Incident Response

- Wat is incident response?
  - Is dat Incident Management, Incident Handling, Incident Analysis ……..?
- Wat is de meerwaarde van een team dat specifiek met incident response bezig is (CSIRT of CERT of CIRT of ……)?
  - We hebben toch al een SOC, ITILv3 met de processen Incident Management en Security Management en ……
  - Wat voegt incident response (team) toe aan dit alles?
- Hoe ziet de dienstverlening van zo'n incident response entiteit er dan uit?
  - Wat kan/mag ik verwachten aan services?

Wat is

'Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.'

TechTarget | SearchSecurity

- Maar dit deden we toch al?

Software Engineering Institute | Carnegie Mellon University

- *'Incident Management: the ability to provide management of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handle'*

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- *'Incident Handling: rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services'*

SECURITY ACADEMY

CIS Center for Internet Security®

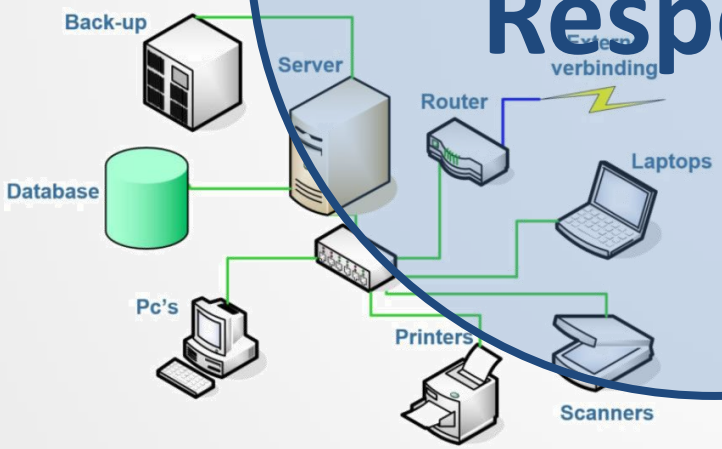
enisa

- *'Incident response and management is: protection the organisation's information, as well as its reputation, by developing and implementing an incident response process / infrastructure (e.g. plans, defined roles, training, communications, management oversight) in order to quickly discover an attack and then effectively contain the damage, eradicate the attacker's presence, and restore the integrity of the network and systems'*

Business
Calamiteiten en crisismanagement

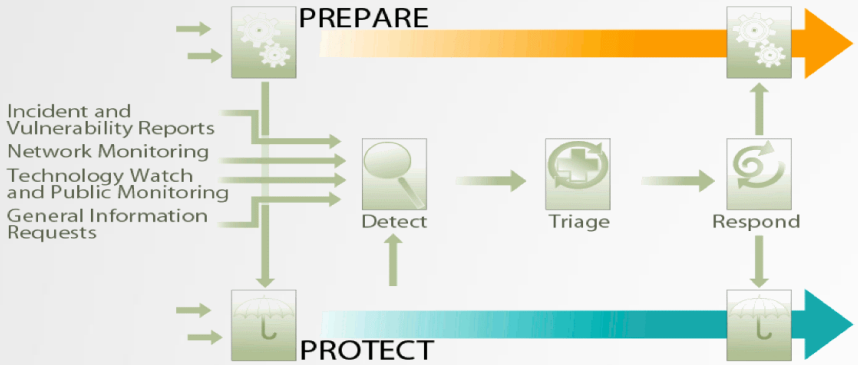
Incident Response

IT
Incident handling

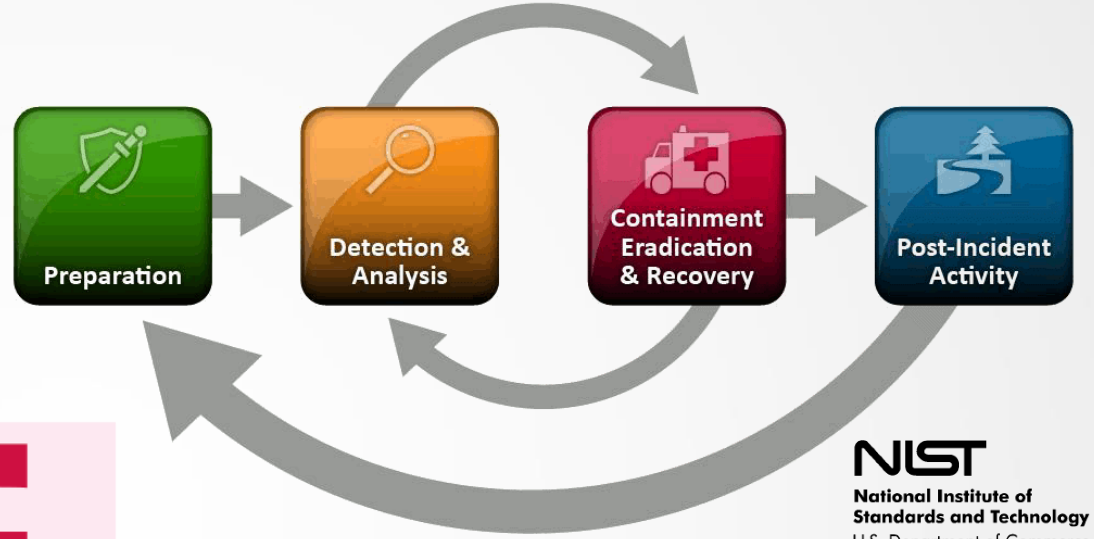


Security Operating Center
Security management

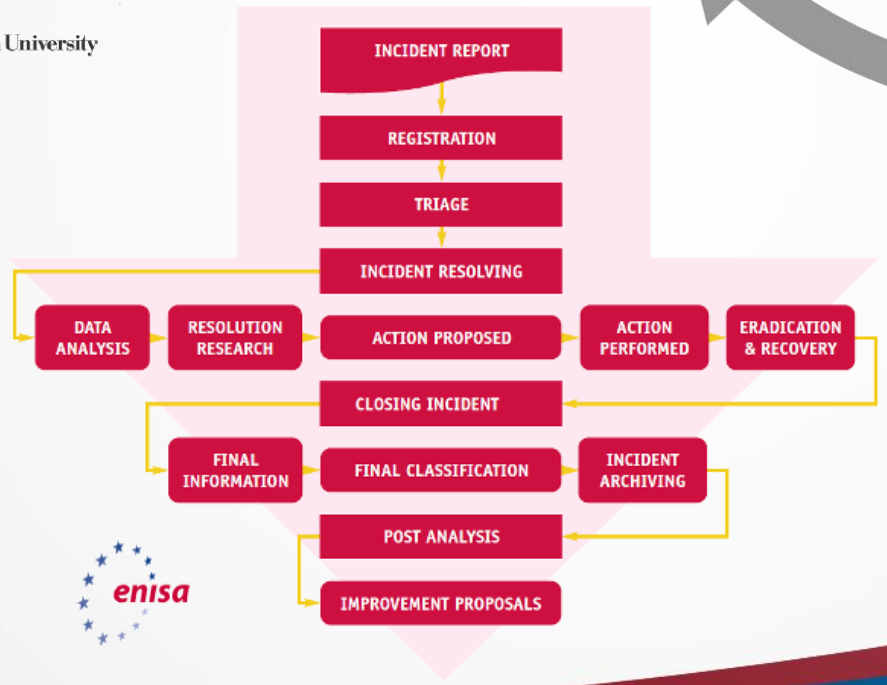
Het proces



Software Engineering Institute | Carnegie Mellon University

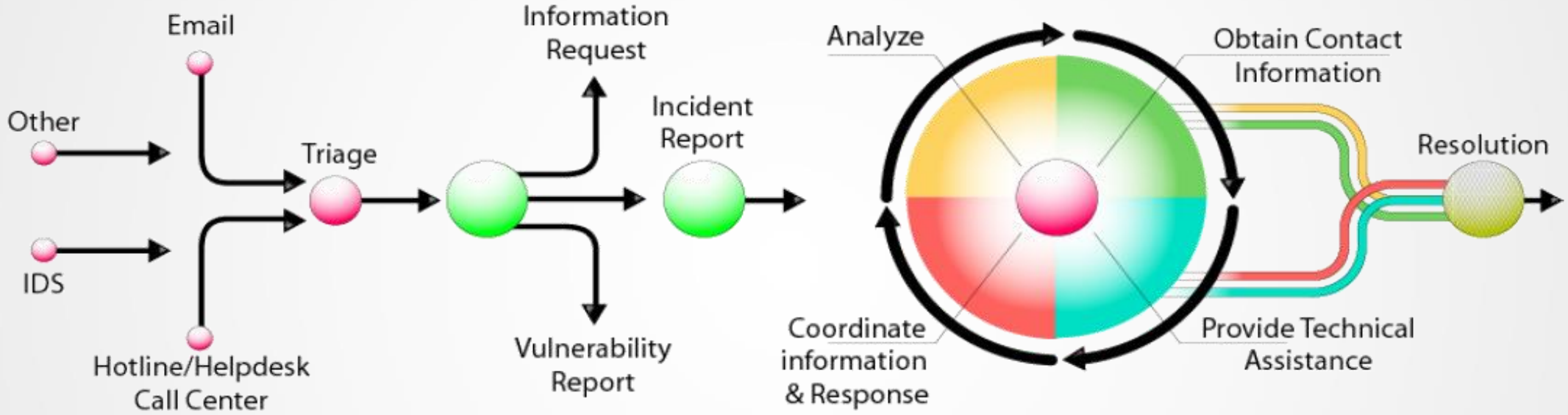


NIST National Institute of Standards and Technology U.S. Department of Commerce



SECURITY ACADEMY

De processtappen wat verder ingekleurd



- CMU/SEI-2003-HB-002

  Handbook for Computer Security Incident Response Teams (CSIRTS's)
  Second edition: April 2003

Toegevoegde waarde van een Incident Response Team

Vier cruciale basisvragen

- Wat gaan we doen? → mission statement
  - Doelstellingen en prioriteiten
- Voor wie doen we het? → verzorgingsgebied
  - Wat is het gebied waaraan het team diensten verleend en welke partners worden daarin onderkend?
- In welke setting doen we het? → positionering in de organisatie
  - Is sterk afhankelijk van volwassenheid van andere organisatieonderdelen
- In welke samenwerking doen we het? → relaties en communicatie
  - Zowel intern binnen het eigen verzorgingsgebied, als extern met collega teams en derden

- Toegevoegde waarde én verzorgingsgebied blijkt vaak uit mission statement
- *'…..-CERT ondersteunt de klant pro-actief om de veiligheid van niet alleen het eigen bedrijfsnetwerk te waarborgen, maar ook de netwerken waarover …….. de dienstverlening aan haar klanten biedt. Onderdeel van het verzorgingsgebied zijn de consumenten ISP's. …….-CERT verzamelt en analyseert bovendien incidenten en geeft advies om deze in de toekomst te voorkomen. Het gaat hier om incidenten die vanuit het verzorgingsgebied reactief zijn aangemeld, alsmede over meldingen van buiten het verzorgingsgebied'*

- Interne CSIRTs leveren diensten voor de eigen organisatie of branche (Z-CERT)
- Nationale CSIRTs leveren diensten voor een land (CERT.br)
- Coördination Centers dragen bij aan het vergroten van de weerbaarheid van bv. de Nederlandse samenleving in het digitale domein (NCSC.NL)
- Analysis Centers verzamelen incident informatie van verschillende bronnen om trends en patronen te analyseren (ISC van SANS)
- Incident Response Providers leveren CSIRT diensten tegen betaling aan andere organisaties (Fox-IT)

- Samenwerking zoeken is ook aansluiten bij FIRST, Trusted Introducer, etc.

- En collega's: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

- Wanneer het duidelijk is wat er van het team wordt verwacht kan er nagedacht worden aan services / diensten die geleverd moeten worden.
  - Waarschuwingsdienst
  - Detecteren van incidenten
    - Pro-actief en re-actief
  - Wordt er ondersteuning geboden bij de afhandeling van incidenten?
  - Of gaat het toch vooral over het rapporteren over mogelijke dreigingen en lopende incidenten
  - Etc. etc.

Dienstverlening van een Incident Response Team

- Er zijn meerdere services die geleverd kunnen worden door een CSIRT
- Uitgangspunt, en richtinggevend, bij de keuze zijn de missie, doelstellingen en het verzorgingsgebied dat is gedefinieerd
- Onderscheid wordt gemaakt* in:
  - Reactieve services
  - Proactieve services
  - Security Quality Management services

* door CMU-SEI en ENISA

- Reactieve services vormen de kern van de activiteiten van een CSIRT
- Deze services worden getriggerd door een melding vanuit een inbraakdetectie- of logging-systeem
- Of door een melding of een verzoek, zoals een rapport van een gehackte host, een wijdverspreide kwaadaardige code of een softwareprobleem

- Deze services bieden hulp en informatie die helpen bij de voorbereiding van de bescherming en beveiliging van de het IT landschap tegen aanvallen, problemen of gebeurtenissen
- De services zullen het aantal incidenten in de toekomst verminderen

Security Quality Management services

- Deze services zijn gericht op het versterken van andere onderdelen en diensten van de organisatie
  - Legal, Audit, HRM etc.
  - Diensten die traditioneel onafhankelijk zijn van incidentafhandeling
- CSIRT assisteert deze afdelingen waarbij het inzicht en de expertise van het CSIRT (identificeren risico's, bedreigingen en systeemgebreken) helpt om de algehele veiligheid van de organisatie te verbeteren
- Deze diensten zijn over het algemeen proactief

Mogelijke services

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓Risk Analysis
- ✓Business Continuity & Disaster Recovery Planning
- ✓Security Consulting
- ✓Awareness Building
- ✓Education/Training
- ✓Product Evaluation or Certification

Software Engineering Institute | Carnegie Mellon University

SECURITY ACADEMY

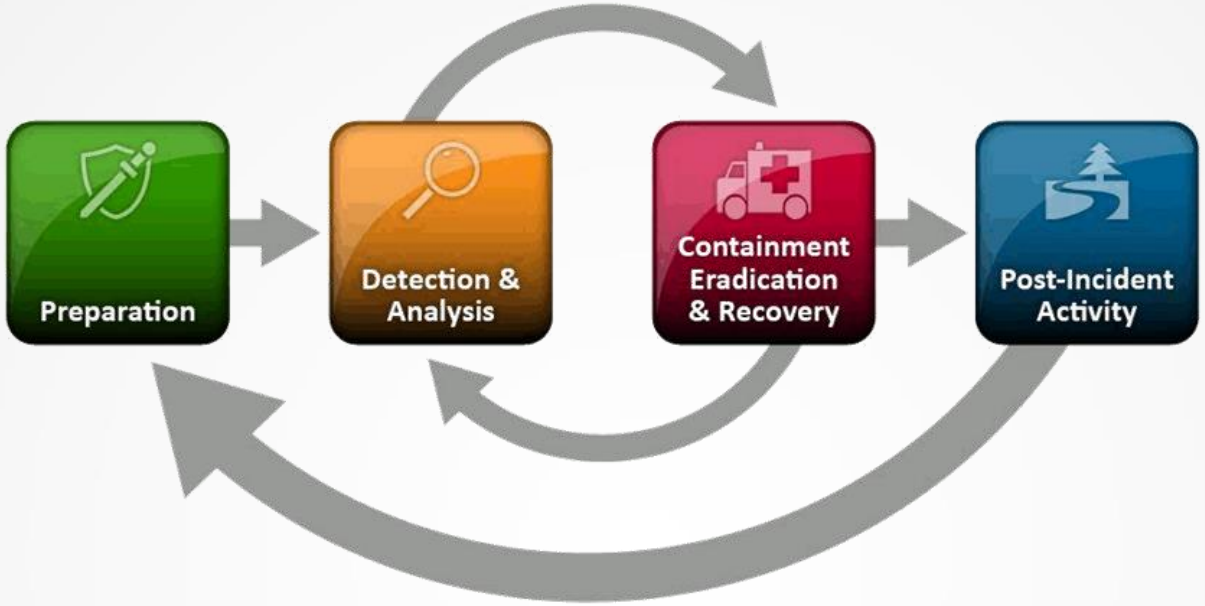
- Organisatie X heeft de volgende doelstelling voor het team gedefinieerd:
- *'X-CSIRT verzamelt en analyseert informatie over bedreigingen en incidenten en geeft advies aan de organisatie om incidenten in de toekomst te voorkomen'*
- Welke services gaat X-CSIRT leveren?

Re-actief
- Alerts and Warnings
- Incident analysis
- Vulnerability analysis
- Artifact analysis

Pro-actief
- Announcements
- Security Related Information
- Dissemination

NIST activiteiten

Preparation
- Preparing to Handle Incidents
- Preventing Incidents



Post-Incident Activity
- Lessons Learned
- Using Collected Incident Data
- Evidence Retention

Detection & Analysis
- Incident Categories
- Signs of an Incident
- Sources of Precursors and Indicators
- Incident Analysis

Containment Eradication & Recovery
- Choosing a Containment Strategy
- Evidence Gathering and Handling
- Identifying the Attacking Hosts
- Eradication and Recovery

Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SECURITY ACADEMY

Goodie bag

- Documenten
  - Incident Management, Whitepaper Georgia Killcrece - Software Engineering Institute, Carnegie Mellon University – december 2005
  - Handbook for Computer Security Incident Response Teams (CSIRTs), Moria J. West-Brown, Don Stikvoort e.a. - Engineering Institute, Carnegie Mellon University – 2^{e} Edition april 2003
  - Strategies for Incident Response and Cyber Crisis Coorperation – ENISA – Version 1.1, August 2016
  - Computer Security Incident Handling Guide – NIST Special Publication (SP) 800-61 Revision 2, August 2012
  - CIS Controls V7 – Center for Internet Security – Maart 2018

- Websites
  - https://searchsecurity.techtarget.com/
  - https://www.sei.cmu.edu/about/divisions/cert/index.cfm
  - https://www.nist.gov/cyberframework
  - https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map
  - https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
  - https://www.first.org/
  - https://www.trusted-introducer.org/