



Cyber Informed Defense

SANS Night Talk - Amsterdam



<https://bhemida.com>

Technical | Strategy Senior Manager

Bassem Hemida

Cyber Security Professional with strategic management experience for over a decade with corporates and multinational organizations throughout Europe and the Middle East.

Awarded Penetration Tester of the Year 2016 from EC-Council Foundation InfoSec Tech & Exec. Winner of SANS Core Netwars, CyberDefense Netwars, DFIR Netwars and GRID Netwars

Download CV

Contact



What I Do



Red Teaming and Cybersecurity Crisis Simulation

Build a Red Team program and leverage Red Team exercises and adversary emulations to obtain a holistic view of an organization's security posture to measure, train, and improve people, processes, and technology for the organization. Also, perform multiple penetration tests, and targeting network-level, client-side-level, and web application-level attack vectors.



IT / OT Cyber Strategy

Balance the requirements to be secure, vigilant, and resilient with strategic objectives and the risk appetite of the organization. Develop an actionable roadmap and governance model to support security priorities in an era where cyber is everywhere.



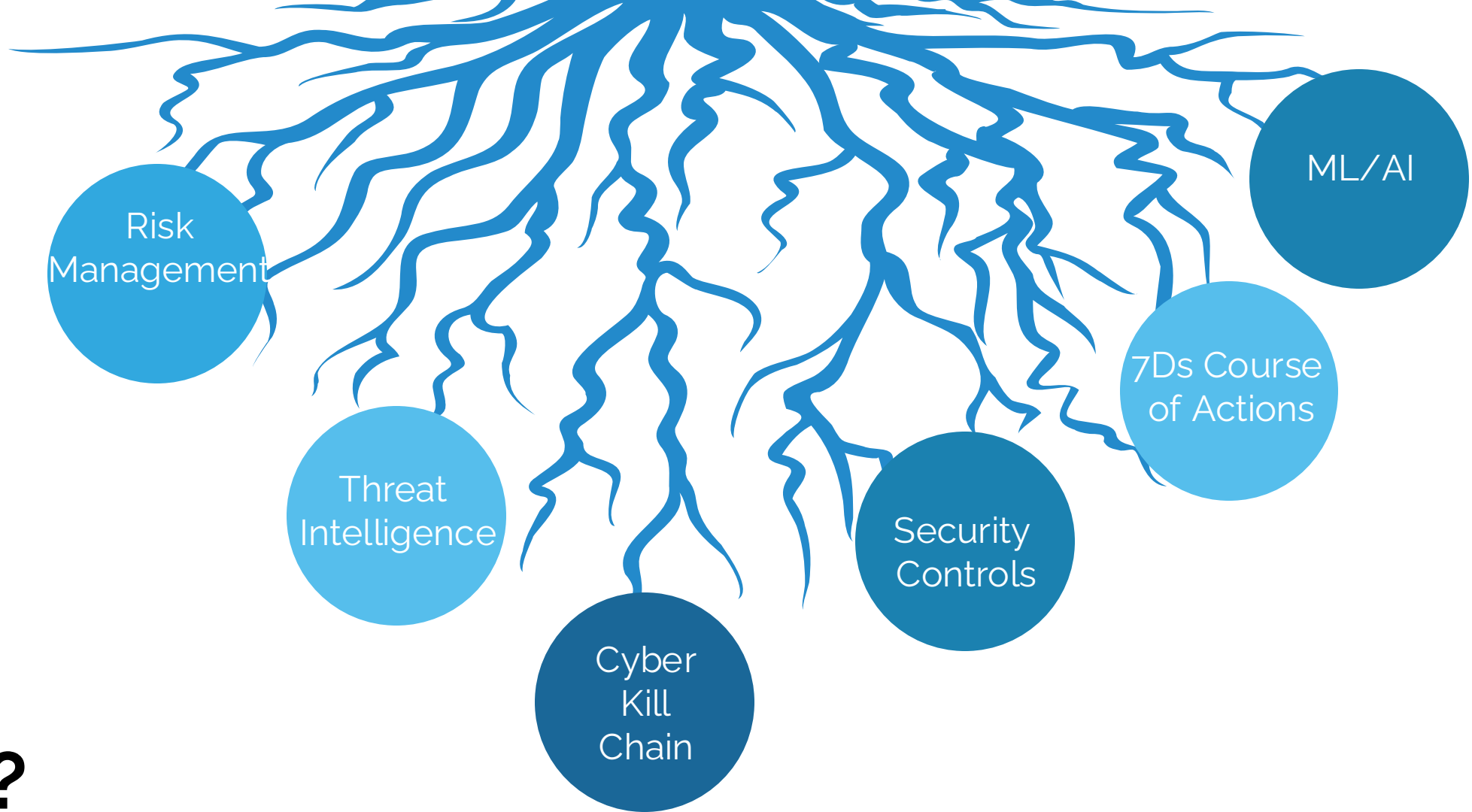
ICS / SCADA Security

Design and audit ICS/SCADA network security architecture and align it with the internationally recognized security standard like ISA99 / IEC 62443 and NERC CIP. Moreover, perform in risk assessments of ICS related technologies and day-to-day cyber-related operations. Also, Perform ICS / SCADA security assessments to identify potential vulnerability malicious adversary scenarios that might significantly impact client operations.



Incident Response

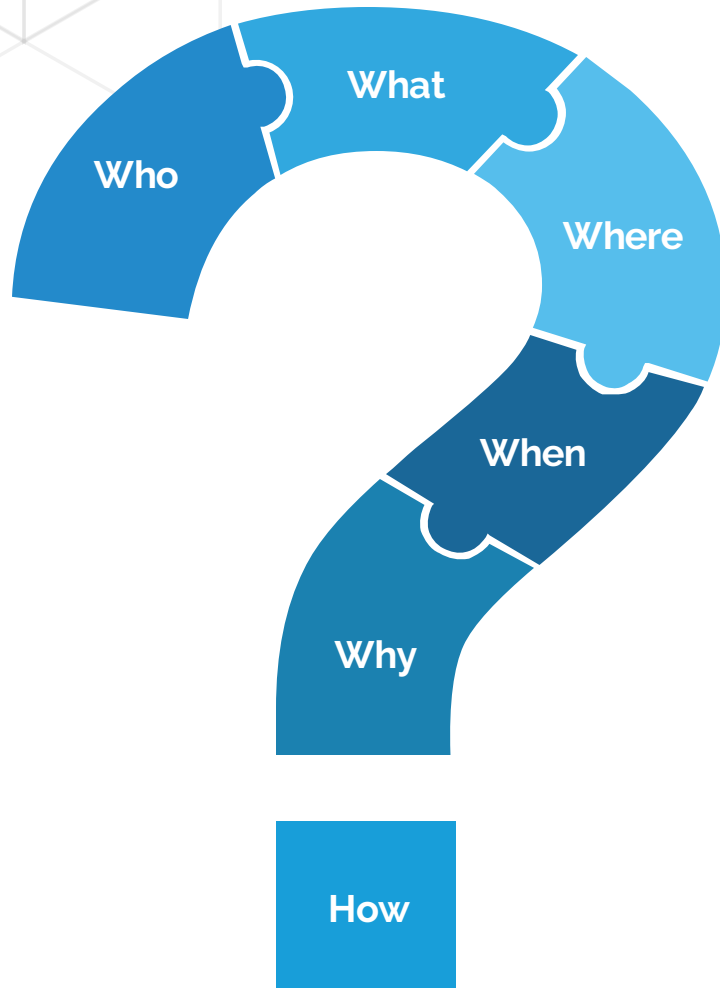
Manage security incidents by understanding common attack techniques, vectors, and tools as well as defending against and/or responding to such attacks when they occur. Concentrating on methods used to detect, respond, and resolve computer security incidents.



Why?

In this talk I am proposing my point of view on how to scale up our cyber strategy to the next level of implementation and operate through more efficient, cost effective and sustainable methods that improve your investment to enhance cyber defence against modern and emerging threats. We will utilize the AI to provide intelligence for more efficiency.

Risk Management



Organizations have limited financial resources and personnel resources. Therefore, organizations must prioritize their security defenses through Risk management to:



**Prioritize / focus
defensive controls
with the best return**



**Prioritize / focus
their limited financial
& personnel
resources**



**Determine which
controls are not
feasible in the
short / long term**



**Measure themselves
for ongoing
management &
compliance**

Risk Management



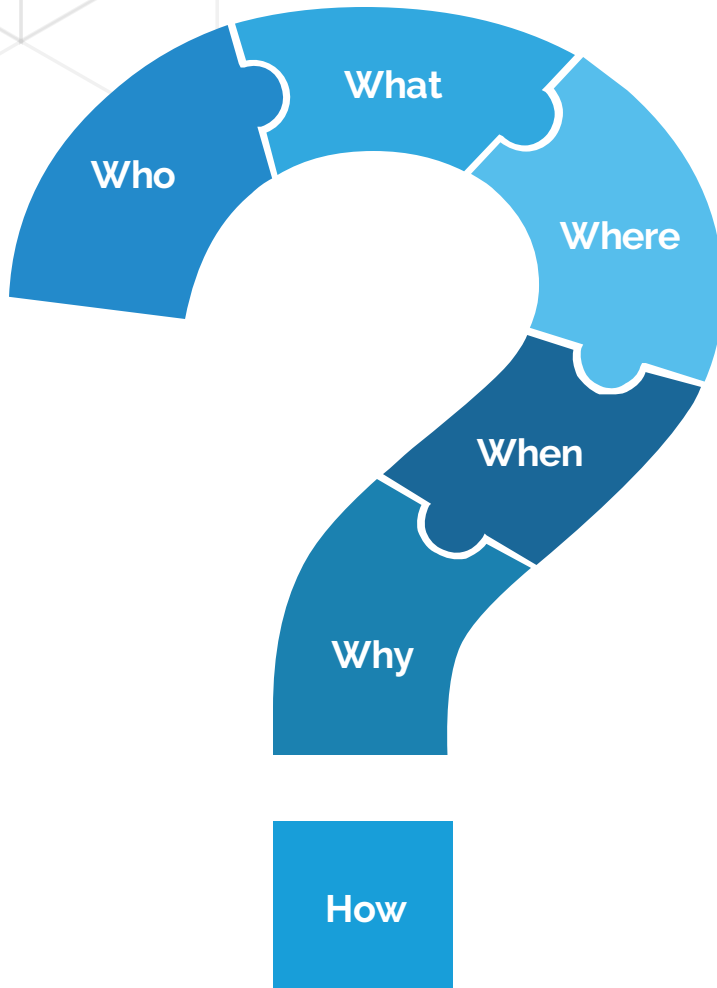
Which one is the correct calculation?

Risk = Likelihood × Impact.

Risk = Threat probability × vulnerability Magnitude

Risk = Criticality (Likelihood × Vulnerability Scoring [CVSS]) × Impact where Criticality = Probability × Severity.

Risk Management



Risk treatment course of actions are not enough

- Risk mitigation: Implement controls and countermeasures to reduce the likelihood or impact of risks. This may include technical, administrative, or physical controls.
- Risk transfer: Shift the responsibility for managing a risk to a third party, such as through insurance, outsourcing, or contractual agreements.
- Risk avoidance: Eliminate the risk by discontinuing the activity or process that introduces the risk.
- Risk acceptance: Acknowledge that the risk falls within the organization's risk tolerance and decide to accept the potential consequences without implementing additional controls.

Why Threats not Risks

Full Chain

Cyberattacks are not singular events but part of an overall scenario, chain of events, or operation, so considering security controls in this way benefits defenders. Instead of trying to develop requirements against “virtual private network (VPN) compromises,” we can think through a full compromise scenario.

$$\text{Risk} = \text{Threat probability} \times \text{vulnerability Magnitude}$$

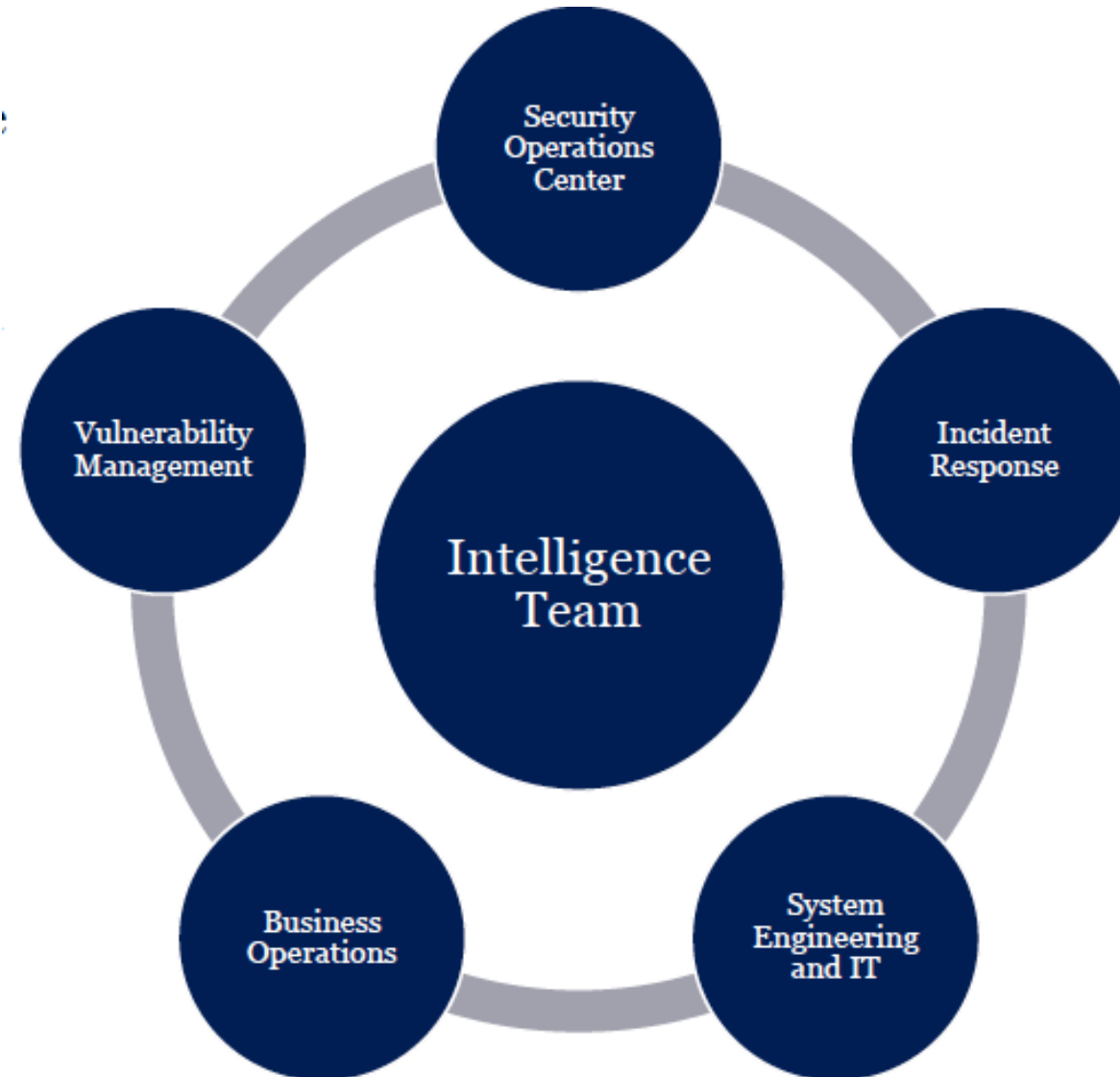
Threat Probability

This represents the likelihood of a cyber attack occurring. It takes into account the intent, opportunity, and capability of potential threat actors. Factors that can influence threat probability include the organization's industry, size, and the value of its data or intellectual property.

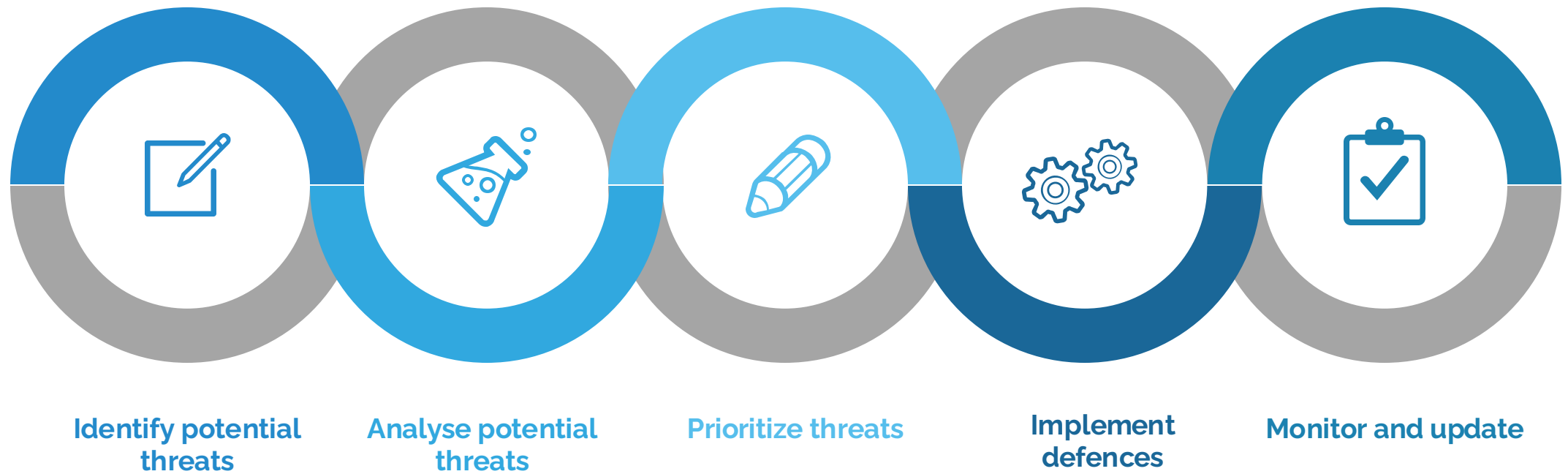
Vulnerability Magnitude

This refers to the potential impact of a successful cyber attack on the organization. It considers the severity of the vulnerabilities present in the organization's systems, networks, and applications. The magnitude of a vulnerability is related to the potential for catastrophic consequences if exploited by an attacker.

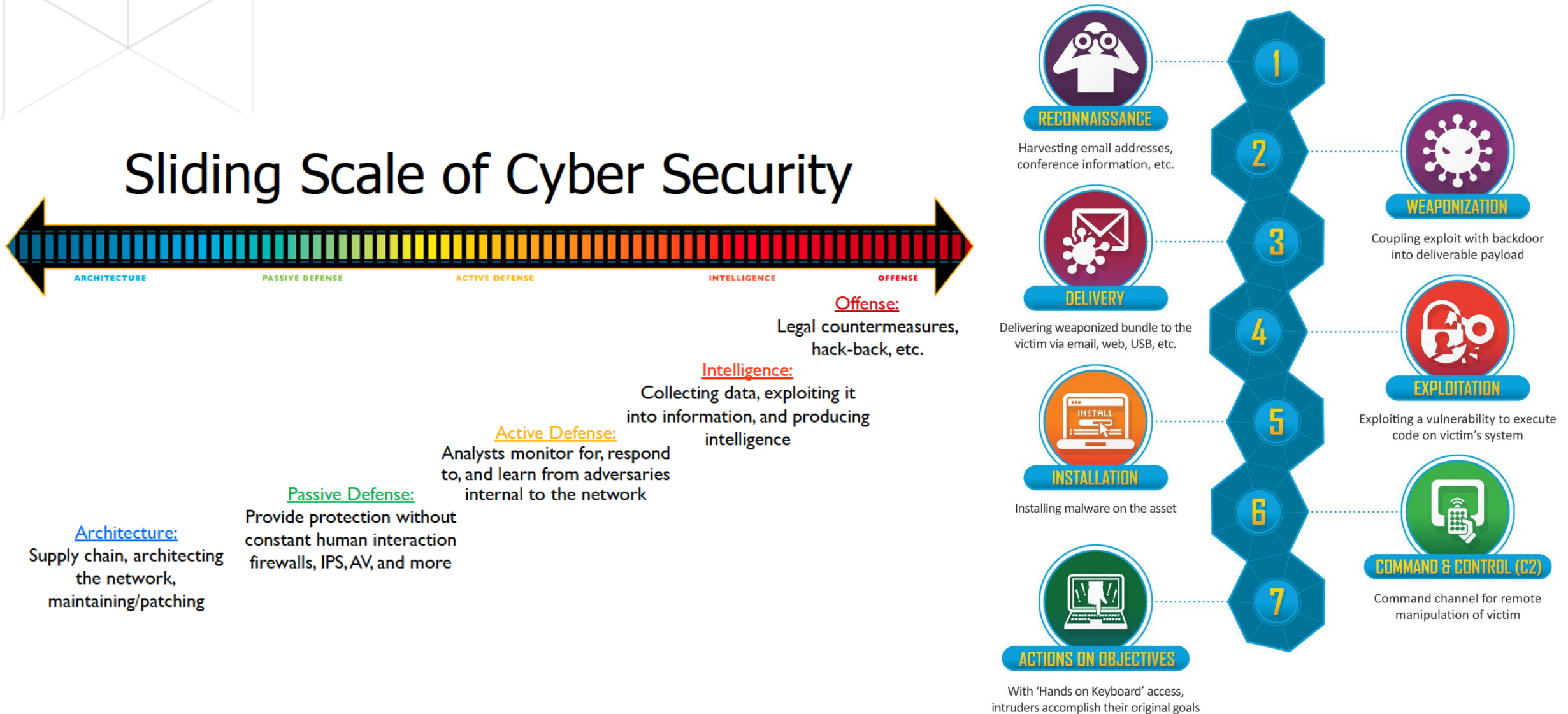
What is the role of threat intelligence?



Cyber informed Defence Approach



Cyber Kill Chain and Sliding Scale of Cyber Security





Bridging both

7Ds course of Actions

The 7Ds course of actions are:

Discover: Identifying and gathering information about potential threats, vulnerabilities, and indicators.

Detect: Monitoring and analyzing network traffic, logs, and other data sources to identify signs of malicious activity or potential threats.

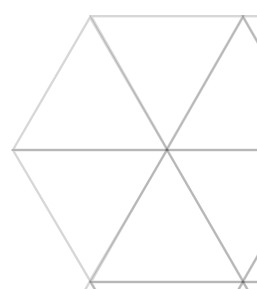
Deny: Implementing measures to prevent unauthorized access, exploitation, or damage to systems, networks, and data.

Disrupt: Taking actions to interrupt or impede an attacker's activities, such as blocking network connections or disabling malicious software.

Degrade: Reducing the effectiveness or efficiency of an attacker's tools, techniques, or infrastructure, making it more difficult for them to achieve their objectives.

Deceive: Employing tactics to mislead or confuse an attacker, such as creating honeypots or providing false information.

Destroy: Eliminating an attacker's capabilities or infrastructure, either through direct action or by coordinating with law enforcement and other organizations.

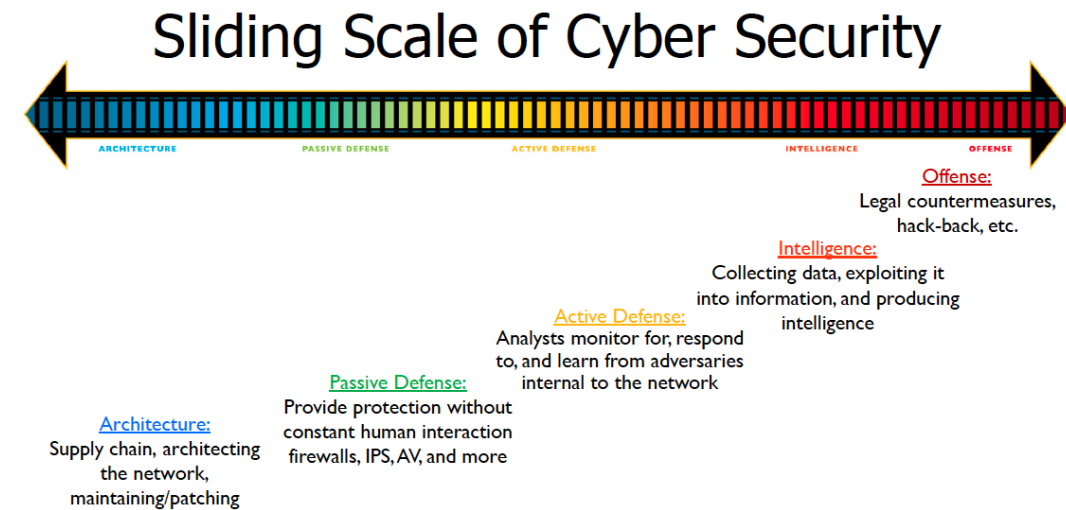


Bridging both - Example

Cyber Kill Chain Stage	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Collect and analyze threat intelligence on ransomware operators.	Analyze potential targets within infrastructure.	Harden email systems against phishing.	Share threat intelligence with industry partners.		Set up deceptive email accounts (honeypots).	
Weaponization	Monitor threat intelligence feeds for new ransomware variants.	Employ security tools to detect weaponization attempts.	Keep security tools updated.	Share weaponization techniques with industry partners.		Use honeypots to collect intelligence on weaponization tactics.	
Delivery	Gather intelligence on phishing techniques used by ransomware operators.	Employ email security measures to detect phishing emails.	Educate users on recognizing and reporting phishing attempts.	Report phishing emails to relevant authorities.	Implement rate limiting or traffic shaping.	Use deceptive email accounts (honeypots) to collect intelligence on phishing tactics.	
Exploitation		Monitor infrastructure for signs of exploitation.	Regularly patch and update software and systems.		Employ countermeasures to degrade exploitation attempts.	Use decoy systems to mislead attackers and gather intelligence on exploitation methods.	
Installation		Use endpoint security tools to detect and prevent ransomware installation.	Implement application control policies.	Share threat intelligence about ransomware installation techniques.		Use deception technologies to mislead attackers about installation success.	Contain, eradicate, and recover using incident response plan (if installation is successful).
Command and Control	Collect intelligence on known malicious C2 servers or IP addresses.	Monitor outbound network traffic for connections to suspicious domains or IPs.	Implement network segmentation and access control policies.	Block communication with known malicious C2 servers.		Use deception technologies to mislead attackers about C2 communication success.	Address C2 communication if detected using incident response plan.
Actions on Objectives	Gather intelligence on ransomware operators' objectives.	Monitor for signs of data exfiltration, encryption, or other malicious activities.	Implement strong access controls, encryption, and DLP measures.	Quickly detect and respond to ransomware activity.	Employ countermeasures to degrade ransomware attacks.	Use deceptive data or systems to mislead attackers about the success of their actions.	Contain, eradicate, and recover from ransomware attacks using incident response plan.

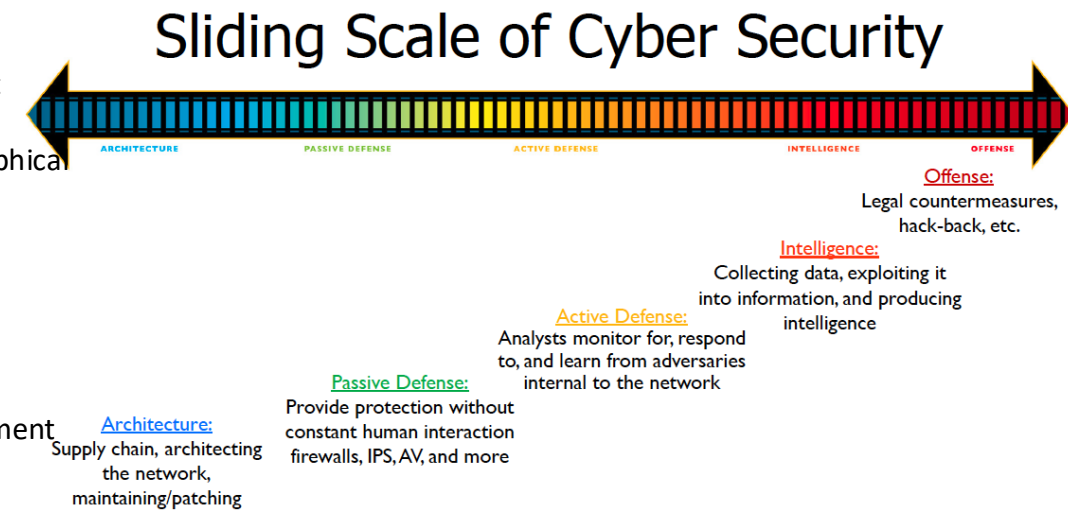
NIST Protect

- **Protect:** This stage involves **implementing measures** to **prevent cyber threats** from penetrating or damaging systems, networks, or applications. This includes implementing/enhancing technology capabilities like firewalls, antivirus software. Also, This includes creating a defensible architecture that focuses on addressing the most likely and relevant threats to the organization, aligning with industry standards such as IEC62443. To secure the infrastructure, organizations should consider the following:
 - Defensible Architecture
 - Design a defensible architecture that focuses on addressing the most likely and relevant threats. The reference architecture should be in line with industry requirements and adopt at least two defense-in-depth designs (Protected Enclaves and Vector Oriented).
 - Implementing Security Measures
 - Deploy/improve firewalls, antivirus software, and other security tools to protect the organization's infrastructure.
 - Regularly patch and update software and systems to mitigate vulnerabilities.
 - Implement strong access controls and authentication measures, such as multi-factor authentication.



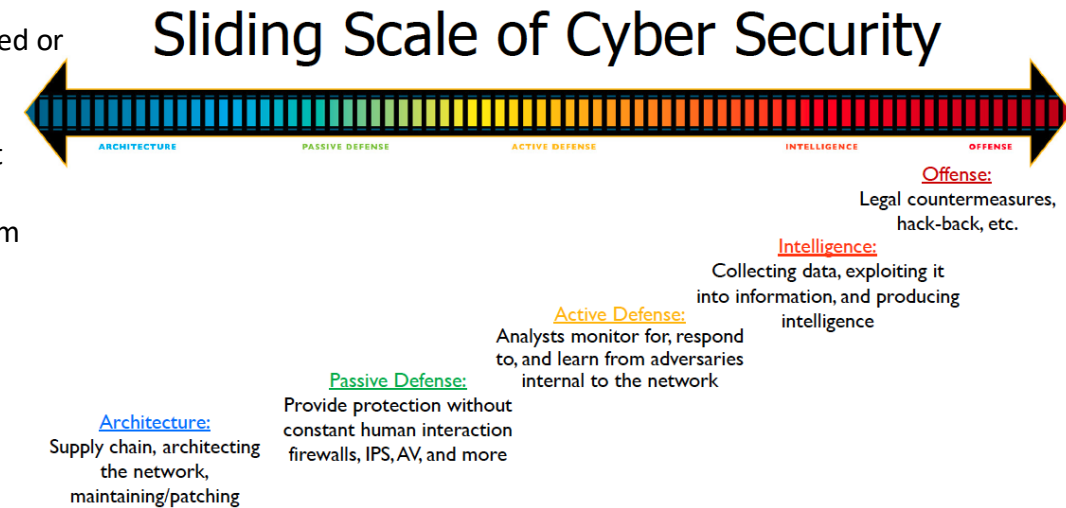
NIST Detect

- **Detect:** This stage involves the **identification** of potential **cyber threats or attacks**. It involves use of security tools and technologies to monitor networks, systems, and applications for any suspicious activities. This can be mapped to your SOC Services.
 - Cyber Threat Intelligence Requirements
 - Establish intelligence requirements based on the organization's risk profile and threat landscape.
 - Identify relevant sources of threat intelligence, such as internal SOC, industry/geographical incidents, open-source intelligence, commercial feeds, and industry partnerships.
 - Implement a threat intelligence platform to collect, aggregate, and analyze threat intelligence data.
 - Security Operations Center (SOC) Services
 - Develop a SOC to monitor networks, systems, and applications for any suspicious activities.
 - Use security tools and technologies, such as Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR), to detect potential threats.
 - Create/conduct a threat hunting activities to proactively search for threats within the organization's environment.
 - Continuous Monitoring and Adaptation
 - Continuously monitor the threat landscape and update the organization's intelligence requirements and security measures accordingly.
 - Share threat intelligence with industry partners and relevant authorities to improve the collective defenses.
 - Establish/Enhance Log Collection Framework requirements to operationalize MITRE frameworks for Enterprise and ICS.

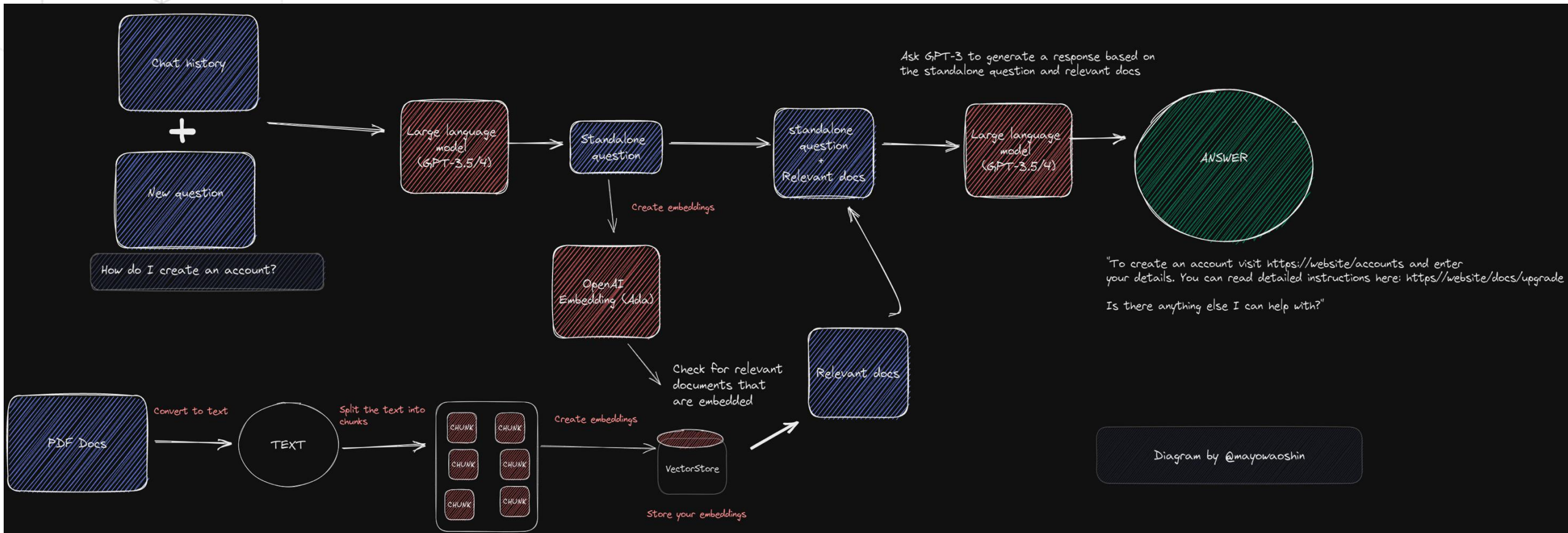


NIST Response

- **Response:** This stage involves developing an incident response plan to **address cyber threats that are detected or occur.**
 - Incident Response Plan
 - Develop a comprehensive incident response plan that addresses cyber threats detected or occurring within the organization.
 - Establish a clear chain of command, roles, and responsibilities for incident response.
 - Train employees on their roles in the incident response process and regularly conduct drills or exercises to test the plan's effectiveness.
 - Regularly review and update the incident response plan based on lessons learned from previous incidents and new threat intelligence.



OpenAI



Thank you

