

Topic 7 Incident Management

Dr Diarmuid Ó Briain

6 Nov 2024



Licence



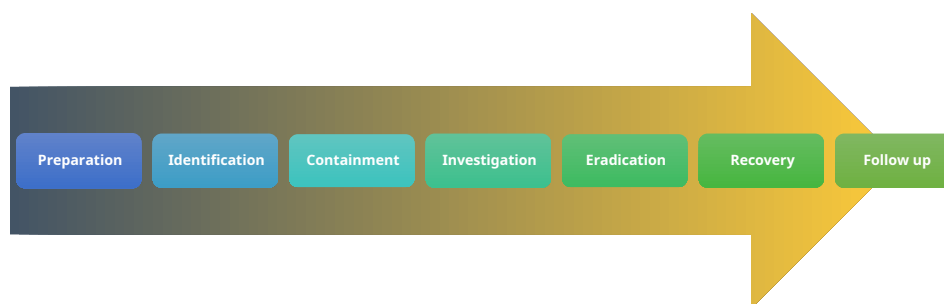
This work is licensed under a Creative Commons
Attribution-ShareAlike 4.0 International License.
Full License: <http://creativecommons.org/licenses/by-sa/4.0>

Learning objectives

By the end of this topic you will be able to:

- Analyse the benefits and drawbacks of different OT Computer Security Incident Response (IR) Teams (CSIRT) structures
- Evaluate the effectiveness of various OT-CSIRT roles and responsibilities
- Design an OT-CSIRT resource allocation plan that optimises cost and performance
- Develop a cyber Incident Response Plan (IRP) that is tailored to the specific needs of an organisation

Incident Response



CSIRT

- The first step in developing an IR capability is team organisation, an Computer Security IR Teams (CSIRT)
- Composed of specialists dedicated to this effort or part-time staff with other day-to-day responsibilities
- In this topic, the OT-CSIRT will refer to the internal response team that is directly supporting the OT
- Other external response teams are organised around specific technical areas or along geographical or organisational boundaries

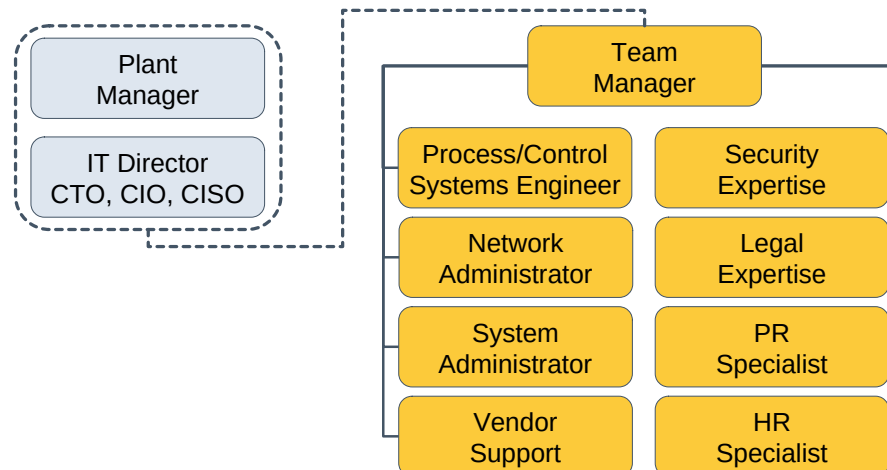
OT-CSIRT Responsibilities

- Acting as an expert resource on cybersecurity threats and vulnerabilities
- Serving as a clearing house for incident prevention, information, and analysis
- Developing organisational policies and procedures related to IR
- Understanding safeguards on the OT
- Identifying operational impacts to the organisation in the event of an incident
- Creating and testing the IRP
- Acting as a single point of contact for all internally reported incidents or suspected incidents
- Responding to the incident when one occurs
- Reporting to key stakeholders and external agencies after the incident such as the National Cyber Security Centre (NCSC) and the Gardaí or police
- Gathering forensic information to support analysis and as evidence for legal actions
- Implementing safeguards to prevent a recurrence of the incident
- Remediating the OT after the incident

OT-CSIRT Organisation

- Centralised
- Distributed
 - Include a strong central OT-CSIRT
 - Remote teams may include contracted specialists or even part-time staff
 - Emphasis on communications and coordination between teams
 - Remote team to be onsite at the source of the incident

OT-CSIRT Orgnisation



Policies and Procedures

- IR decisions are being made under pressure of production stoppage, high financial cost, inconvenient times such as those where authority may not be readily available
- Procedures and supporting policies to be developed while team members are not under pressure is crucial
- Clearly written, detailed operating procedures that are tested before an event occurs and published within the organisation
- Problems in the mechanics, accuracy, and timeliness of the procedures should be discovered during the development phase, when adjustments can be made, rather than in the middle of an actual response

Incident Response Plan

- The initial IRP should:
 - Direct the establishment and define the authority of the OT-CSIRT
 - Lay the foundation for the IRP
 - Although many additional security-related policies exist that should be considered, those that relate more directly to OT are as follows:
 - Human Resources
 - Information Disclosure
 - Communications

Building the Cyber IRP

- **Overview, Goals, and Objectives**
 - Define what will be accomplished
 - Organisation can provide direction and guidance for overall business objectives in comparison to the response options to the incident

Building the Cyber IRP

- **Incident Description**
 - Many IT-type incidents are fairly easily classified, i.e. DoS, unauthorised access, accessing protected and private information, defacing web pages, misuse of services, etc.
 - In the OT environment, clear definitions of what is a security incident must be identified and communicated
 - Differentiate between a cybersecurity and non-cybersecurity incident
 - Accurate descriptions of an incident will also prevent unnecessarily activating the OT-CSIRT

Building the Cyber IRP

• Incident Detection (Discovery)

- Includes ways in which an incident is identified and reported
- Detecting most incidents will require automated analysis tools, system behaviour patterns, and an awareness of what to look for among operators, supervisors, and other staff
- Operators and the process engineers are usually critical to detection of unusual operations and are the first to note a difference in system behaviour
- The IRP must address automated systems, expectations for staff, contractors, and partners when suspicious activity is detected; and procedures for help desk and call centre staff

Building the Cyber IRP

• Incident Notification

- Identified event needs to be prioritised to determine the cause and whether this is a minor system event or if it requires immediate escalation
- This section of the plan should identify the contact information for incident reporting:
 - Basic work phone
 - Mobile phone
 - E-mail
 - Instant messaging
 - Pager information for internal staff

Building the Cyber IRP

• Incident Notification

- This section of the plan should also address the following circumstances:
 - After-hours phone and pager
 - Offsite contact numbers
 - Contact information for customers and partners
 - Phone or pager numbers for backup staff
 - Contact information for management and rules for escalation
 - Criteria for filtering out false positives
 - Contact information for any relevant regulatory authorities
 - NCSC contact numbers and information
 - Vendor/integrator responsibilities and contact information

Building the Cyber IRP

• Incident Analysis

- Address how to evaluate and analyse a reported incident
- In this stage of incident management, those receiving the report must determine:
 - Impact on the facility or personnel safety may be caused by the event
 - If incident is real or a false positive
 - What stage the incident is in; beginning, in process, or has already occurred
 - What the impact might be to the organisation
 - The specific type of incident
 - What systems and equipment are or may be affected by the incident
 - If the system has failed over to an available backup system
 - If the incident has the potential to spread
 - What organisations will be affected and who should be part of the response

Building the Cyber IRP

• Response Actions

- Defines the procedures to follow for each type of incident detected
- When defining the response actions, consider the following:
 - The response must be directly associated with the incident type
 - The plan must account for contingency situations
 - The actions identified in the plan must include a comprehensive response covering
 - Containment of the problem
 - Restoration of operations prevention of a reoccurrence
 - The response procedures should be tested in a situation as realistic as is practical
 - The response actions must be weighed against business impact and approvals secured in the planning stages
 - All available perspectives should be involved in preparing the plan
 - The actions must take into consideration any forensics requirements

Building the Cyber IRP

• Communications

- The communications section should include:
 - Lists of all necessary contacts in the media, emergency responders, civil authorities, and local and global organisational contacts
 - A designated point of contact to speak for the organisation when an incident occurs
 - Prepared and vetted statements and press release information, available for immediate use
 - Reporting chains both internal and external to the organisation
 - A current list of contact names with the respective skill sets at key vendors for critical systems and components in the overall OT
 - A description of alternate methods to handle impaired communications

Building the Cyber IRP

• Forensics

- Collecting, examining, and analysing data related to an incident along with protecting incriminating evidence for use in legal action against a suspected offender
- This data can be found in:
 - Available logs, Physical components, E-mails, voicemail, texts, and telephone records.
 - Recommended practice (NISTIR 8428) is available that focuses completely on cyber forensics related to OT
 -

Building the Cyber IRP

• Exercising the Plan

- Conduct and evaluate the results from an IR drill
- Review, analyse, and change the procedures without suffering the effects of catastrophic decisions or even lost production
- Evaluate unexpected behaviour during drills
- Adjust and making the plan more effective and streamlined prior to a full test

Building the Cyber IRP

• Exercising the Plan

- When setting up the IR simulation, consider:
 - Drills should address as many critical scenario types as possible and the nature of the drill adjusted accordingly
 - Mimic real-world conditions as much as is practically possible in order to discover weaknesses in the IRP
 - The drill should simulate worst-case conditions
 - Involve all those who may be involved in the response and mitigating efforts
 - Hold drills regularly
 - Cause the staff to think through unusual situations.
- OT-CSIRT should draw upon the experience of other facilities in preparing for the drills and potential incidents

INSPIRING FUTURES

setu.ie | 21

Building the Cyber IRP

• System State and Status Reporting

- Associate automated mechanisms with the hardware or software that report information about the system
- Use debugging software tools for incident detection and resolution
- Approaches to automating system components are:
 - Networks Intrusion Detection Systems (NIDS)
 - Protocol-based Intrusion Detection System (PIDS)
 - Host-based Intrusion Detection System (HIDS)
 - Intrusion Prevention System (IPS)
- Because of the immaturity of IPS technology and the high risk of inadvertently causing OT failure, these systems are not currently recommended for OT environments
- Extensive preliminary testing to ensure OT compatibility is highly recommended before system deployment

INSPIRING FUTURES

setu.ie | 22

Building the Cyber IRP

• System State and Status Reporting

- Network Device Logging
- Configuration of Data Generators
 - Where will the log files be stored?
 - How long will the log files be stored?
 - Will older log files be deleted or archived?
 - What parameters are being investigated? (Ports, login/logout times, abnormal traffic cycles and times, etc.)



INSPIRING FUTURES

setu.ie | 23

Incident Prevention

- Preventing a cyber incident is preferable to responding to one
- Much more difficult task in OT due to AIC vs CIA
 - Patch Management
 - Vendor Interaction

INSPIRING FUTURES

setu.ie | 24

Patch Management

- Difficulties in scheduling maintenance windows on production systems to perform the patch
- Equipment that is no longer supported and no patches are available
- Patches that were issued by a third party, not the original vendor or supplier
- Testing of a patch in a non-production environment before implementing it on the production systems, especially where equipment is unique and expensive
- Creating a test bed or simulated environment
- Creating a viable backup of the system configuration as a DR point of the working system, if the last known good configuration needs to be deployed

Patch Management

- Development of patch roll-back procedures, should it be discovered that a patch interferes with proper OT operation
- Patches that cause issues with adjacent applications in the OT
- Receiving patches from vendors in a timely fashion
- Accepting the testing processes used by the vendor, including both unit and integrated system tests
- Assuming the risk that the patch will not bring down or impact the production system
- Knowing the time it takes to deploy the patch, or knowing how long it takes to remove the patch if necessary
- Working with and patching software embedded in OT components

Vendor Interaction

- OT products can have a long service life extending 20 years or more
- Number of customers is relatively small when compared with products in the IT environment
- Interaction between the customer and the technical staff of the vendor is critical
 - Establish an SLA with vendors to ensure ongoing patches and related support
 - Participate in customer user groups and provide ongoing feedback to the vendor's technical and sales staff.
- When responding to an incident
 - The relationship of technical or support staff at the vendor site is critical
 - Consider the inclusion of the vendor's technical personnel as an extension of the OT-CSIRT
 - This may require contracts with SLAs that define what help can be expected

Incident Management

- Four key primary activities:
 - Detection
 - Containment
 - Remediation
 - Recovery and Restoration

Incident Detection

• Detection by Observation

- User observation of abnormal system or component behaviour by any member of the organisation, including operators, process engineers, or system administrators
- After-the-fact approach
- An intrusion and cyber attack is currently taking place or has already occurred
- No initial protection or prevention capability provided to a cyber incident

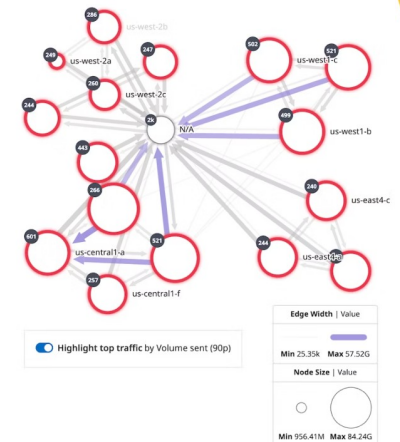
• Automated Detection Methods

- Applications or routines, such as
 - Network monitors and Network traffic analysis applications
 - IDSs and antivirus programs can detect and flag malware, intrusion attempts, policy violations, and exploits, as well as component failure
- Automated approaches still require some human interaction for configuration, review, analysis, and action

Incident Response Tools

• Network Performance and Monitoring

- Network Performance Monitors
- Availability Monitors
- Application Monitors

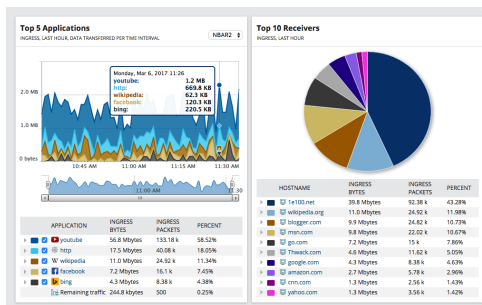


DataDog Network Performance Monitoring

Incident Response Tools

• Network Traffic Analysis

- Netflow Capture and Analysis
- Packet and Traffic Reconstructors



SolarWinds NetFlow Analyzer

Incident Response Tools

• Network Troubleshooting

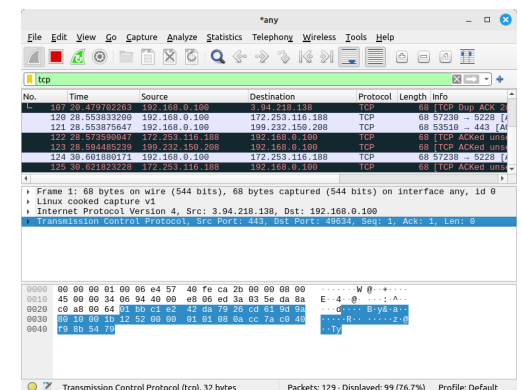
- Protocol Analyser
- Traceroute and whois tools

```

-$ traceroute www.setu.ie
traceroute to www.setu.ie (172.67.41.36), 30 hops max, 60 byte packets
 1  gateway (192.168.0.1) 1.811 ms 2.758 ms 2.653 ms
 2  109.255.186.1 (109.255.186.1) 10.439 ms 17.298 ms 18.767 ms
 3  109.255.251.158 (109.255.251.158) 15.093 ms 14.993 ms 16.888 ms
 4  162.159.36.15 (162.159.36.15) 24.042 ms 23.957 ms 23.866 ms
 5  172.67.41.36 (172.67.41.36) 22.222 ms 23.690 ms 23.606 ms
    
```

```

-$ whois setu.ie
Domain Name: setu.ie
Registrar Domain ID: 700080-IEDR
Registrar WHOIS Server: whois.weare.ie
Registrar URL: https://www.heatnet.ie/services/hosting/domain-registration
Updated Date: 2023-03-04T14:58:07Z
Creation Date: 2011-01-18T00:00:00Z
Registry Expiry Date: 2024-01-18T14:51:28Z
Registrar: HEAnet
Registrar IANA ID: not applicable
    
```



Security Information and Event Management (SIEM)

- SIEM tools are versatile tools that can be used for a variety of network security and monitoring tasks
 - Industrial Defender, LogRhythm, Siemens, Waterfall Security, Dragos Industrial Security Platform



Incident Categorisation

- Cyber attacks should be categorised, and the response prioritised based on that categorisation
- Categorisation should be based on the type of incident and the potential damage to the OT
- Type of incident will drive the appropriate level of response. The IRP should outline in detail what the level of response (and level of effort) should be for each type of incident
- This planning should occur well in advance of an actual event
- The prioritisation of the response should be based on the current and potential effect to the OT, and the criticality of the effected equipment and system to company operations

Incident Categorisation

- The following are recommended categorisation/prioritisation steps to take:
 - Assign a principal investigator responsible for identifying and mitigating each incident
 - Validate if the incident is a malicious or non-malicious occurrence. If the event is non-malicious, the full OT-CSIRT will not be required, though some resources may be used to solve the problem
 - Identify and evaluate the evidence in detail and keep accurate documentation with controlled access to the evidence
 - Coordinate with the specific personnel that provide operating business unit network services to the effected system
 - Specific steps unique to the organisation should be included. They should be clearly defined in the IRP and should guide the actions of the OT-CSIRT when categorising and prioritising an incident

Incident Containment

- The primary case for containment is where malware in some form has been left on the OT
- **Malware**
 - Stop the spread to other parts of the system
 - Prevent continued damage to the OT within an isolated segment
- **Malware containment**
 - Automated technologies such as virus removal programs to eliminate the problem and restore system functions
 - Only acts against known malware and cannot remediate Zero Day vulnerabilities
 - Halt services while the incident is being handled
 - Disruptive measure typically disabling a service
 - Block certain types of network connectivity by using a filtering process
 - Effective and quick means of temporarily restricting network connectivity to infected systems attempting to establish connection to an external system

Incident Remediation

- **Fix the source of the problem**
 - May include eradication of any malware left on the system, removal or replacement of vulnerable equipment, reconfiguration and patching of equipment or software, and possible access cancellation for certain personnel
- **Careful analysis should be performed to verify the path taken by the intruder**
 - Automated eradication tools: antivirus software, spyware detection and removal utilities, and patch management software
 - Restore system to a set point before the infection or reloading key system files
 - Reinstallation and securing of the OS and application followed by restoring data from backup files

Incident Remediation

- A complete rebuild should be considered if the following system characteristics are present:
 - The intruder gained root or administrator-level access to the system
 - Back-door type access has been granted that is not readily identified
 - System files were replaced by the malware or directly by the intruder
 - The system is unstable or does not function properly after antivirus software, spyware detection and removal utilities, or other programs or techniques eradicate the malware

Incident Recovery and Restoration

- Establish contingency plans with available equipment identified before the incident
- Patch and maintain all backup systems to the same level as the primary systems
- Conduct regular and planned testing at a planned specific time to verify plans
- Establish plans to run segments of the OT in isolation prior to an incident
- Test backup equipment against realistic time-frames found in a worst-case scenario
- Establish and run acceptance tests and procedures
- Define procedures as part of the IRP to provide for the proper authority to accept the tests and declare the OT fully operational

Post Incident Analysis and Forensics

- **Lessons learned**
 - Where an attempt is made to analyse the incident, the response, and the impact to discover and document what could have been done differently to improve the response
- **Recurrence prevention**
 - Applying what was learned in remediating discovered weaknesses in the cybersecurity programme
- **Forensics**
 - Includes capturing and protecting data as evidence for potential legal actions

Incident Recurrence Prevention

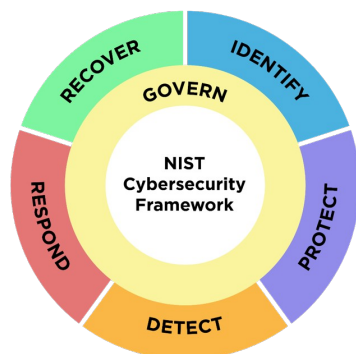
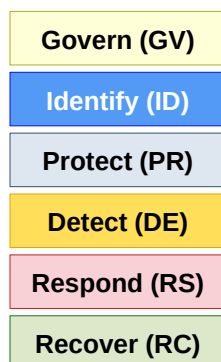
- Once a vulnerability has been discovered, it will remain an open door until preventive action is taken
- One of the primary purposes of the lessons learned exercise is to analyse the incident and initiate action to prevent a recurrence of the exploit
- Considerations following on the incident:
 - Identify access methods
 - Understand intruder motivation
 - Assess and strengthen specific OT components
 - Review detection methods

NIST

SP 800-61 Rev 3 DRAFT Incident Response

CSF 2.0 Functions

- Describes essential cybersecurity outcomes that can help an organisation reduce its cybersecurity risk.



CSF 2.0 Functions

Govern (GV)	Establish and monitor the organisation's cybersecurity risk management strategy, expectations, and policy
Identify (ID)	Help determine the current cybersecurity risk to the organisation
Protect (PR)	Use safeguards to prevent or reduce cybersecurity risk
Detect (DE)	Find and analyse possible cybersecurity attacks and compromises
Respond (RS)	Take action regarding a detected cybersecurity incident
Recover (RC)	Restore assets and operations that were impacted by a cybersecurity incident

NIST SP 800-61r3 Draft

- NIST considers earlier models as no longer reflecting the current state of IR.
- Today, incidents occur frequently and cause far more damage.
- Recovery can take weeks or months due to their breadth, complexity, and dynamic nature.
- IR should be integrated across organisational operations.
- The lessons learned during IR should often be shared as soon as they are identified, not delayed until after recovery concludes.
- Continuous improvement is necessary to keep up with modern threats.

NIST SP 800-61 rev 3 and CSF 2.0 Functions

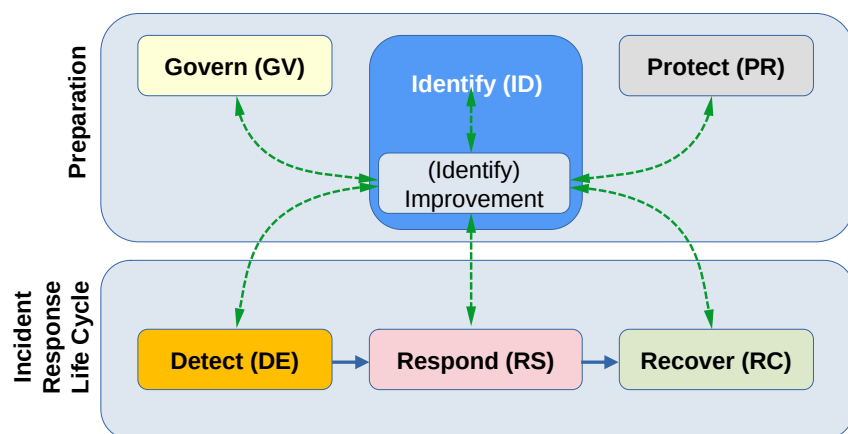
Preparation Activities


Govern (GV)	Establish and monitor the organisation's cybersecurity risk management strategy, expectations, and policy
Identify (ID)	Help determine the current cybersecurity risk to the organisation
Protect (PR)	Use safeguards to prevent or reduce cybersecurity risk

Incident Response Activities

Detect (DE)	Find and analyse possible cybersecurity attacks and compromises
Respond (RS)	Take action regarding a detected cybersecurity incident
Recover (RC)	Restore assets and operations that were impacted by a cybersecurity incident

NIST SP 800-61 rev 3 - Incident Response Lifecycle






Ollscoil
Teicneolaíochta
an Oirtheisirt
South East
Technological
University

Exercise #6.1

Lessons Learnt Exercise



INSPIRING FUTURES

Lessons Learnt Exercise

- In a Lessons Learnt exercise, what are the key questions that should be answered?
 - Break away and list the questions you think should be answered as part of the exercise
 - Lecturer will facilitate a discussion on the question



5

Learning objectives

You should now be able to:

- Analyse the benefits and drawbacks of different OT CSIRT structures ✓
- Evaluate the effectiveness of various OT-CSIRT roles and responsibilities ✓
- Design an OT-CSIRT resource allocation plan that optimises cost and performance ✓
- Develop a cyber IRP that is tailored to the specific needs of an organisation ✓

**TUS**
Ólíscoil Teicneolaíochta na Sionainne:
Lia Tíre, An tIarthar Láir
Technological University of the Shannon:
Midlands Midwest



EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir
Sinsearach

✉ diarmuid.obriain@tus.ie | www.tus.ie
Campas Maolais, Páirc Maolais,
Luimneach, V94 EC5T, Éire



Thank you

