for quick recovery.

CYBER-PHYSICAL SYSTEMS

- **Definition:** Cyber-Physical Systems (CPSs) are systems that integrate computational elements (**software, hardware, and networking**) with **physical processes, enabling real-time monitoring and control of physical entities**. These systems are designed to interact with the physical environment, collect data, and use that data to influence the physical processes through actuators and controllers.
- **Key Applications:** CPSs are widely used across various sectors:
  - ✓ **Healthcare**: Medical devices such as insulin pumps and pacemakers.
  - ✓ **Energy**: Smart grids and power distribution systems.
  - ✓ **Transportation**: Autonomous vehicles and intelligent transportation systems.
  - ✓ **Industrial Control Systems (ICS)**: Factories, refineries, and production facilities, where machines interact with their environment using CPS.



General architecture of cyber-physical systems

- Components:
  - ✓ **Sensors**: Gather data from the environment (**e.g., temperature, pressure, or motion**).
  - ✓ **Actuators**: Perform physical actions based on commands from controllers (e.g.**, open valves, adjust motors**).
  - ✓ **Controllers**: Process data from sensors and send control signals to actuators to **maintain system stability**.
  - ✓ **Communication Networks**: Allow for **data transmission between sensors, actuators, and controllers**. These are often IP-based but can also include legacy protocols.

CHARACTERISTICS OF CYBER-PHYSICAL SYSTEMS

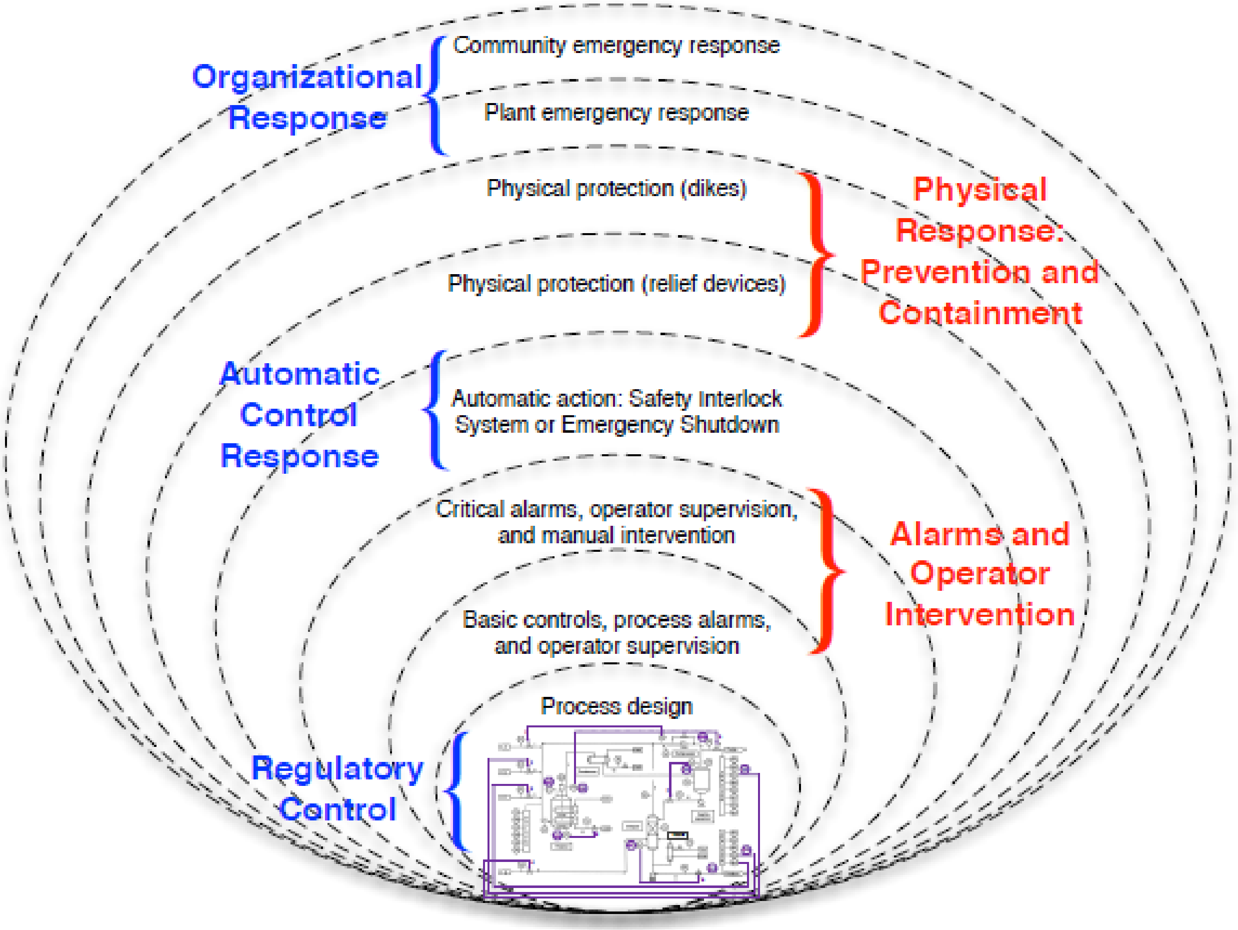
- **Embedded Systems-** CPS devices are resource-constrained
- **Real-Time Systems-** CPSs must operate in real-time
- **Networking Protocols-** Many CPSs use IP-based protocols for communication
- **Wireless Communications-** Wireless networks are also common in CPSs
- **Control Systems-** CPSs rely on feedback control loops to monitor physical processes
- **Cyber Risks** - integration of CPSs with networked systems, especially IP networks, exposes them to the same cyber threats that affect traditional IT systems
- **Physical Risks-** Since CPSs control physical processes, any compromise in the cyber domain can directly affect the physical world, causing damage or failure.

RISKS IN CYBER-PHYSICAL SYSTEMS

- **Consequences of CPS Attacks:**
  - ✓ **Power Grids**: Blackouts could lead to **disruptions in other critical system**s, including communication networks and hospitals.
  - ✓ **Transportation Systems**: **Autonomous vehicle hacking could lead to accidents**, endangering passengers and pedestrians.
  - ✓ **Medical Devices**: **Attacks on devices like insulin pumps or pacemakers can lead to fatal consequences for patients.**

PRPROTECTIONS AGAINST NATURAL EVENTS AND ACCIDENTS

- Failures in control equipment in Cyber-Physical Systems (CPSs) can lead to **significant damage to people, the environment**, and other infrastructures.
- To address this, engineers have developed several mechanisms to protect these systems from accidents and natural failures.
- However, these mechanisms are not always sufficient to protect against cyber-attacks.



Organizational Response
Community emergency response
Plant emergency response
Physical protection (dikes)
Physical protection (relief devices)
Physical Response: Prevention and Containment
Automatic Control Response
Automatic action: Safety Interlock System or Emergency Shutdown
Critical alarms, operator supervision, and manual intervention
Basic controls, process alarms, and operator supervision
Alarms and Operator Intervention
Process design
Regulatory Control

Layers of protection for safety-critical ICS.

Layers of protection for safety-critical ICS (Industrial Control Systems (ICS).

Example : Pipeline Management and Control Systems- Used in oil and gas pipelines, transporting crude oil, natural gas, or refined products across long distances.

1. Process Design and Basic Controls

-Basic controls manage **normal operations**, with algorithms and systems automatically adjusting the physical environment based on data from sensors. **Process alarms and operator supervision** when normal operation deviates.

2. Safety Instrumented Systems (SIS) and Emergency Shutdown

- If a sensor detects high pressure in a system, the SIS can automatically close a valve to prevent a rupture.

3. Physical Protections

- physical protection mechanisms are deployed to prevent or contain accidents.

4. Fault Tolerance, Reliability, and Robust Control

- CPSs are designed for reliability and fault tolerance

5. Organizational and Community Response

- If an **accident escalates beyond the control of automated and physical protections**, emergency response protocols are activated.

Limitations of Protections for Cyber-Security

- While these protections are **effective against natural events and accidents, they are not always enough to safeguard against cyber-attacks.** Traditional safety mechanisms assume failures will occur independently and non-maliciously, which makes them vulnerable to attackers who can bypass or exploit these protections.

Examples of limitations:

- **Attackers can inject false data into sensors**, making the system believe everything is normal when, in fact, it's heading toward failure.
- Fault-detection systems, which are designed to detect natural failures, can be bypassed if **attackers inject data that mimics a plausible but incorrect system state**.
- **Stuxne**t, for example, **manipulated safety systems in a nuclear facility to cause physical damage while keeping the operators unaware** of the issue.

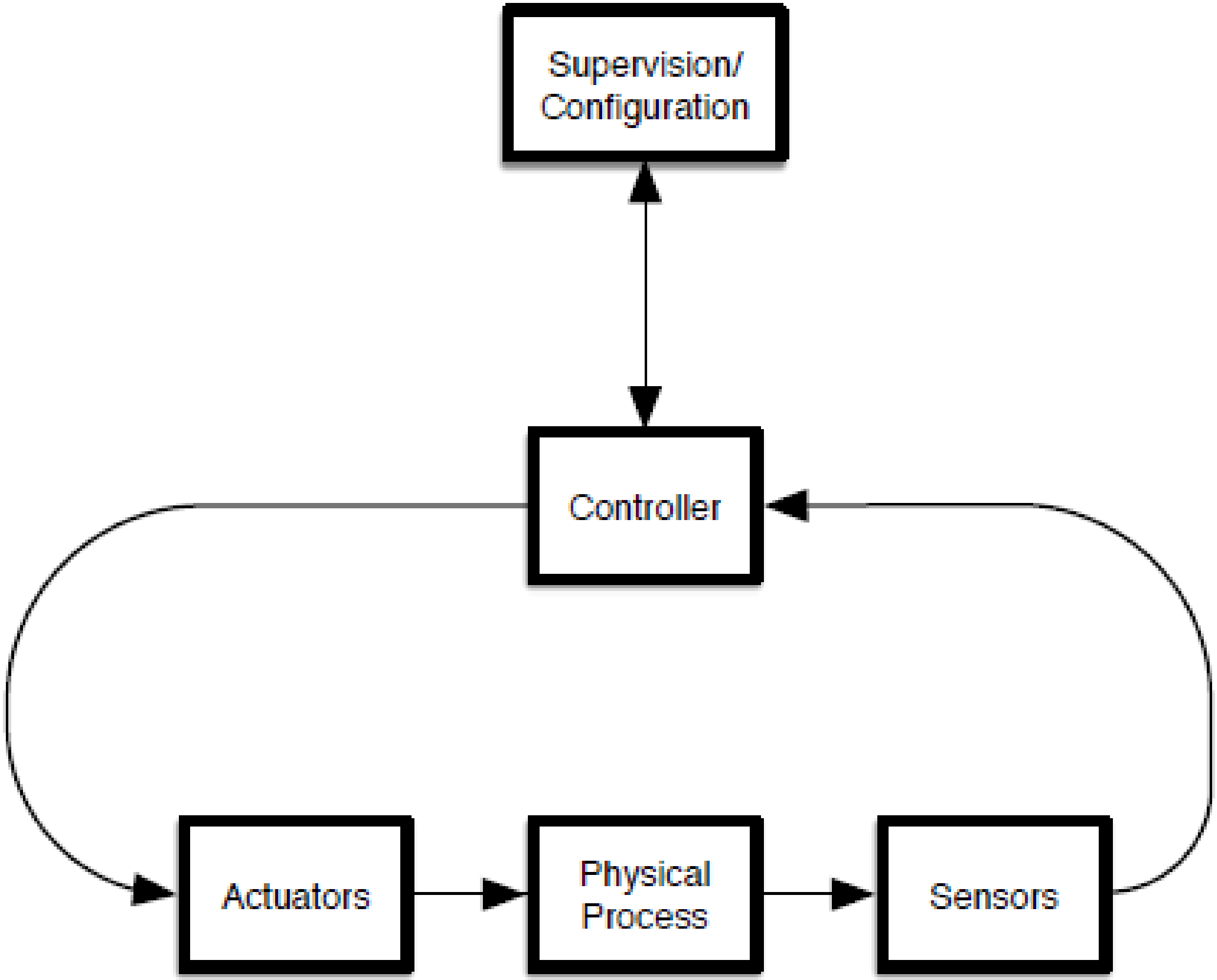
Safety vs. Security Tensions

Safety : focuses on protecting people, the environment, and assets from harm or hazards arising from system failures, process malfunctions, or unintended operational conditions. In ICS, safety aims to ensure that processes run within safe limits to prevent accidents.

Security: focuses on protecting systems, networks, and data from malicious threats, unauthorized access, and attacks that could disrupt or compromise operations. In ICS, security aims to prevent, detect, and respond to intentional cyber threats.

- Adding security mechanisms to a CPS can sometimes conflict with safety requirements. For example:
  - ✓ A **software patch intended to fix a vulnerability might require a system reboot**, **temporarily shutting down critical safety functions**.
  - ✓ **Preventing unauthorized access could also delay first responders in accessing systems during emergencies**, such as medical devices.
- Thus, designers of CPSs must carefully **balance safety and security** to ensure systems remain functional and safe while also being protected from cyber threats.

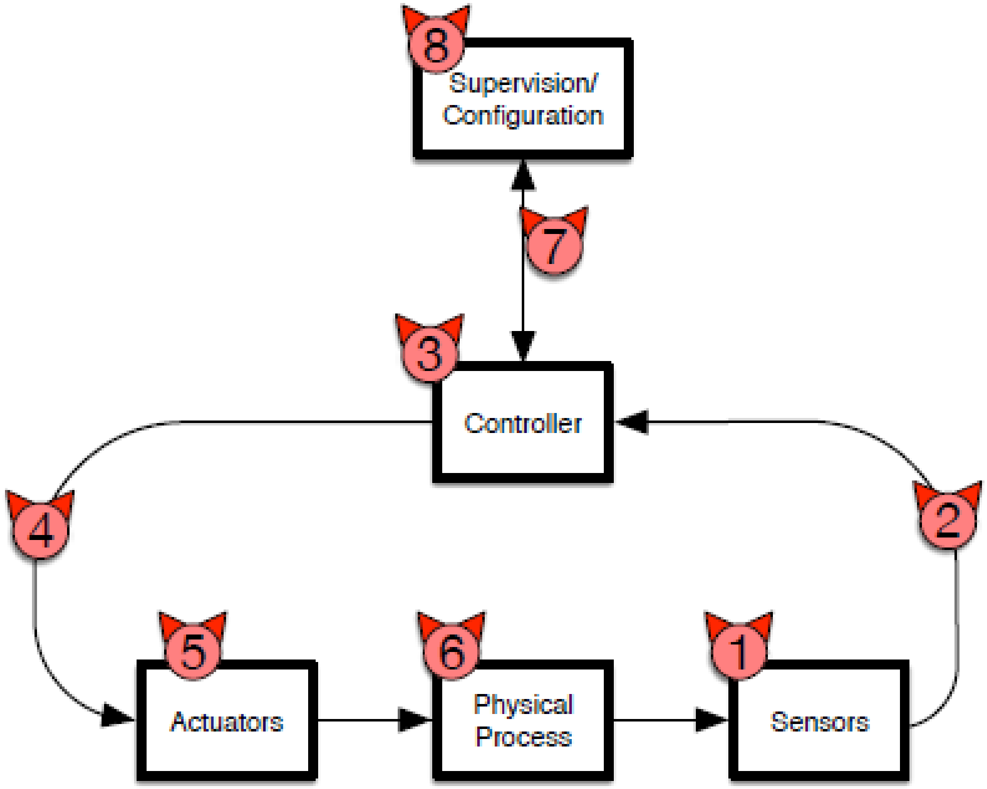
- CPSs face unique security and privacy challenges that extend beyond the conventional concerns of IT systems.
- **Security Concerns:**
  - ✓ **CPSs can be attacked at any point in the system architecture**, leading to cascading failures across both cyber and physical domains.
  - ✓ Attack Vectors:
    - ➢ **Sensors**: **Attackers can inject false data into sensors**, causing the system to make incorrect decisions based on faulty data.
    - ➢ **Controllers**: **Malicious actors can compromise controllers** to issue unsafe commands to actuators.
    - ➢ **Networks**: **Communication paths** between sensors, controllers, and actuators are **vulnerable to disruption through denial-of-service or man-in-the-middle attacks**.



General Architecture of a CPS.

Attacks Against CPSs

- CPSs are vulnerable to several forms of cyber-attacks that can exploit different parts of the system architecture.



Attack Points in a CPS.

Common attack points in CPSs include:

1. **Sensor Compromise:** Attackers inject false data, causing the system to make incorrect adjustments (e.g., tampering with temperature readings in an industrial plant).
2. **Network Disruption:** Denial-of-service attacks prevent data from reaching controllers, causing systems to operate on outdated information.
3. **Controller Compromise:** Controllers can be hacked to send malicious commands to actuators, leading to dangerous physical consequences (e.g., Stuxnet altered commands to cause centrifuges to spin at unsafe speeds).
4. **Actuator Tampering:** Compromising actuators can result in them performing unintended actions, which can have direct physical effects (e.g., shutting down a power plant's cooling system).

Transduction Attacks: **These attacks exploit physical properties to manipulate sensors without directly hacking them**. For instance, attackers could **use sound waves to interfere with a drone's gyroscope, causing it to lose stability.**

Privacy Concerns:

- CPS devices collect vast amounts of data related to physical processes, often without user awareness. **This data includes sensitive personal information** such as:
  - ✓ **Driving Habits:** Collected by connected vehicles.
  - ✓ **Health Data:** Collected by medical devices like pacemakers or smartwatches.
  - ✓ **Energy Consumption:** Recorded by smart meters in homes and businesses.
- **Risks of Surveillance:** The **data collected by CPSs can be used for surveillance or criminal targeting**. For example, driving data collected by vehicles could be accessed by hackers or even law enforcement agencies without user consent.

High-Profile, Real-World Attacks Against CPSs

- Several high-profile attacks on CPSs illustrate the potential for widespread disruption and physical damage:
  - ✓ **Stuxnet (2010): This worm targeted Iran's nuclear enrichment facilities by manipulating the control systems of centrifuges, causing them to spin at unsafe speeds**. Stuxnet was a sophisticated, state-sponsored attack that introduced a new era of cyber warfare.
  - ✓ **Ukrainian Power Grid Attacks (2015 and 2016): In 2015, attackers gained remote access to SCADA systems in Ukraine's power grid, causing widespread blackouts.** The 2016 attack was more automated, using the **Industroyer malware**, which directly exploited vulnerabilities in industrial control protocols.
  - ✓ **Triton (2017):** Triton targeted the safety systems of an industrial plant, specifically aiming at the safety instrumented systems (SIS). This **attack demonstrated the intent to cause physical damage and potentially harm lives by disabling critical safety mechanisms**.