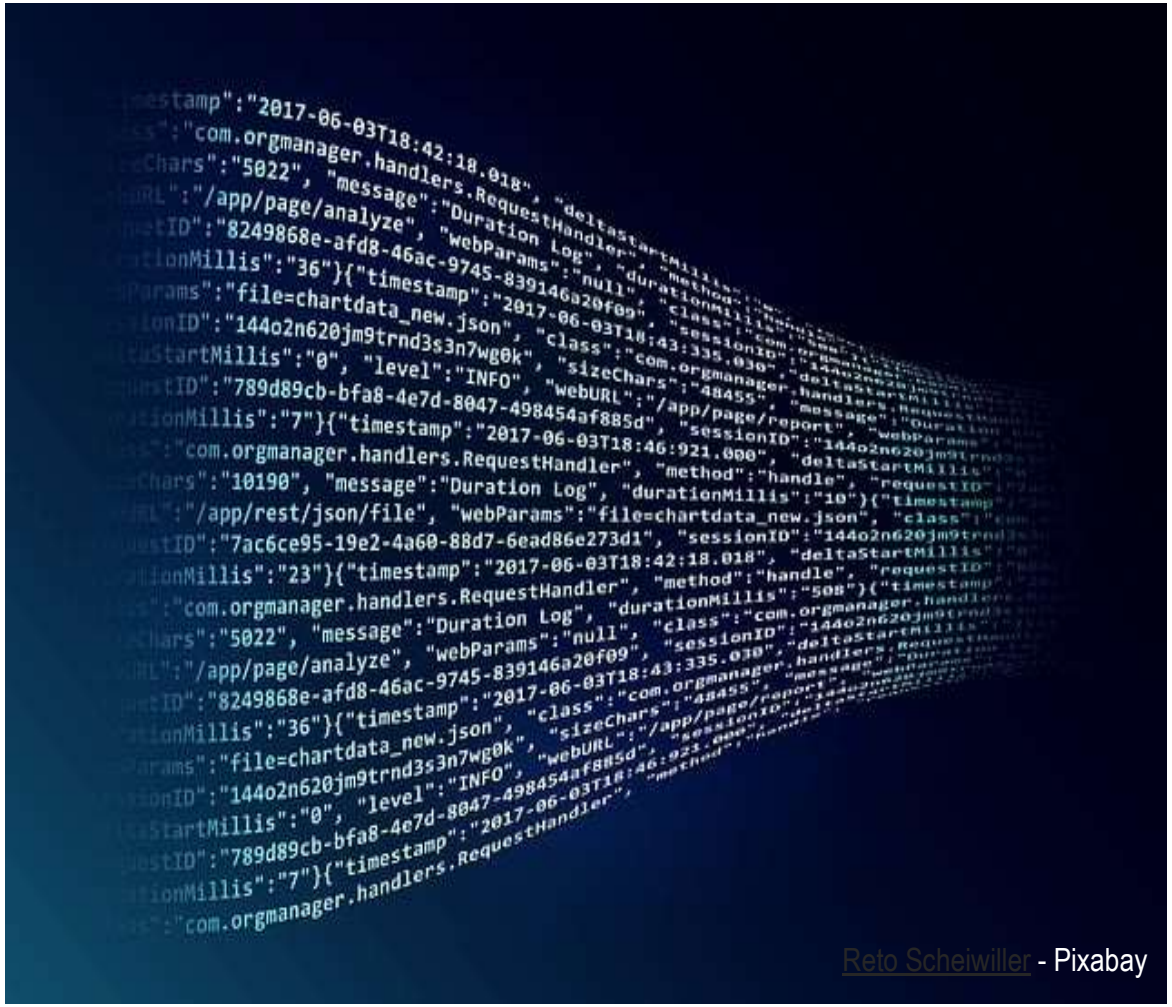
LASW - Latin American STAMP Workshop 2024

Using Active STPA in Cybersecurity Data Analysis

André Yoshimi Kusumoto, PhD student - kusumoto@ita.br
Carlos Henrique Netto Lahoz, PhD - carloslahoz@univap.br

Introduction

- Data is the most critical asset for RD&I organizations in the aerospace industry
- It must be protected from unauthorized access.
- In a project, data is usually generated and collected at practically every stage of the development.
  - Verification tests, simulations, proofs of concept or data acquisition.
- It is necessary to define a cybersecurity policy to ensure that data is properly stored, protected and only available by authorized users.



CSAM (CyberSecurity Asset Management)

- At first, identify the infrastructure that supports data storage and which should be protected as a priority.
  - Sensitive data, Firewall, Data Storages, Switches and others
- Cybersecurity Framework (NIST) [1]
  - Identify Function emphasizes the importance of defining which processes, systems, data, resources, and assets are critical to the business.
- NIST Special Publication 1800-5 - National Cybersecurity Center of Excellence (NCCoE) [2]
  - Can be used for monitoring and managing physical and logical IT assets (Guide)

Zero Trust

- Perimeter security model is no longer adequate to meet cybersecurity requirements and support business demands [3].
  - Malicious attacks originating from within the organization (i.e., lateral movement)
- It is assumed that every access requests are considered unreliable

Zero Trust

"*Never trust, always verify*" [6]

Monitoring

Network traffic monitored

Access requests classified with PoLP (Principle of Least Privilege)

Large volume of data

Different sources

It must be processed in real time

Identify potential attack attempts or unusual behavior

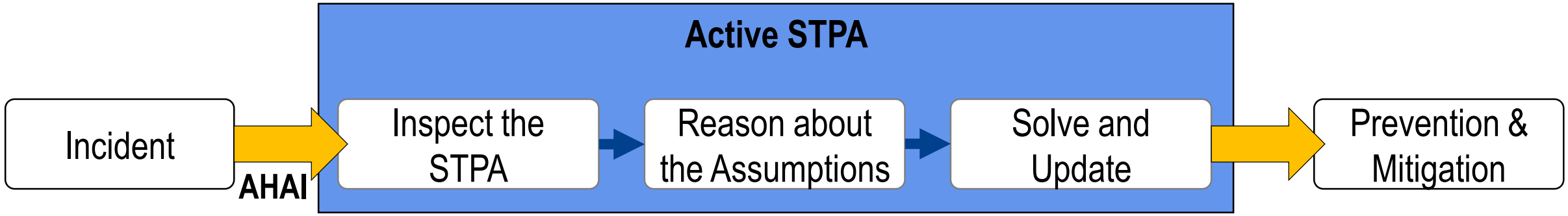
Artificial Intelligence

- Machine Learning (ML) techniques may be necessary.
  - Ex. Natural Language Processing (NLP) can be used to recognize patterns in reports forwarding by IT Team or Blue Team.
  - Results may indicate that the resource may become the next target of a cyberattack.
- The processed data will serve as a data source for feedback in the entire system, resulting in the reassessment of assumptions.

Gerd Altmann por Pixabay

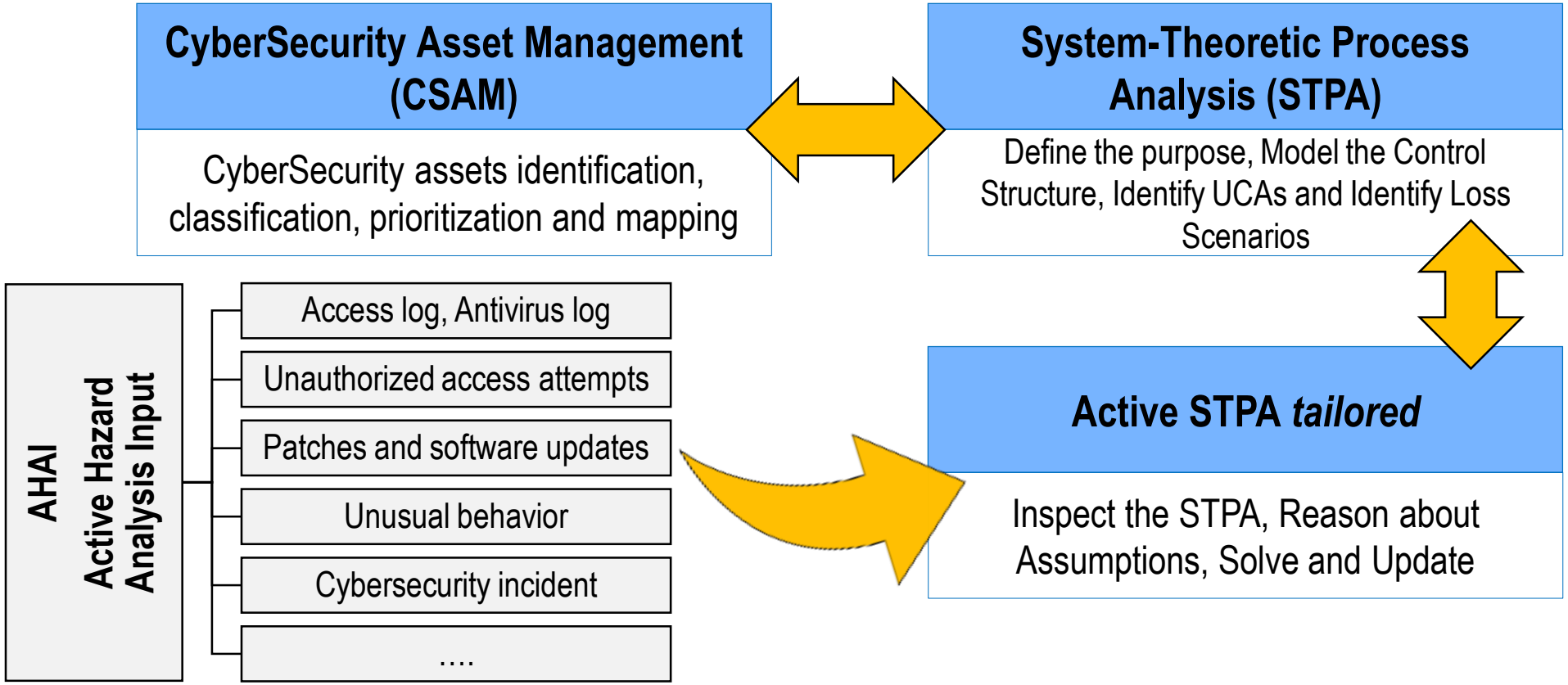
Active STPA

- Recursive approach for hazards analysis based on STPA (Systems-Theoretic Process Analysis) [4].
- Uses collected data as inputs to identify indicators that may increase defined hazards.
- It is possible to use an existing STPA or create one.
- From one or more AHAI (Active Hazard Analysis Input), a Safety Analyst (SafeA) defines whether updating the hazard analysis is necessary [4].



Phases of Active STPA [4]

Active STPA for Cybersecurity Data Analysis



Systems Engineering concepts applied to cybersecurity analysis in aerospace RD&I organizations, using the Active STPA tailored.

Active STPA for Cybersecurity Data Analysis

CSAM (CyberSecurity Asset Management)

- Identification, classification, prioritization and mapping

1. Storage Servers
2. Corporate Firewall
3. Switches and Routers

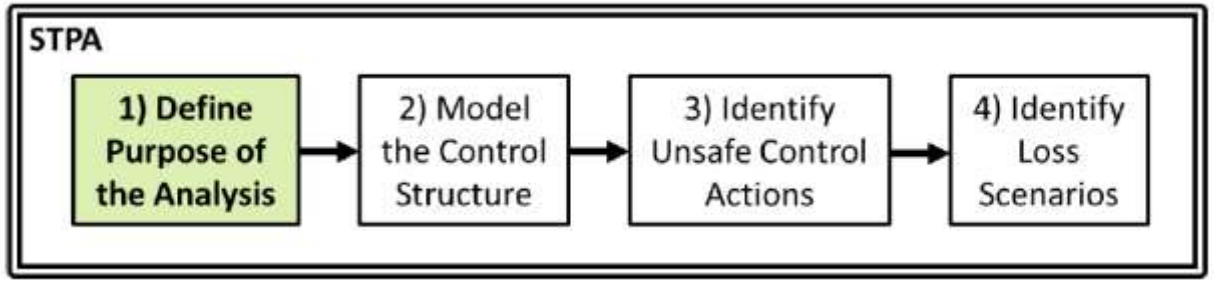
Resources

- User clients
- IT Team
- Blue Team

Active STPA for Cybersecurity Data Analysis

To apply the **Active STPA**, the organization needs to [4]:

1. Create an original STPA or use an existing one
2. Implement the controls recommended by the STPA
3. Collect operational data
4. Run the Active STPA



STPA Method [5]

The **Blue Team (BT)** will be responsible for generating the STPA.

Purpose of the Analysis could be defined as

"Identify possible vulnerabilities and insecure relationships in the manipulation of sensitive data in aerospace RD&I organizations".

Active STPA for Cybersecurity Data Analysis

Identify Losses

L1 - Organization's Reputation
- Image of an outdated institution
- Institution that does not prioritize security
- Executives lacks motivation for information security investments.
- Demonstrates lack of knowledge regarding the laws and contracts that must be followed
- Institution that does not invest in training its team

L2 - Relevant Information
- Loss of test data of new aerospace systems
- Loss of data acquired from tests contracted by external organizations
- Test reports copied and publicly disclosed on the internet
- Deficiencies or limitations data of military equipment
- Attack or defense limitations of military systems
- Loss of personal data of the team involved in tests
- Loss of data on aircraft used in tests
- Unreliable data due to system invasion

L3 - Material Resources
- Loss of aircraft during flight tests
- Loss of material under development
- Loss of aerospace systems under development
- Loss of sensors used in tests

L4 - Human Resources
- Loss of crew involved in flight tests
- Loss of aircraft mechanics during maintenance
- Stress and anxiety due to problems generated by cyber attacks
- Difficulty in decision-making that can lead to internal discussions due to instability and lack of data credibility

L5 - Delay in the development of new projects
- Loss of contracts due to delay
- Payment of penalties for non-compliance with deadlines.

Active STPA for Cybersecurity Data Analysis

Identify system-level hazards

H1 - Web Systems Developed without Security Requirements [All losses]

H1.1 - Systems developed in an insecure environment [L2, L3, L4, L5]
H1.2 - Systems developed using outdated tools [L2, L3, L4, L5]
H1.3 - Systems developed without receiving security updates [L2, L3, L4, L5]
H1.4 - Systems developed using outdated external modules [L2, L3, L4, L5]

H2 - Software or modules out of date [All losses]

H2.1 - Outdated software [L2, L3, L4, L5]
H2.2 - Software dependent on unsupported legacy platforms [L2, L3, L4, L5]
H2.3 - Software using outdated external modules [L2, L3, L4, L5]

H3 - Access of external elements to sensitive data [L2, L3]

H3.1 - Use of aircraft technical data for attacks [L2, L3]
H3.2 - Use of test results in unauthorized projects (i.e., Espionage) [L2]
H3.3 - Use of data about weapon limitations [L2, L3]

H4 - Hardware out of date [L2, L3]

H4.1 - Use of security policies that disallow equipment updates [L3]
H4.2 - Updating equipment that may result in system deactivation due to incompatibilities. [L3]
H4.3 - During equipment acquisition, not including contract items that cover necessary hardware updates [L3]
H4.4 - Hardware with outdated configurations [L2, L3]

H5 - Invasion of Devices and Systems [L1, L2, L3, L4]

H5.1 - Use of weak passwords in system access accounts [L2, L3]
H5.2 - Lack of security updates provided by the manufacturer [L2, L3]
H5.3 - Devices and systems providing unreliable or incorrect information [L2]

H6 - Devices Without Connectivity [L1, L2, L5]

H6.1 - Switches/Routers without connectivity [L1, L2, L5]
H6.2 - Corporate Firewall without connectivity [L1, L2, L5]
H6.3 - Application Servers without access [L1, L2, L5]

H7 - Power Outage [L1, L2, L5]

H7.1 - Unexpected power outages [L1, L2, L5]

Active STPA for Cybersecurity Data Analysis

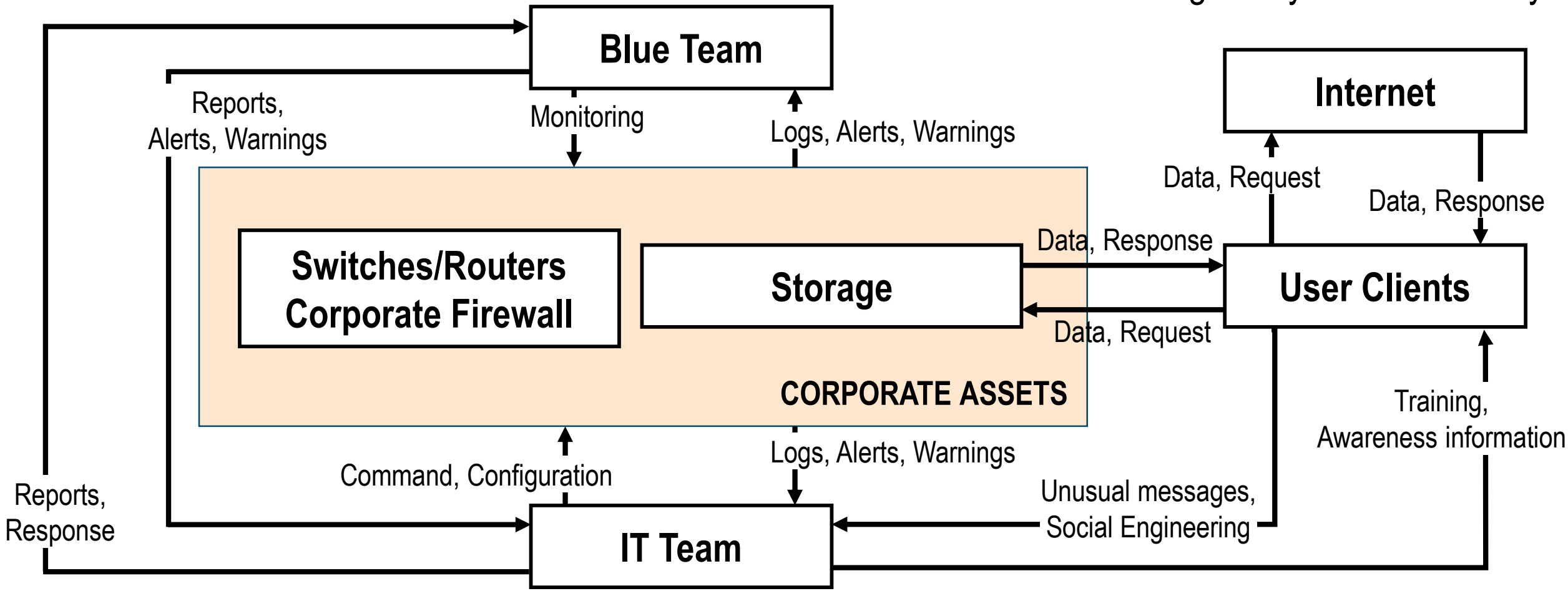
Deriving a list of System-level Constraints (SC) and System-level Requirements (SR)

- SC-1 - Acquisition of equipment with technical support (e.g., software/firmware updates) specified in the contract [H4].
- SC-2 - Acquisition of equipment with an extended warranty and immediate replacement or as quickly as possible [H6].
- SC-3 - Establish an Information Security Policy that defines the rules and procedures for handling and processing sensitive data, as well as the responsibility of those handling the data [H3]
- SR-1 – Use best practices of security development [H1].
- SR-2 – The software development life cycle should include system maintenance stages that ensure its cybersecurity [H2].
- SR-3 – Implement data links with redundancy [H6].
- SR-4 – Ensure redundancy of power sources such as electrical generators [H7].

Active STPA for Cybersecurity Data Analysis

Model of Control Structure

Defining the system's boundary



Identify Unsafe Control Actions (UCAs)

Control Action	Not Provided causes hazards	Provided leads to hazard	Provided too early, too soon or out of order	Continuous actions provided for too long or stopped too soon
Monitoring	UCA-01 - The Blue Team does not analyze the logs, alerts and warnings provided from devices [H4,H5,H6]	UCA-02 - The Blue Team does not performs real-time monitoring [H3,H5, H6, H7]	UCA-03 - The Blue Team conducts a threat analysis long after the initial incident has taken place [H3,H5,H6]	
Logs, Alerts, Warnings	UCA-04 - Devices do not provide any logs, alerts or warnings [H4,H6]	UCA-05 - Devices provide unreliable information [H5] UCA-06 - Devices provide too much information [H5]	UCA-07 - Devices provide logs, alerts or warnings after the incidents [H4,H5,H6]	UCA-08 - Devices show a lot of useless alerts [H2,H4,H5]
Reports, Alerts, Warnings	UCA-09 - The Blue does not provide reports, alerts and warning [H1]	UCA-10 - The Blue Team provides unreliable information [H1,H2]	UCA-11 - The Blue Team provides reports only after the incidents [H7]	
Commands, Configuration	UCA-12 - The IT Team does not configure properly the switches/routers or the corporate firewall [H5] UCA-13 - The IT Team does not execute the logs, Alerts and Warning analysis [H5,H6,H7].	UCA-14 - The IT member uses a non-admin account to access the admin site of switches/routers or corporate firewall [H5] UCA-15 - The IT Team performs the update without a impact analysis [H4]	UCA-16 - The IT member uses an old procedure to configure the switches/routers or corporate firewall [H5] UCA-17 - The IT Team performs the update too late [H4]	UCA-18 - The IT Team does not update the configuration of switches/routers or corporate firewall [H4]

Active STPA for Cybersecurity Data Analysis

Identify Unsafe Control Actions (UCAs)

Control Action	Not Provided causes hazards	Provided leads to hazard	Provided too early, too soon or out of order	Continuous actions provided for too long or stopped too soon
Data, Requests	UCA-19 - The User Clients do not verify if destination is correct [H1,H2] UCA-20 - The User Clients do not use a business security solution (i.e. antivirus application) [H1,H2] UCA-21 - The User Clients do not use a encryption algorithm to protect the message [H1,H2]	UCA-22 - The User Clients send confidential information using a regular connection without encryption [H3,H5]. UCA-23 - The User Clients use a weak password [H5] UCA-24 - The User Clients access a malicious hyperlink receives by e-mail [H5]		UCA-25 - The User Clients perform several unsuccessful access attempts [H5]
....	.....	....	.....	.....

Active STPA for Cybersecurity Data Analysis

Identify Losses Scenarios

UCA-01 - The Blue Team does not analyze the logs, alerts and warnings provided from devices [H4,H5,H6]

- There is no member of Blue Team with technical training to analyze logs, alerts and warnings

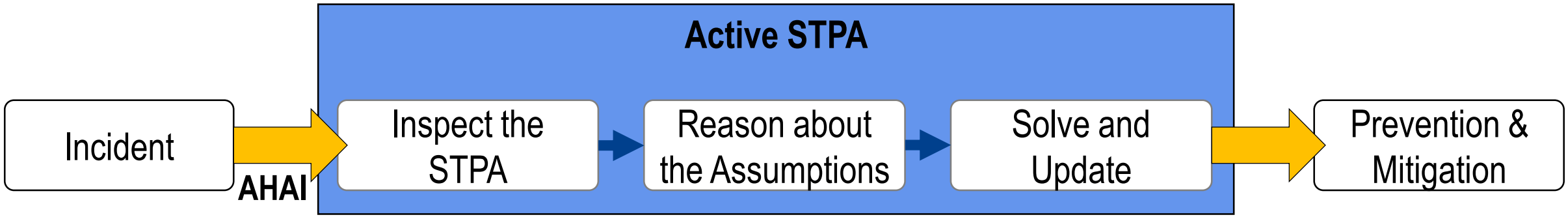
UCA-02 - The Blue Team does not performs real-time monitoring [H3,H5, H6, H7]

- The real-time monitoring is not a regular task of Blue Team
- Another tasks have more priority over real-time monitoring

UCA-25 - The User Clients perform several unsuccessful access attempts [H5]

- Possible DOS attack.
- Storage Server might be unavailable

Active STPA for Cybersecurity Data Analysis



Phases of Active STPA [4]

- The Blue Team (BT) will be responsible for acting as Security Analyst (SecA)
- Using Machine Learning techniques will lead to increased process automation (AHAI)
- In Cybersecurity, attacks will occur regardless of the deployment of all necessary defense mechanisms. That is, hazard analysis will allow the deployment of the correct mechanisms to prevent a system from being invaded, but it will not prevent the attack from occurring.
- Therefore, it doesn't prevent the incident, but it can prevent the accident (loss).

Active STPA for Cybersecurity Data Analysis

Real-time Monitoring Indicators

- Indicators can also be used with Open-Source Intelligence (OSINT) resources to provide possible solutions for attack or vulnerability found.
- Integrated with Artificial Intelligence [7]

Example

- Several unsuccessful access attempts of a specific user client to a storage server could be AHAI identified by Machine Learning techniques.
- Another AHAI (e.g., antivirus log) indicates that a malware was found in computer system of the same user client.
- The OSINT can be used as an integrated tool to present information about this malware

Active STPA for Cybersecurity Data Analysis

- AI-generated results (AHAI) could enhance the work of SecA (Blue Team).

Inspect STPA

- IT infrastructures are common and typically similar.
- Therefore, STPA analysis can be considered generic in most cases.

Reason about the Assumptions

- Identify violated assumptions, **Analyze trends,** Investigate causal and contributing factors, Determine the reason for broken assumptions and **Verify if contingency protections worked**
  - **Analyze trends -** AI-generated results can indicate trends (for example, attacks from a specific country or region)
  - **Verify if contingency protections worked -** OSINT – Implement new protections that were not previously considered unsafe

Active STPA for Cybersecurity Data Analysis

Solve and Update

- **List possible defenses**, Analyze tradeoffs, **Determine the optimum solution**, **Implement new defenses and protections**, Update the STPA (if necessary)
  - **List possible defenses** – AI-generated results with or not OSINT applications
  - **Determine the optimum solution** – OSINT enables identifying known and new vulnerabilities
  - **Implement new defenses and protections** – The BT reports updates and new security mechanisms to IT Team that should be implemented

Buffik por Pixabay

Conclusion

- Static security analysis is no longer sufficient to ensure the cybersecurity of sensitive data.
- Emerging techniques, such as Active STPA in a Zero Trust scenario, Machine Learning and OSINT, provide an alternative for more dynamic and assertive monitoring.
- In real-time monitoring, data sources can be used as input to identify unusual behavior and vulnerabilities in dynamic monitoring system.
- Using System Engineering techniques such as tailored Active STPA, combined with Machine Learning techniques, can result in cybersecurity assurance for sensitive data.

References

[1] M. P. Barrett. "**Framework for Improving Critical Infrastructure Cybersecurity Version 1.1**", National Institute of Standards and Technology (NIST), 2018.

[2] M. Stone, et al. "**NIST Special Publication 1800-5**", NIST, 2018.

[3] J. Kindervag, "**No More Chewy Centers: The Zero Trust Model Of Information Security**", Cambridge: Forrester, 2016.

[4] D. S. Castilho. "**Active STPA: Integration of Hazard Analysis into a Safety Management System Framework**" Cambridge: MIT, 2019, p. 184.

[5] N. G. Leveson and J. P. Thomas. "**STPA Handbook. Safety Science**", Cambridge, 208.

[6] National Security Agency (NSA). "**Embracing a Zero Trust Security Model**", NSA, 2021.

[7] Browne, T.O., Abedin, M. & Chowdhury, M.J.M. "**A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications"**. Journal Information Security. 23, 2911–2938 (2024).