Co-funded by
the European Union

Course: IT Fundamentals of Cyber Security

Project: Cyber Security 4 ALL(CS4ALL)

CHAPTER VI

Risk Management and Incident Response

Content

- ✓ Risk Management Methodologies and processes
  - Risk Identification, Assessment and Analysis
  - Risk Monitoring and Review
  - Risk Management frameworks
- ✓ Incident Response planning frameworks
  - Phases of Incident Response
  - Incident Response Team structure
  - Creating an Incident Response plan and Best practices
- ✓ Post Incident Analysis and lessons learned
  - Step in post Incident Analysis and Root cause analysis
  - Assessing Incident Response Effectiveness
  - Lessons learned Documentation and updating Incident Response plan
  - Real world examples and case studies of post Incident Analysis

Co-funded by the European Union

Co-funded by
the European Union

Risk Management Methodologies and Processes

What is Cybersecurity Risk Management?

Cybersecurity risk management is the process of identifying an organization's digital assets, reviewing existing security measures, and implementing solutions.

Risk Identification, Assessment and Analysis

- **Risk Identification**

❑ **Identifying Assets**

Identify the assets that must be protected, and their priorities.

❑ **Threats**

Identify potential sources of harm to the assets (information, data) that you need to protect.

❑ **Identifying Vulnerabilities**

Identify weaknesses in your overall cybersecurity environment that could make you vulnerable to those threats

Co-funded by the European Union

- **Risk Assessment**

A risk assessment is a process used to identify potential hazards and analyze what could happen if a disaster or hazard occurs. There are numerous hazards to consider, and each hazard could have many possible scenarios happening within or because of it.

A cybersecurity risk assessment can be split into many parts, but the five main steps are: scoping, risk identification, risk analysis, risk evaluation and documentation.

Co-funded by
the European Union

• Risk Analysis

➢ Risk analysis refers to the review of risks associated with the particular action or event.

➢ Types of Risk Analysis:
- Quantitative
- Qualitative

➢ Steps in Risk Analysis Process:
- Conduct a Risk Assessment Survey.
- Identify and Analyze the risks.
- Develop a risk management plan.
- Implement the risk management plan.
- Monitor the risks.

Co-funded by the European Union

Risk Monitoring and Review

Monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance.

Continuous security monitoring also gives you real-time visibility into your IT security data, offering advantages such as:

- Identifying and addressing vulnerabilities through remediation strategies
- Maintaining a strong risk posture by constantly monitoring for potential threats, including ransomware, phishing, and other cyber incidents
- Improving incident response by quickly identifying and responding to potential threats

Providing cybersecurity metrics that can assess the state of security at all levels of an organization

- Managing third-party risks by monitoring vendor risk management security practices
- Monitoring the overall effectiveness of all security controls
- Using threat intelligence to identify emerging threats and trend

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

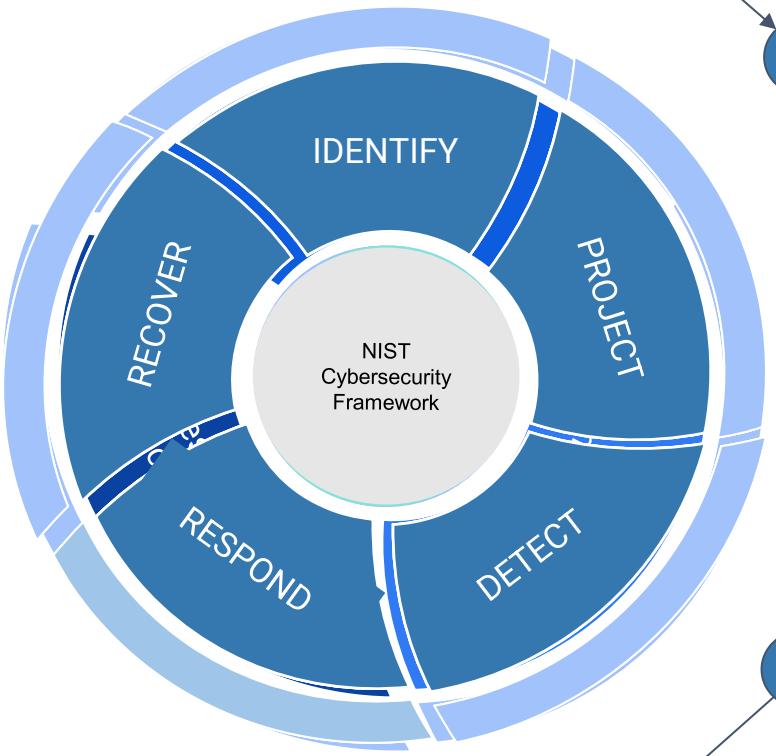
Risk Management Framework

There are several cyber risk management frameworks, each of which provides standards organizations can use to identify and mitigate risks.

- NIST CSF
- ISO 27001
- DoD RMF
- FAIR Framework

Co-funded by the European Union

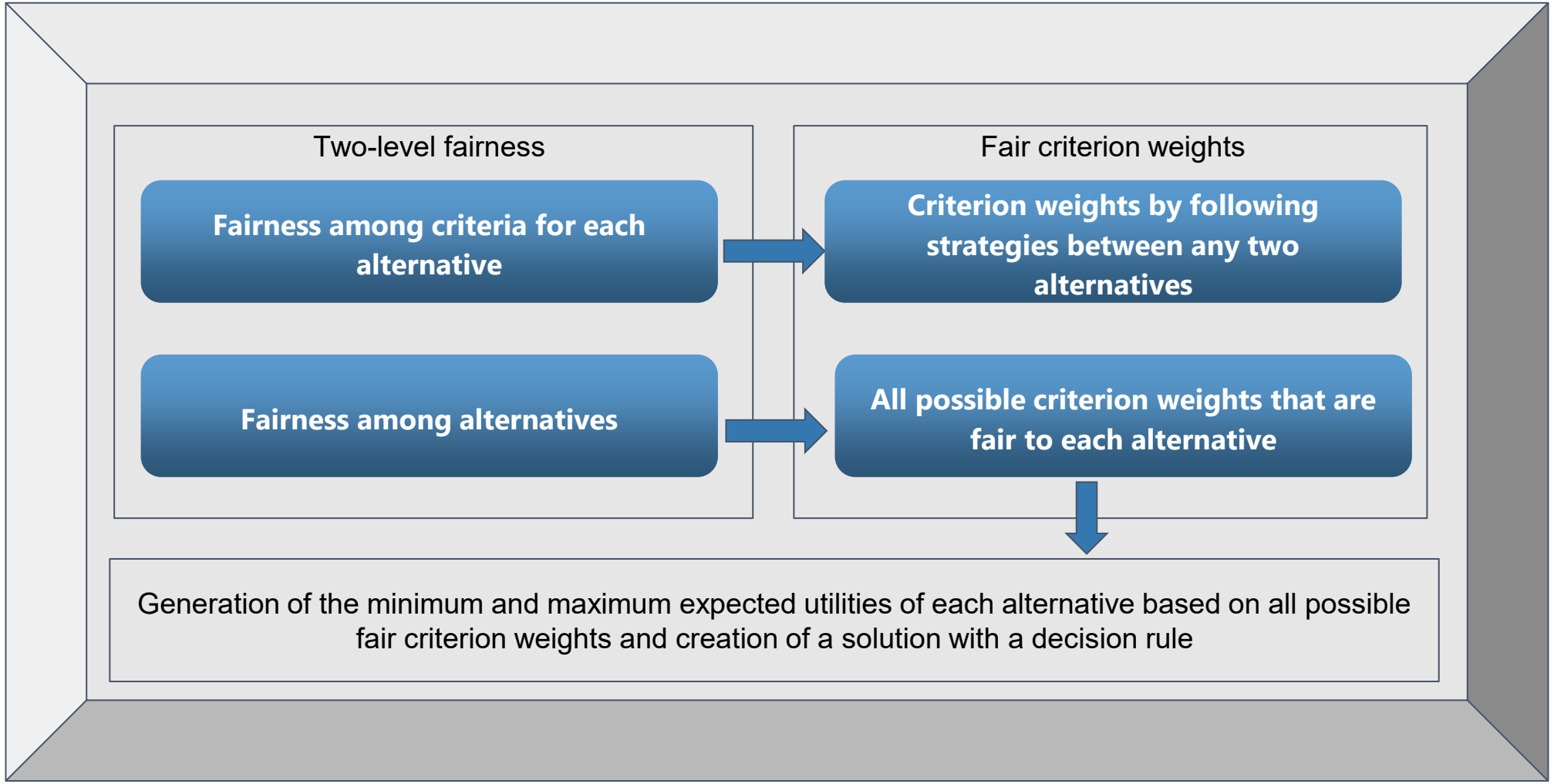
NIST FRAMEWORK



1. Scope the Organizational Profile
2. Gather needed information
3. Create the Organizational Profile
4. Analyze the gaps and create an action plan
5. Implement action plan and update Profile

Co-funded by
the European Union

FAIR FRAMEWORK



Co-funded by the European Union

Incident Response Planning and Procedures

The incident response lifecycle

Incident response is a structured process organizations use to identify and deal with cybersecurity incidents.

- **Minimizing damage:** A structured response helps contain threats quickly, reducing the extent of damage to systems and data.
- **Reducing recovery time:** By having a clear plan and procedures in place, organizations can recover more swiftly from incidents, minimizing downtime and operational impact.
- **Enhancing security posture:** Regularly reviewing and updating the incident response process helps organizations improve their defenses and be better prepared for future incidents.
- **Ensuring compliance:** Many regulatory frameworks require organizations to have incident response plans. Following a defined lifecycle helps meet these requirements and avoid penalties.

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Phases of Incident Response

Phase 1: Preparing for Potential Incidents

Define clear communication channels, implement response checklists, and provide staff with quality cybersecurity training.

Phase 2: Identifying and Assessing Threats

Assess whether an event is a cyber attack, evaluate its intensity, and classify the cyber security incident based on nature of attack.

Phase 3: Containing the impact

Isolate the affected systems and impede the incidence from propagating further.

Phase 4: Investigating and Eradicating Threats

Make sure that the threat is no longer present in the organization's network by investigating the root cause of the incident and eradicating threats from the system.

Phase 5: Recovering and Restoring Operations

Restore the affected systems to their pre-incident state to get your business back up and running as normal.

Phase 6: Learning from the Incident

Document everything that occurred during the incident and the response. Use this information to recognize the area for improvement in the organization's security posture and the incident response plan.

Phase 7: Ongoing Testing and Evaluation

Strengthen your security posture by continuously testing and evaluating your incident response plan to ensure that it remains current and effective.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Incident Response Team Structure

- **Team leader**—responsible for coordinating team activities and reporting to upper-level management.
- **Communications**—responsible for managing communications throughout the team and organization. These members are also responsible for ensuring that stakeholders, customers, and public authorities are properly informed about incidents.

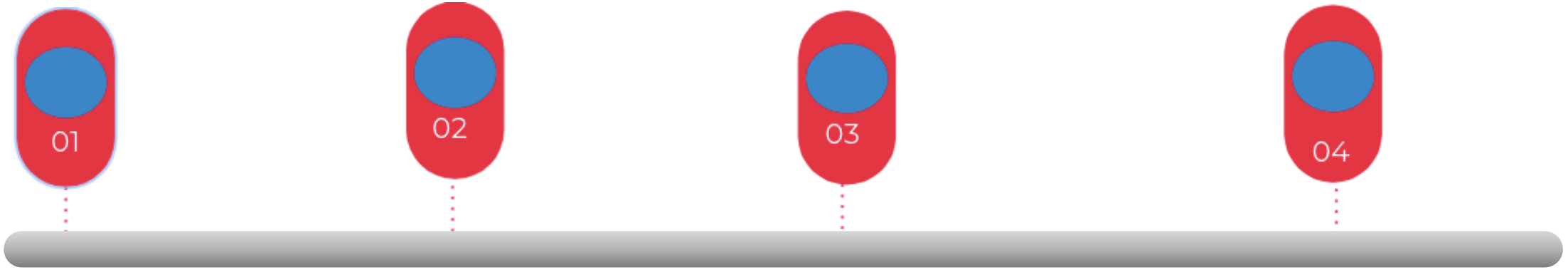
Co-funded by the European Union

- **Lead Investigator**—responsible for performing primary investigation of events, guiding the efforts of other analysts, and providing in-depth evaluation of cyber security incidents.
- **Analysts and researchers**—responsible for supporting the lead investigator and providing threat intelligence and context for an incident. These members are also often responsible for carrying out the incident response process.
- **Legal representation**—responsible for providing legal guidance in terms of compliance, interactions with law enforcement, and standards of integrity for forensic evidence.

Co-funded by the European Union

Creating an Incident Response Plan and Best Practices

A Cybersecurity Incident Response Plan is a document that gives IT and cybersecurity professionals instructions on how to respond to a serious security incident, such as a data breach, data leak, ransomware attack, or loss of sensitive information. According to the National Institute of Standards and Technology (NIST), there are four phases to most effective incident response plans:



1.Preparation

2. Detection and Analysis

3. Containment, eradication, and recovery.

4. Post-incident activities.

Co-funded by the European Union

Post Incident Analysis and Lessons Learned

- A post-incident review is a detailed retrospective that allows you to comprehensively examine a cybersecurity event, such as a data breach, leak, cyber attack, and so on.

- It involves closely analyzing each part of an incident from beginning to end to gather insights and strengthen cyber resilience.

Co-funded by the European Union

Steps in Post Incident Analysis and Root Cause Analysis

1. Find the Root cause:

Address the problem from the very beginning, not just the end.

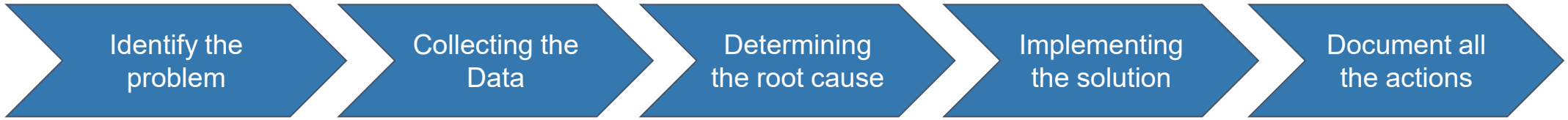
2. Improve Resilience:

Mature your security program by investigating attacks from start to finish.

3. Scope the Damage:

Iteratively assess the complete picture of damage to prevent future incidents.

4. Root Cause Analysis (RCA):



Co-funded by the European Union

Assessing Incident Response Effectiveness

Keys to assessing incident response effectiveness is as follows:-

1. **Speed metrics :** When it comes to incident response, speed is clearly of the essence. The faster the security team can contain a threat, the less damage the threat can do. Speed metrics are critical in measuring the effectiveness of incident response.

2. **Effectiveness metrics:** Another set of incident response metrics hinges on the permanence, or durability, of the resolution. It can measure by Percentage of incidents undergoing RCA ,Percentage of prescribed fixed completed on time

3.**Efficiency metrics :** Finally, it is important to track how efficiently an organization responds to incidents.It can be determined by Total cost of incident, Security staff time on incident.

Co-funded by
the European Union

Lesson Learned Documentation and Updating Incident Response Plan

1. It helps identify the root cause of the incident, which is essential for preventing similar incidents from happening the future.

1. It provides an opportunity to evaluate the incident response process and identify areas that need improvement.

1. It provides an opportunity to assess the effectiveness of existing controls and make necessary changes.

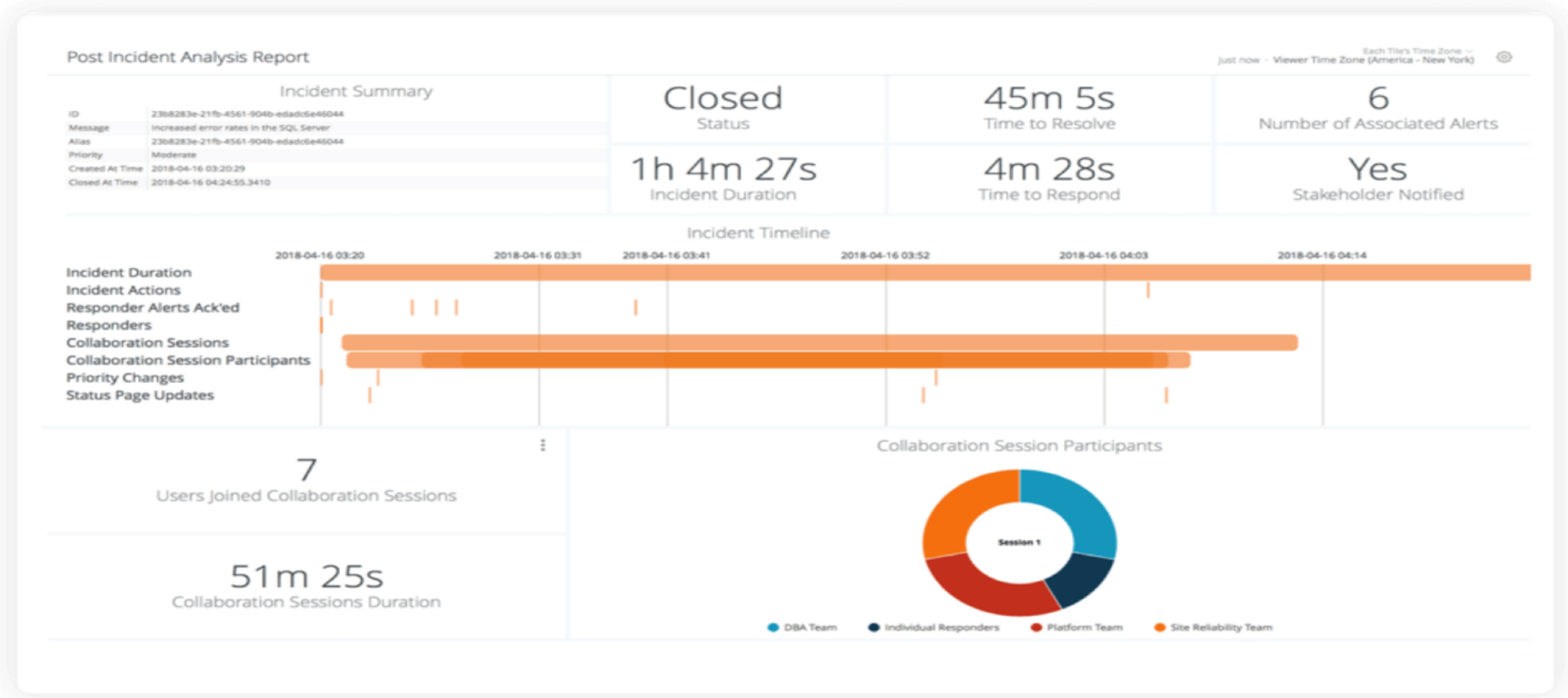
CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Real World example and case studies of Post Incident Analysis

- ✓ Social engineering attacks: Mailchimp and Cisco.
- ✓ Privilege abuse: International Committee of the Red Cross (ICRC).
- ✓ Data leak: Microsoft and Pegasus Airlines.
- ✓ Insider data theft: Tesla.
- ✓ Intellectual property theft: Apple, Yahoo.
- ✓ Third-party vendor attacks: American Express, T-Mobile.

Co-funded by the European Union

Example Post Incident Analysis Report:



Co-funded by
the European Union

Conclusion

- In today’s dynamic and interconnected environment, effective risk management and incident response are paramount for organizations seeking to safeguard their assets, reputation, and operational continuity.
- Risk management provides a structured approach to identifying, assessing, and mitigating potential threats, enabling organizations to proactively address vulnerabilities before they escalate into significant issues.
- Incident responses the critical mechanism that allows organizations to react swiftly and effectively when incidents occur.

Questions & answers

Invite questions from the audience.

Co-funded by
the European Union

Resources:

Reference Books:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
3. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
4. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J.David Irwin.CRC PressT&FGroup

Reference Links:

1. https://www.researchgate.net/publication/360686332_Cybersecurity_Management for_Incident_Response
2. https://www.researchgate.net/publication/381671293_SECURITY_RISK_MANAGEMENT a_reminder
3. https://www.sciencedirect.com/science/article/abs/pii/S0531513104005643

Co-funded by the European Union

THANK YOU!

Co-funded by
the European Union