Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Topic 8 Incident Management

Dr Diarmuid Ó Briain

12 Aug 2025

Version: 3.0

Licence

Learning objectives

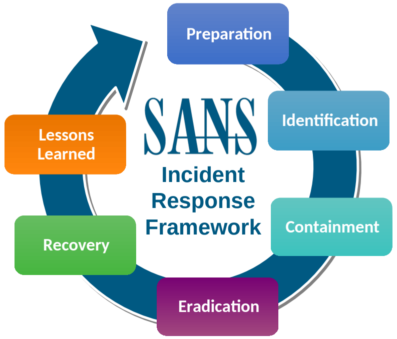
By the end of this topic you will be able to:

- Explain the phases of the SANS Incident Response Framework (IRF)
- Identify and apply various methods for incident detection and containment
- Formulate a comprehensive Incident Response Plan (IRP) that incorporates team roles, policies, procedures, and considerations for Operational Technology (OT) environments
- Summarise the core principles of the ISO/IEC 27035 standards and NIST SP 800-61r3 and explain how they guide incident management practices
- Describe the crucial steps for incident eradication and recovery

SANS

Incident Response

SANS Incident Response Framework


SANS
Incident Response Framework
Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned

- Get ready for incidents by creating a plan, defining roles, and establishing a CSIRT
- Detect and analyse incidents to determine their nature, scope, and severity
- Stop the incident from spreading by isolating affected systems and taking immediate action
- Remove all traces of the threat, including malware and vulnerabilities
- Restore affected systems to a normal, secure state, which may involve using backups or rebuilding
- Review the incident to understand what happened and how to improve for the future

Preparation — 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

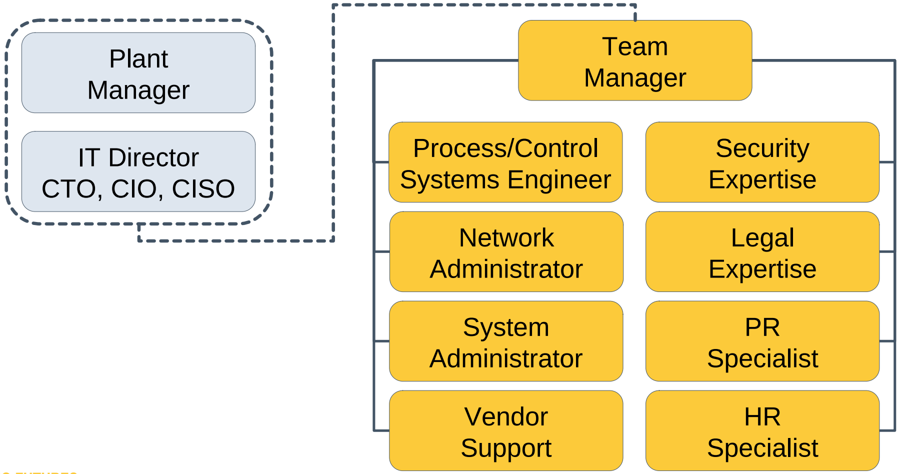
Preparation — OT-CSIRT: Responsibilities

- Acting as an expert resource on cybersecurity threats and vulnerabilities
- Serving as a clearing house for incident prevention, information, and analysis
- Developing IR related organisational policies and procedures
- 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 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

Preparation — 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

Preparation — OT-CSIRT: Organisation



Plant Manager

IT Director CTO, CIO, CISO

Team Manager

Process/Control Systems Engineer

Security Expertise

Network Administrator

Legal Expertise

System Administrator

PR Specialist

Vendor Support

HR Specialist

Preparation — Policies and Procedures

- **Decisions under pressure**: IR decisions are often made under pressure due to production stoppages, high costs, and inconvenient timing
- **Proactive development**: Procedures and policies should be developed and tested when the team isn't under pressure
- **Clear documentation**: Create and publish clear, detailed procedures that are tested before an event occurs
- **Pre-event testing**: Problems with procedures should be discovered during the development phase, not during an actual incident

Preparation — 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

Preparation — IRP: Overview, Goals, 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

Preparation — 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

Preparation — 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

Preparation — 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

Preparation — 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

Preparation — 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

Preparation — 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

Preparation — 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

Preparation — 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

Preparation — 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

Preparation — 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

Preparation — IRP: System State & 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

Preparation — IRP: System State & 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.)

syslog

Preparation — IRP: 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

Preparation — IRP: 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

Preparation — IRP: 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

Preparation — IRP: 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

Identification — 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

Identification — Incident Detection

- Early detection is crucial to prevent damage to OT systems. Two main methods:
  - **User Observation**: Operators or engineers notice abnormal system behaviour
  - **Automated Detection**: Systems like network monitors, IDS, and antivirus programs flag issues

Identification — Detection by Observation

- User observation is "after-the-fact," meaning an incident is already underway
- This approach risks physical damage, data theft, and malware injection
- Watch for warning signs that could indicate an attack:
  - Unusual network traffic or high CPU usage
  - Unexpected user accounts, account lockouts, or cleared log files
  - Disabled security controls or unexpected patch changes
  - Erratic equipment behaviour or unexpected changes in configuration

Identification — Automated Detection Methods

- Automated systems are essential for 24/7 monitoring, as manual observation is often impossible
- Most networked OT systems have some form of automated detection, from simple firewall logging to sophisticated commercial IDS
- A proper balance of automation and human interaction is critical for success

Identification — Components of Automated Systems

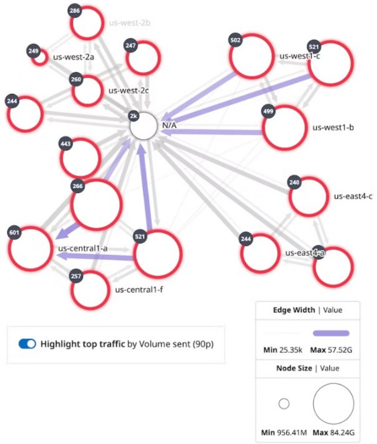
- **Detection Method**: The system must be programmed to recognise "out-of-range" events, such as a known virus signature, a denial-of-service attack, or an OT component behaving outside of pre-set thresholds
- **Event Reporting**: The system must capture and present data in a useful format, such as a log file or an audit table. For OT, it's often best to report only on deviations from normal
- **Human Communication**: The system must communicate flagged events to a human operator, who can then filter out false positives, separate maintenance issues from cyberattacks, and initiate an appropriate response

Identification — Improving Human Response

- Human observation and response are often the weakest link. To support OT personnel:
  - Centralise Logging: Consolidate data from various sources into a single, consistent format
  - Filter Data: Use algorithms to process raw data and simplify what the operator needs to review
  - Create Effective Alerts: Set up automated email, pager, or audible alarms for critical events
  - Ongoing Training: Continuously train analysts to improve detection algorithms and teach operators to better understand the data

Identification — Incident Response Tools

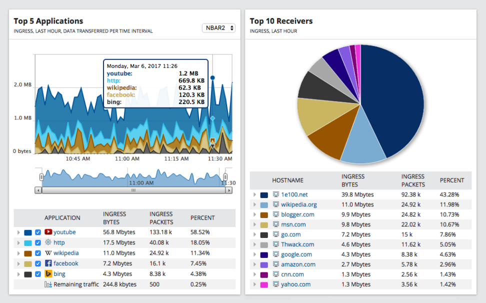
- **Network Performance and Monitoring**
  - Network Performance Monitors
  - Availability Monitors
  - Application Monitors



DataDog Network Performance Monitoring

Identification — Incident Response Tools

- **Network Traffic Analysis**
  - Netflow Capture and Analysis
  - Packet and Traffic Reconstructors



Top 5 Applications
INGRESS, LAST HOUR, DATA TRANSFERRED PER TIME INTERVAL
NBAR2

Monday, Mar 6, 2017 11:26
youtube: 1.2 MB
http: 669.8 KB
wikipedia: 62.3 KB
facebook: 120.3 KB
bing: 220.5 KB

APPLICATION	INGRESS BYTES	INGRESS PACKETS	PERCENT
☑ youtube	56.8 Mbytes	133.18 k	58.52%
☑ http	17.5 Mbytes	40.08 k	18.05%
☑ wikipedia	11.0 Mbytes	24.92 k	11.34%
☑ facebook	7.2 Mbytes	16.1 k	7.45%
☑ bing	4.3 Mbytes	8.38 k	4.38%
Remaining traffic	244.8 kbytes	500	0.25%

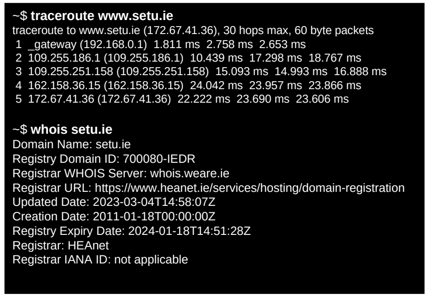
Top 10 Receivers
INGRESS, LAST HOUR

HOSTNAME	INGRESS BYTES	INGRESS PACKETS	PERCENT
1e100.net	39.8 Mbytes	92.38 k	43.28%
wikipedia.org	11.0 Mbytes	24.92 k	11.98%
blogger.com	9.9 Mbytes	24.82 k	10.73%
msn.com	9.8 Mbytes	22.02 k	10.67%
go.com	7.2 Mbytes	15 k	7.86%
Thwack.com	4.6 Mbytes	11.62 k	5.05%
google.com	4.3 Mbytes	8.38 k	4.63%
amazon.com	2.7 Mbytes	5.78 k	2.96%
cnn.com	1.3 Mbytes	2.56 k	1.43%
yahoo.com	1.3 Mbytes	3.56 k	1.42%

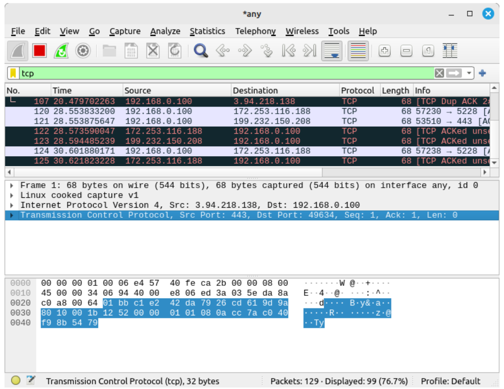
SolarWinds NetFlow Analyser

Identification — Incident Response Tools

- **Network Troubleshooting**
  - Protocol Analyser
  - Traceroute and whois tools



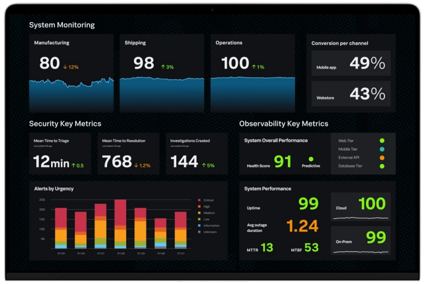
```
~$ traceroute www.setu.ie
traceroute to www.setu.ie (172.67.41.36), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  1.811 ms  2.758 ms  2.653 ms
 2  109.255.186.1 (109.255.186.1)  10.439 ms  17.298 ms  18.767 ms
 3  109.255.251.158 (109.255.251.158)  15.093 ms  14.993 ms  16.888 ms
 4  162.158.36.15 (162.158.36.15)  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
Registry Domain ID: 700080-IEDR
Registrar WHOIS Server: whois.weare.ie
Registrar URL: https://www.heanet.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
```


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

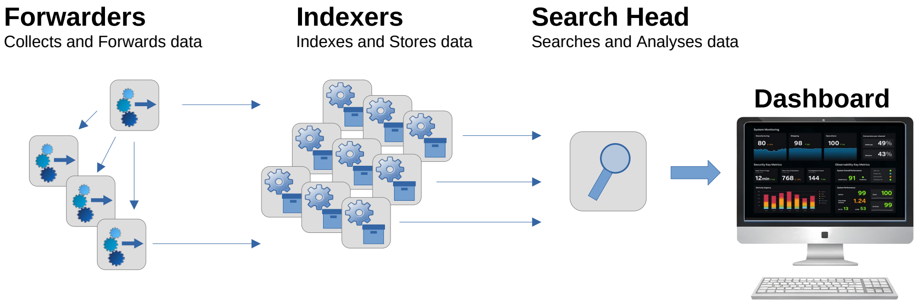
```
tcp

No.   Time          Source           Destination      Protocol Length Info
  107 20.479702263  192.168.0.100    3.94.218.138     TCP      68 [TCP Dup ACK 2
  120 28.553833200  192.168.0.100    172.253.116.188  TCP      68 57230 → 5228 [A
  121 28.553875647  192.168.0.100    199.232.150.208  TCP      68 53510 → 443 [AC
  122 28.573590047  172.253.116.188  192.168.0.100    TCP      68 [TCP ACKed unse
  123 28.594485239  199.232.150.208  192.168.0.100    TCP      68 [TCP ACKed unse
  124 30.601880171  192.168.0.100    172.253.116.188  TCP      68 57238 → 5228 [A
  125 30.621823228  172.253.116.188  192.168.0.100    TCP      68 [TCP ACKed unse

▸ Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 3.94.218.138, Dst: 192.168.0.100
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 49634, Seq: 1, Ack: 1, Len: 0

0000  00 00 00 01 00 06 e4 57  40 fe ca 2b 00 00 08 00   ·······W @··+····
0010  45 00 00 34 06 94 40 00  e8 06 ed 3a 03 5e da 8a   E··4··@· ···:·^··
0020  c0 a8 00 64 01 bb c1 e2  42 da 79 26 cd 61 9d 9a   ···d···· B·y&·a··
0030  80 10 00 1b 12 52 00 00  01 01 08 0a cc 7a c0 40   ·····R·· ·····z·@
0040  f9 8b 54 79                                        ··Ty

Transmission Control Protocol (tcp), 32 bytes    Packets: 129 · Displayed: 99 (76.7%)    Profile: Default
```

Identification — Security Info & Event Management

- 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



Identification — Splunk Data Pipeline



Forwarders
Collects and Forwards data

Indexers
Indexes and Stores data

Search Head
Searches and Analyses data

Dashboard

Identification — Categorisation & Prioritisation

- **Categorise**: Classify the incident based on its type and potential damage to the OT
- **Prioritise**: Prioritise the response based on the incident's effect and the criticality of the affected equipment to operations
- **Plan Ahead**: This planning should be detailed in the IRP and occur well before an actual event

Identification — Key Questions for Categorisation

- How did the exploit occur? Was it internal or external?
- What type of tools were used?
- What systems and networks are affected? Can the problem spread?
- Are there legal or safety issues?
- How quickly could the impact escalate if not contained?
- Can systems safely fail-over?
- How critical are the affected components?

Identification — Recommended Prioritisation Steps

- **Assign an Investigator**: A principal investigator should be responsible for each incident
- **Validate Maliciousness**: Determine if the incident is malicious or non-malicious. A non-malicious event may not require the full OT-CSIRT
- **Evaluate Evidence**: Carefully document and evaluate all evidence
- **Coordinate**: Work with the business unit personnel who provide network services to the affected system
- **Define Steps**: The IRP should clearly define specific, unique steps for categorising and prioritising incidents

Containment

- Containment is a crucial step for any incident, from malware to unauthorised access
- The main goals are to stop the spread and prevent further damage to OT systems
- Strategies are not one-size-fits-all; they depend on the malware, the system, and your organisation's risk tolerance

Containment — Methods to isolate threats

- **Automated Technologies**
  - using tools like antivirus for known threats
- **Halting Services**
  - temporarily disabling services to stop spread while keeping other components online
- **Disabling Connectivity**
  - restricting network access to infected systems to completely isolate them

Eradication

- Eradication removes the root cause of the problem, whether it's malware, vulnerabilities, or unauthorised access
- The goal is to remove the threat with minimal disruption
- Removal methods include automated tools and system restoration
- A full system rebuild is needed for severe infections, such as when an attacker gains administrative access
- Always verify after removal to ensure the system is clean and working correctly

Recovery — Recommendations

- OT recovery has unique challenges because critical services often can't be shut down
  - This means using temporary workarounds such as fail-over systems or isolating components, which can introduce new risks
- Redundancy is key, but triple redundancy is often too expensive
  - When backups fail, production stops, creating immense pressure to restore operations fast

Recovery — Recommendations

- **Plan and prepare in advance**: Have contingency plans, maintain patched backup systems, and regularly test your fail-over procedures
- **Create isolation plans**: to understand how parts of your OT system can run independently if needed
- **Set realistic expectations**: by testing your backup equipment for worst-case scenarios, such as needing power for days, not just hours
- **Conduct acceptance tests**: to ensure systems are fully restored and more secure than before the incident
  - Define who has the authority to declare the OT system operational

Lessons Learned Exercise

- **Post-incident analysis**: is a critical opportunity to improve security posture. It helps identify weaknesses and prevent a similar incident from happening again
- **Conduct the exercise as soon as possible**: after recovery to avoid leaving the OT system vulnerable to the same exploit
- **Ensure all OT-CSIRT members participate**: and that the process is well-structured
- **Get external input from vendors or other experts**

Lessons Learned — Key Questions to Address

- What systems were affected and how?
- How was the incident detected, and could we have found it earlier?
- What vulnerabilities allowed the breach?
- What went wrong in the response process (communication, authority, etc.)?
- What changes are needed to our standards, procedures, and solutions?

Lessons Learned — Prevent Recurrence

- **Strengthen access methods**: by identifying how the intruder got in. Solutions could range from better background checks for insider threats to additional antivirus for malware
- **Understand the intruder's motivation**: was it to steal data or cause physical damage? This helps you prioritise security resources on the most likely targets
- **Assess and strengthen components**: that were exploited. This analysis can justify replacing outdated equipment, patching systems, or strengthening security around critical devices
- **Review and improve detection methods**: An incident often reveals that your detection systems were not strong enough to catch the threat early

Overview of ISO/IEC 27035

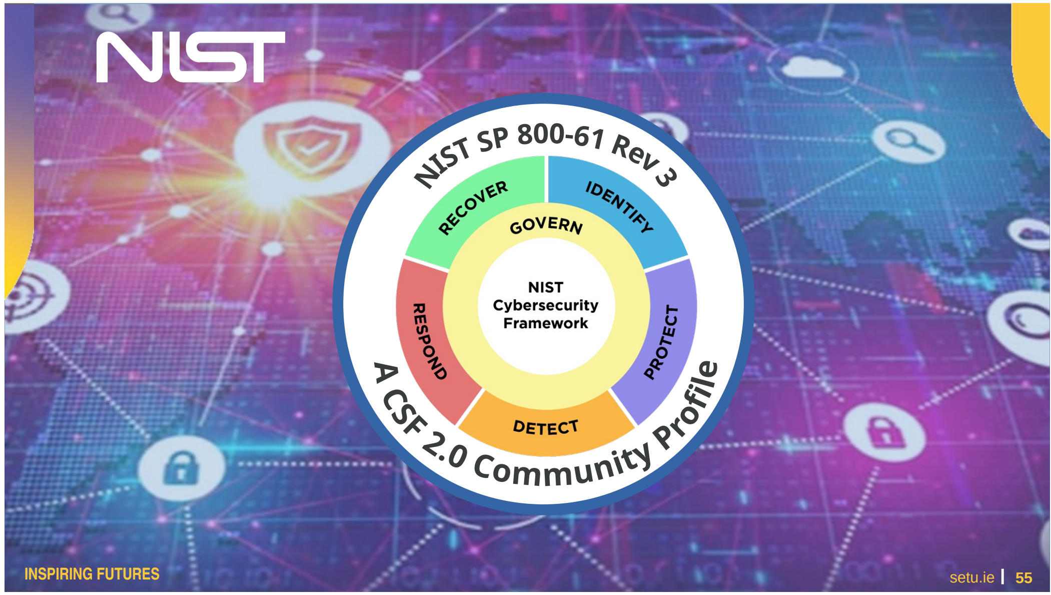
- ISO/IEC 27035 is an international standard for information security incident management from the ISO/IEC 27000 series
- It provides a comprehensive framework for an organisation's IR programme
- The series is broken into multiple parts, each focusing on a specific aspect of incident management

ISO/IEC 27035-1: Principles and Process

- This is the foundational document of the series
- It outlines a generic, five-phase process for managing incidents:
  - **Plan and Prepare**: Establish policy, team, and training
  - **Detect and Report**: Identify and report security events
  - **Assess and Decide**: Evaluate if an event is an incident
  - **Respond**: Investigate, contain, and recover
  - **Learn Lessons**: Analyse the incident to improve future security
- It covers the full lifecycle of an incident, including proactive planning and post-incident review

Other Parts of the ISO/IEC 27035 Series

- **Part 2** gives detailed guidance on the Plan and Prepare and Learn Lessons phases
- **Part 3** focuses on technical operations within a Security Operations Centre (SOC) for detection and response
- **Part 4** provides guidelines for coordinating IR between multiple organisations



CSF 2.0 Functions

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

Govern (GV)

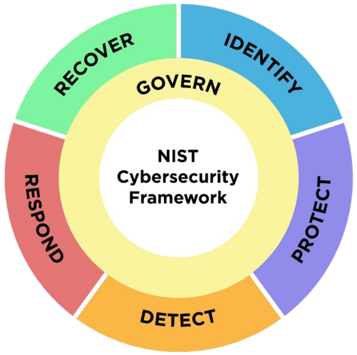
Identify (ID)

Protect (PR)

Detect (DE)

Respond (RS)

Recover (RC)



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 800-61 Revision 3

- 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 800-61r3 and CSF 2.0 Functions

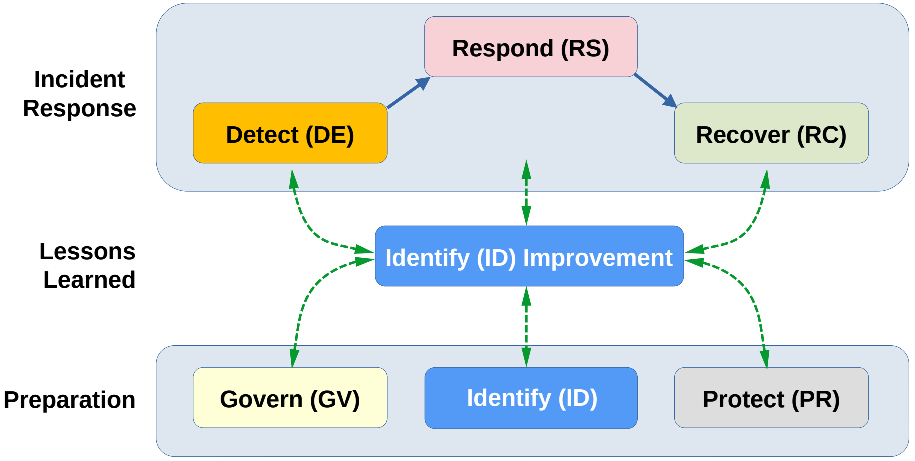
- **Preparation Activities**

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 800-61r3 - Incident Response Lifecycle

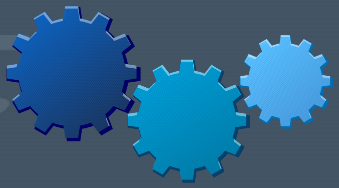


NIST SP 800-61r3 - Incident Response Lifecycle

- **IR is a cyclical process**: not a one-time event. It involves Detecting (**DE**) a threat, Responding (**RS**) to it, and Recovering (**RC**) from it
- **The Lessons Learned phase is crucial**: After an incident, you must Identify (**ID**) Improvement opportunities by analysing what happened
- **Preparation**: These identified improvements directly feed back into Preparation efforts
- **Insights from a lessons-learned exercise**: inform and strengthen the overall security posture, including Govern (**GV**), Identify (**ID**) risks, and Protect (**PR**) systems
- This model highlights how every incident, successful or not, should be used to make the organisation more resilient and prepared for future events

Exercise #6.1

Lessons Learnt Exercise



Lessons Learnt Exercise

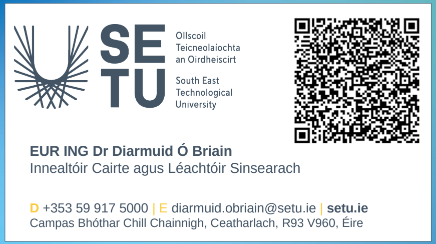
- In a Lessons Learnt exercise, what are the key questions that should be answered?
  - Break away and list the questions you think should be answered as part of the exercise
  - Lecturer will facilitate a discussion on the question

5

Learning objectives

You should now be able to:

- Explain the phases of the SANS IRF ✓
- Identify and apply various methods for incident detection and containment ✓
- Formulate a comprehensive IRP that incorporates team roles, policies, procedures, and considerations for OT environments ✓
- Summarise the core principles of the ISO/IEC 27035 standards and NIST SP 800-61r3 and explain how they guide incident management practices ✓
- Describe the crucial steps for incident eradication and recovery ✓



SE TU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

D +353 59 917 5000 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

SE TU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Thank you

engcore
advancing technology