INDUSTRIAL CONTROL SYSTEMS
Community of Interest

GUIDANCE: Considerations for Cyber Incident Response Planning within Industrial Control Systems/Operational Technology.

Introduction

This guidance is designed to help organisations understand specific considerations that are required within Industrial Control Systems (ICS)/Operational Technology (OT) systems and to better prepare for a cyber incident within an ICS/OT environment. It is designed to complement and to be read in conjunction with the NCSC's general Incident Response and Management guidance, and focuses on the specific and unique aspects relating to ICS/OT environments.

Having an effective Incident Response Plan in place also supports several Outcomes within the NCSC's Cyber Assessment Framework (CAF). A summary of the related Indicators of Good Practice (IGPs) covered in this guidance is shown at the end of this article.

If you are responsible for the management or maintenance of ICS/OT assets, this article will help you to navigate the challenges you may encounter when adopting mature incident response planning processes.

Per NCSC's guidance it is important to assume that your systems ICS/OT will be breached in the future, this could be due to:

- high numbers of legacy systems within ICS/OT environments,
- limited visibility in the operation of the systems from the perspective of asset management,
- limited visibility of network communications,
- communication conduits to external systems.

Additionally, ICS/OT environments, despite best efforts, can often be lacking in segregation from the Information Technology (IT) environment, and/or segmentation within the ICS/OT environment.

It is worth noting that for Operators of Essential Services (OES) covered by the Security of Network & Information Systems Regulations (NIS-R) that they would be regulated via the use of NCSC's CAF

and would have to have access to the appropriate logging and monitoring within their ICS/OT environments.

For those operators that are covered by the Health and Safety Executive, OG86, Appendix 2, Section D, details requirements for Incident Response planning.

While Cyber Incident Response Plans (IRPs) should cater for both IT and ICS/OT systems, consideration must be made for the key differentiators found in ICS/OT environments. So, in this article, we're going to walk through specific concerns in ICS/OT Incident Response preparation and planning.

We have broken the specific areas of concern down to the following:

- Preparation
- Detection
- Triage
- Taking responsive action
- Tracking and Reporting
- Stakeholder Engagement
- Lessons Learned

Preparation

Lessons learned from responding to high profile cyber-attacks provides a clear message that preparation is essential, such as the E-ISAC/SANS Defense Use Case1 from the Analysis of the Cyber Attack on the Ukrainian Power Grid.

Preparation - Define roles and responsibilities.

When considering roles and responsibilities within the ICS/OT Cyber IRP, here are a couple of considerations to make:

- For ICS/OT regardless of which teams perform analysis and/or collection, the roles and responsibilities should be clearly defined. This is particularly important in relation to plant operation, safety and decision making associated with production, quality, and safety, which requires the identification and neutralisation of the threat and building confidence that the system can be returned to a safe operational state.
- Incident Response companies that are held on retainer should be capable of being able to provide support with resources that are comfortable operating in hazardous environments. In some cases, those resources may need to be certified to operate on the industrial sites, so you should consider who to use and how to on-board them including any required health and safety inductions, drugs and alcohol checks etc.

Roles and Responsibilities should always include the following:

- Plant Operations
- Safety system and assurance managers
- Production managers

For further information on roles and responsibilities please see NCSC's Guidance on building A Cyber Security Incident Response Team (CSIRT).

An ICS/OT specific Incident Response decision tree describing how the communication will flow throughout the whole Incident Response lifecycle would help define the roles and responsibilities needed, and how key stakeholders will be integrated and called on/off.

Action point: Develop an ICS/OT specific Incident Response decision tree/play book.

It is important to establish Cross-Functional incident response teams, comprising members from both IT security and ICS/OT departments. Having pre-designated team leads who are responsible for coordinating communication, decision-making, and task assignments between the IT security and ICS/OT teams. These individuals and teams can share relevant threat intelligence, indicators of compromise (IOCs), and forensic findings between IT security and ICS/OT teams, across implemented secure communication channels and information sharing platforms.

Action point: Identify and train key individuals to act as the coordination point between IT and ICS/OT Teams.

Preparation - Prepare an ICS/OT specific Cyber Incident Response Plan

ICS/OT systems and networks are typically sensitive to availability and integrity requirements, requiring the Incident Response procedures to consider how systems can be interacted with for forensic collection. Those considerations should be documented in an ICS/OT specific response plan, which may have to cater for different systems used across an ICS/OT operator's estate, such as different sites, industrial processes, or functionality of the systems.

- **Action point:** Create an IRP that is specific to your ICS/OT environment.

Key sections to include in your ICS/OT Cyber IRP include the following:

- Scope
    - Consider whether the ICS/OT Cyber IRP is to be enforced, whether it covers all of your ICS/OT environment or is on a site or business unit basis. If the later, consider interaction points and escalation routes between teams.
- Contact details for key roles.
    - Appoint roles and provide their contact details.
- Description of Incident Response process covering the full lifecycle of an incident
    - Use established frameworks such as the SANS PICERL framework (as shown in Figure 1 below) or NIST.SP.800-61r2.
- Templates for recording and reporting incidents.
    - If you are an Operator of Essential Service (OES), produce a template for the reporting requirements to assist the IR team in ensuring that they capture the right information in a timely manner.

CISA have produced an excellent document providing further detail on what should be included within an ICS/OT Cyber IRP. The Information Commissioner's Office provides further details on reporting requirements for OES, although within in the UK each Competent Authority may have a specific requirement - for instance the Department for Energy Security & Net Zero (DESNZ) provide the following guidance for the Energy Sector, which is based on thresholds (see Annex D).

In addition to exercising the ICS/OT IRP as mentioned later in this article, training and awareness of on elements covered within the plan need to be provided to those identified within it as having responsibilities.

Action Point: Provide Training and Awareness to staff involved in the ICS/OT IRP, so that they are better trained for the roles they are responsible for.

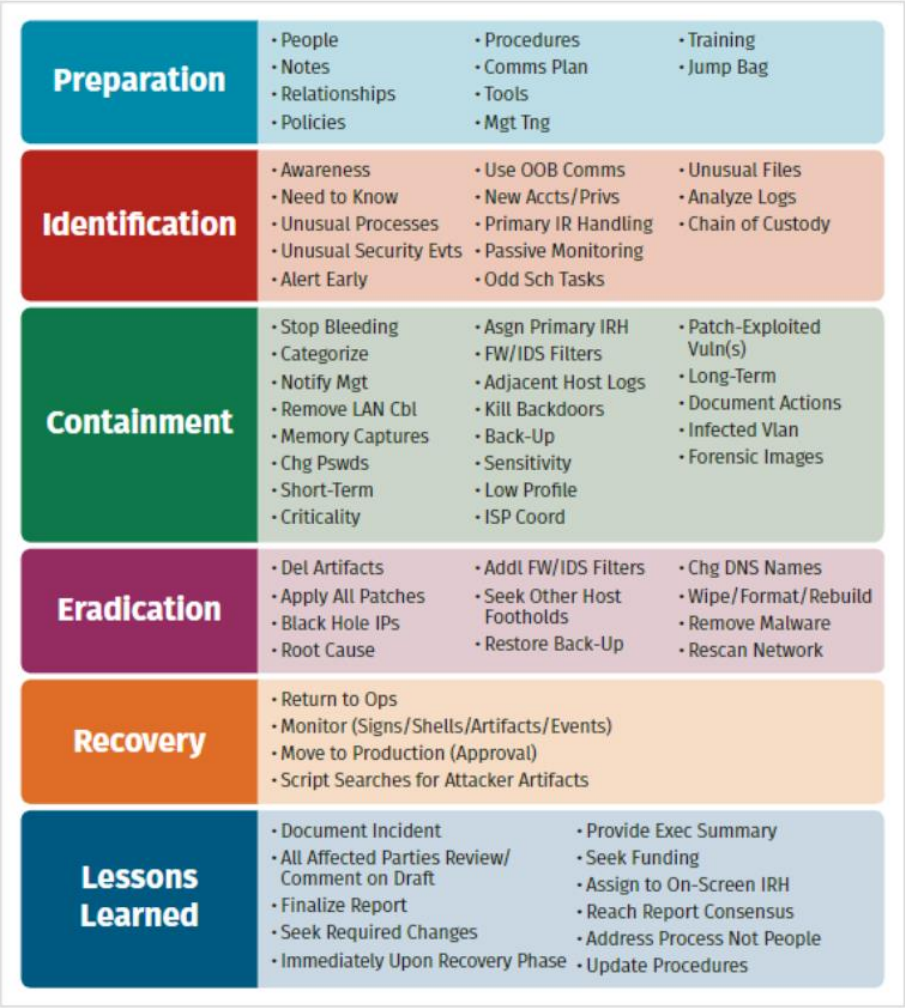

Figure 1. PICERL Phases[7]

Figure 1 - Six Phases in the Incident Response Plan (PICERL)

Detection

Detection of cyber security events from ICS/OT networks has been a long-standing challenge for ICS/OT operators, particularly those with legacy systems which were not designed with security in mind. Being able to detect, correlate and analyse events from ICS/OT is crucial in being able to respond and recover from an incident.

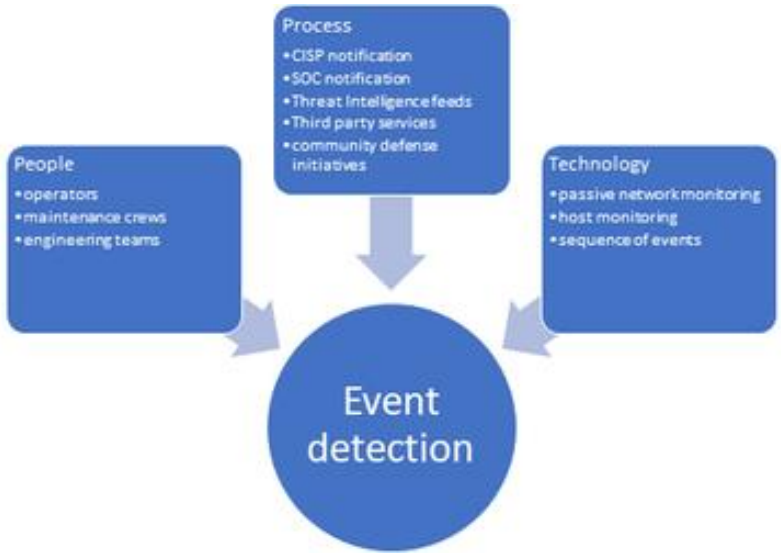

Figure 2 - Event Detection in ICS/OT environments

Further guidance and insights on logging and monitoring within ICS/OT environments that supports event detection can be found on the ICS COI Website. Operators also utilise the concept of Security Operations Centres (SOCs), with specialised SOC analysts, who will monitor events on a 24/7 basis. NCSC has additional guidance on SOCs and the functions and roles within them.

Detection - People

Operations, engineering, and maintenance teams will know your systems best and how they behave. Training these teams to report suspicious behaviour, and Building a culture that encourages the reporting of suspicious behaviour is a necessary long-term organisational activity, that will increase event detection coverage, and also helps to raise awareness of cybersecurity with those who do not perform cybersecurity roles full time.

A useful reference for what to consider when training ICS/OT operators to report potential cybersecurity events has been created by NERC in the US and is found here.

- **Action point:** Document the event detection examples from your environment in your ICS/OT Cyber IRP. Including notifications could come from helping to reinforce security culture across the organisation, and regular reviews of the ICS/OT Cyber IRP can be used to check validity of the event detection capability.

Detection - Process

Security events from network monitoring, host logging or security appliances such as firewalls can be used by your ICS/OT monitoring teams to detect and respond to events. This could be taking decisive and specific action to an event, or it could be activating the incident response plan to gather the team and investigate in more detail. It can be challenging for ICS/OT operators to hire and retain ICS/OT security specialists to perform the monitoring function. Third party monitoring arrangements can be considered to supplement ICS/OT operators' organisational capability. Options for support range from the integration of ICS/OT monitoring solutions into enterprise SOC (see NCSC related guidance), or outsourcing the monitoring to a Managed Security Services Provider.

Sources of cybersecurity events can also be found from outside of your own organisation. ICS/OT operators can utilise community notification arrangements such as Information Sharing and Analysis Centers, monitoring NCSC CISP notifications and subscribing to NCSC's early warning system. Further information on Threat information is also available on NCSCs website. The UK government also published a paper to help government departments with understanding how they should handle threat information which operators will also find useful.

Detection - Technology

Detection capability for ICS/OT systems if IT based can rely on the deployment of Endpoint, Detection and Response (EDR) solutions which are commonly deployed across entire enterprise networks (although quite often a business/risk decision is made to not enable the response solution). Passive network monitoring is often a good solution to deploy to minimise disruption to ICS/OT systems and assets where active scanning or host-based agents are prohibited, impractical or dangerous to deploy.

Regardless of the choices that ICS/OT operators make in terms of threat detection technology deployment, services, or in-house capability, they should have a clear understanding of what logging and monitoring coverage exists today for their environment. This is key to help understand potential gaps and improvements to logging and monitoring coverage. Even more importantly, it provides the incident response team (however it is composed) with a clear picture of where and how to collect logs to facilitate analysis.

- **Action point:** Develop a Collection Management Framework, sometimes referred to as a logging inventory, this is documented result of determining what logging and monitoring is in place across an environment. This can include documenting things like where network monitoring is currently deployed, which hosts are configured with log forwarding. This document can also be used to list out where forensic collection can be performed from assets. For example, there may be little monitoring deployed, but pointing out where logs or images could be manually collected will still be very useful to an incident response team.

Triage

Triage - Identify critical systems.

Operators of ICS/OT should have a well-documented inventory identifying critical systems and assets. These may have been identified through business continuity planning activities, risk management activities, table top exercise's, crown jewel analysis or CCE activities. Regardless of how they are formed, they should be used to determine what matters most to the ICS/OT operations, and therefore inform the incident response team on where to prioritise efforts for performing triage and forensic collection.

Triage - scope and scale.

ICS/OT operators should focus on how to scope out the scale of an incident in terms of how many systems, sites or business units are affected and in terms of how severe the incident is. This is important in helping to inform which resources are required internally and externally, which teams need to be informed, which regulatory reporting needs to be initiated. It is also vitally important for informing the teams responsible for collecting forensic evidence or performing any additional monitoring. Collecting forensic evidence in industrial environments and transferring it to somewhere it can be analysed is typically a challenging process that takes significant amounts of time and specialised resource (a useful resource developed by NIST in the US can be found here). Being able to use collection in a timely and strategic manner will reduce the load on the incident response team and help them keep agile in their response efforts.

- **Action point:** Document in the ICS/OT Cyber IRP where the incident response team can find ICS/OT specific forensic collection procedures.
- **Action point:** Plan ahead to think about which collection tools can be used, by whom and how they would be authorised for use, and how collected evidence can be securely transferred to where it can be analysed.

Taking responsive action

Taking responsive action - Increased threats

Plans should be in place to temporarily enhance the security of your network and information systems. You may choose to enact these plans in response to new or heightened levels of risk (e.g. a widespread outbreak of very damaging malware), informed by an organisation's security awareness and sources of threat intelligence.

Taking responsive action - Containment

Being able to implement containment methodologies can provide response team with some quick response options during an incident. Containment methodologies for industrial environments should be clearly defined and agreed ahead of time to allow for their swift implementation in an authorised manner. ICS/OT operators should use a zones and conduits model to help identify where and how containment can be implemented. Care must be taken when considering and acting to implement containment measures, as the responsibility for doing so will almost certainly lay with the authorised operators of the systems, not the Incident Response Team. The Incident Response Team need to be able to provide the advice, without overstepping designated plant operating responsibilities. Having pre-developed, tested and agreed containment methodologies will obviously decisions needed to be made during an incident.

Consideration should be given to the disconnection of the likes of SCADA servers/workstations and HMIs from the ICS/OT network if infected with malware. Ideally the methodologies (likely centred around disconnecting networks from IT/DMZ's/vendor remote access/Site Island Mode) will also clearly describe what the impact will be to plant operations in order for stakeholders to make a risk informed decision. For example, if plant disconnection at this location occurs, visibility will be lost to X systems, or services to Y will be affected. These actions would support:

- Isolation of the ICS/OT environment if the threat is detected in the wider IT/Enterprise business network and has not yet reached the ICS/OT environment.
- To prevent malware connecting out to its command and control network.
- Stop any remote access that has been established by a threat.

Action point: Document where and how containment can be implemented across the ICS/OT environment. Include this information in the ICS/OT Cyber IRP alongside the consequences and potential consequences associated with the action. For example, cutting the links to the system may reduce risk from further lateral movement of an attacker, but may also result in a loss of visibility to operators of the system or visibility of security monitoring to that network segment. Having detailed network mapping documentation available of all connections in and out of the ICS/OT environment defining the purpose of each, including which connections are essential to maintain normal operations and what can be safely disconnected would support quicker containment activities. Another activity to have undertaken to support quicker containment

activities would be to have a separate firewall policy pre-defined that limits connectivity to the minimum necessary which can be quickly installed on enforcement/containment points.

Taking responsive action - Recovery

If the analysis has determined that recovery measures are required, a well-documented arrangement for performing system restoration will be needed. It is common for ICS/OT operators to utilise control system vendors or integrators to support in the recovery and restoration efforts. As with containment actions, the Incident Response team should be providing advice and guidance to the operations team who will have responsibility for making the recovery decision and actions.

For many ICS/OT operators there will be a reliance on vendors to support the process for recovery from backup. There will also be a reliance on prompt access to backups, (and for the likes of Programmable Logic Controllers (PLCs), the programming software to download the program to the PLC). For many ICS/OT packages, it is likely to be possible to use standard hardware and operating systems. However, for other vendor solutions, more bespoke hardware will be required. This will require additional consideration for ICS/OT operators over IT recovery/remediation.

Additionally, it is not uncommon for the same ICS/OT site to use multiple versions of the same or similar systems (which could mean that making relevant backups of assets more challenging). Consideration should be given to the fact that assets may need to be replaced as they have been rendered unusable, or a faster response to recovery would be the replacement of the asset.

As part of the documented arrangement for performing system restoration it would it be useful for ICS/OT operators to work out how long restoring systems to a known good state would take, as an operator might take different steps if they know that it would take 2 hours to wipe and restore known good backups onto their ICS/OT systems rather than 2 weeks.

Factoring system restoration time that would ensure safety and integrity is likely to be very important, in addition to considering what resources (time/expertise/software/hardware) is required to achieve it.

It is also important to make sure that ICS/OT Operators know whether they could fully rebuild their systems if they were impacted is important. Especially given the legacy nature of a lot of ICS/OT environments, understanding if there are viable like for like spares, or what would be done if for instance the manufacturer of an old Windows based HMI been bought out and the original software copy is no longer around.

Action point: Document in the ICS/OT Cyber IRP the support required for the recovery and restoration of systems and industrial processes, including contact details for vendors and/or system integrators. ICS/OT operators may already have in place arrangements for the storage and testing of backup images and the acquisition spares for restoration from the result of business continuity planning and disaster recovery procedures. Where these already exist, consider if they

can be used in relation to responding to a cyber incident. For example, consider how testing of the images can be performed to ensure that backups are not also compromised, and consider how the containment efforts can be validated to ensure that a replacement system is not introduced into a network which is still compromised.

Action point: Reference Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) outputs into the ICS/OT Cyber IRP, listing out or providing document references to where and how backups are created, stored, and tested.

Tracking and Reporting

Tracking and Reporting - Timelines

Building a timeline of an incident is crucial regardless of whether it is a cybersecurity event in and IT or ICS/OT environment, or whether it is an industrial accident or malfunction of a system resulting in an operational incident. ICS/OT operators should put in place arrangements to ensure that the incident response team are recording incident timelines throughout the incident.

Key information to record includes:

- Time of event occurring, including checking that time from systems is synchronised or adjusted for drift.
- Time that information was received from stakeholders.
- Time that action was taken and who actions were assigned to.

Action point: Create a template that incident response providers can use to record and track details on an incident and include this (or a reference to it) within the ICS/OT Cyber IRP.

Tracking and Reporting - Communicating

ICS/OT typically is performing functions that are the core of the business in terms of revenue generation and will be performing functionality that is preventing hazardous situations such as loss of containment, personnel protection or protecting against uncontrolled environmental discharges. Therefore, it is vitally important that incident response teams are able to advise operations and safety personnel on the impact or potential for impact on operations and the systems performing safety functions. Incident response teams are recommended to keep this in mind throughout an incident response investigation, and actively consider and record this during regular incident response update calls. Regular and clear communication is key from the incident response team with other stakeholders which should include operations, health & safety representatives, engineering, and maintenance teams.

Communications across teams should cover and regularly revisit:

- What is known about the attack and/or malware? (or was it an attack or a failure / mistake in a change configuration?)
- What is the potential impact on the plant?
- Which systems/sites have been affected?
- What are the actions that need to be assigned and to whom?

The use of templates can aid these discussions as well as referring to a predefined and agreed incident severity matrix which should be recorded within the ICS/OT Cyber IRP. Examples of incident severity matrices are provided in the NCSC's Incident Management guidance. An ICS/OT specific example could be:

- Critical – Loss of essential service for extended duration, major equipment damage, offsite multiple injuries or fatalities,
- High – Reduction in operational production, plant damage/system outage, long term impact on business continuity, onsite injury
- Medium – short term impact on production, lost time accident,
- Low – minor deviation on low importance system

The Mitre ATT&CK ICS specific framework lists 12 techniques under the 'Impact' tactic that could be considered when developing this matrix.

An understanding is required of the regulatory requirements related to incident reporting and compliance obligations specific to ICS/OT environments. Nominated individuals should notify regulatory agencies as required by applicable regulations and standards, providing timely and accurate information about the incident and remediation efforts. Identified staff should work closely with legal teams to navigate the legal and regulatory considerations associated with incident response, such as preserving evidence for potential legal proceedings and complying with data protection laws.

Action point: Decide and document the ICS/OT incident severity matrix aligned to your ICS/OT operations.

Lessons Learned

As with any incident response or project closeout, taking the time to discuss, document and disseminate lessons learned are key to improving an organisations capability. This is no different for ICS/OT incident response but is provided here to ensure it is not forgotten. It is recommended to include the follow areas for consideration during any lessons learned activities:

- What went well, where can we celebrate the capability and commitment from our teams?
- How can we ensure we can better protect and detect against the attack vector?
- What were the blockers to making decisions?
- Where are improvements required on monitoring and logging coverage?
- What new critical assets were identified? (and fed back into the triage process).

Lessons Learned - Testing Capability

While learning from a real incident is very useful. There is no better way of testing an organisation's ability to perform incident response than to test it. Often the term "exercising" conduces thoughts that an exercise must involve a significant amount of planning and time away from a day-job for key operational staff. However, exercising can and should include a range of walk-throughs, drills, tabletop exercises up to company-wide and sector-wide exercises. NCSC guidance is available providing effective steps to creating a cybersecurity exercise. Examples of exercising capability can include the following:

- Gamification using decisions and disruptions or similar.
- Rehearsal of concept drill
- Team walkthrough of Cyber IRP and/or procedure
- Generic scenario tabletop exercises
- Customised tabletop exercise crafted to be specific to systems, operations and procedures used by the operator.
- Sector-wide exercise such as PowerPlay and GridEx

Tabletop exercises are very useful for exercising an operator's ability to activate an ICS/OT incident response team, and work in collaboration with other teams including corporate communications, operations and legal. For ICS/OT, there is often a need to ensure that there is sufficient cyber security maturity of an operator prior to undertaking a reasonably sized tabletop exercise (i.e. ½ to 1 day event, multiple teams involved). In those situations, the operators would benefit from performing more generic tabletop exercises, closer in reality to a drill or rehearsal of concept, such as a facilitated lead walkthrough of a scenario and some basic steps required throughout. Drills and walkthroughs are less intensive, and still provide huge benefit in practising aspects of an ICS/OT Cyber IRP which are difficult, i.e. forensic collection, determining if an event warrants declaring an incident. (Note - The NCSC defines a cyber incident as a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990))

Action Point: Schedule in an ICS/OT incident response exercise at least once a year. This could be part of a combined IT and ICS/OT incident response (noting that most threats to ICS/OT environments come through the IT/Enterprise environment first. It is also important to note that more and more ICS/OT is being monitored by hybrid IT and ICS/OT SOC functions. Thus, Incident Response exercises need to be wider than just the operational teams - the operational teams are likely to have incident response plans for other types of operational failure, the emphasis here is on CYBER incident and therefore other security specialists must be involved. A key part of the exercise activity is to review the result, to check the efficiency of your IRP.

Action Points

We have captured the following ICS/OT environment specific Action Points in this guidance:

- Develop an ICS/OT specific Incident Response decision tree/Play Book.
- Identify and train key individuals to act as the coordination point between IT and ICS/OT Teams.
- Create an ICS/OT Incident Response Plan that is specific to your ICS/OT environment.
- Provide Training and Awareness to staff involved in the ICS/OT IRP.
- Document the event detection examples from your environment in your ICS/OT Cyber IRP. Including notifications could come from helping to reinforce security culture across the organisation, and regular reviews of the ICS/OT Cyber IRP can be used to check validity of the event detection capability.
- Develop a Collection Management Framework, sometimes referred to as a logging inventory, this is documented result of determining what logging and monitoring is in place across an environment. This can include documenting things like where network monitoring is currently deployed, which hosts are configured with log forwarding. This document can also be used to list out where forensic collection can be performed from assets. For example, there may be little monitoring deployed, but pointing out where logs or images could be manually collected will still be very useful to an incident response team.
- Document in the ICS/OT Cyber IRP where the incident response team can find ICS/OT specific forensic collection procedures.
- Plan ahead to think about which collection tools can be used, by whom and how they would be authorised for use, and how collected evidence can be securely transferred to where it can be analysed.
- Document where and how containment can be implemented across the ICS/OT environment. Include this information in the ICS/OT Cyber IRP alongside the consequences and potential consequences associated with the action. For example, cutting the links to the system may reduce risk from further lateral movement of an attacker, but may also result in a loss of visibility to operators of the system or visibility of security monitoring to that network segment. Having detailed network mapping documentation available of all connections in and out of the ICS/OT environment defining the purpose of each, including which connections are essential to maintain normal operations and what can be safely disconnected would support quicker containment activities. Another activity to have undertaken to support quicker containment activities would be to have a separate firewall policy pre-defined that limits connectivity to the minimum necessary which can be quickly installed on enforcement/containment points.
- Document in the ICS/OT Cyber IRP the support required for the recovery and restoration of systems and industrial processes, including contact details for vendors and/or system integrators. ICS/OT operators may already have in place arrangements for the storage and testing of backup images and the acquisition spares for restoration from the result of business continuity planning and disaster recovery procedures. Where these already exist, consider if they can be used in relation to responding to a cyber incident. For example, consider how testing of the images can be performed to ensure that backups are not also

compromised, and consider how the containment efforts can be validated to ensure that a replacement system is not introduced into a network which is still compromised.
- Reference BCP and DRP outputs into the ICS/OT Cyber IRP, listing out or providing document references to where and how backups are created, stored, and tested.
- Create a template that incident response providers can use to record and track details on an incident and include this (or a reference to it) within the ICS/OT Cyber IRP.
- Decide and document the ICS/OT incident severity matrix aligned to your ICS/OT operations.
- Schedule in an ICS/OT incident response exercise at least once a year. This could be part of a combined IT and ICS/OT incident response (noting that most threats to ICS/OT environments come through the IT/Enterprise environment first. It is also important to note that more and more ICS/OT is being monitored by hybrid IT and ICS/OT SOC functions. Thus, Incident Response exercises need to be wider than just the operational teams - the operational teams are likely to have incident response plans for other types of operational failure, the emphasis here is on a CYBER incident and therefore other security specialists must be involved. A key part of the exercise activity is to review the result, to check the efficiency of your IRP.

Resources

Various ICS/OT specific Incident Response and Management resources have been mentioned throughout this article. In addition, the following resources are also available:

- The International Society of Automation has a wealth of resources to support those running ICS/OT environments with their Incident Command System for Industrial Control Systems (ICS4CS) programme. ICS4ICS is specifically designed to improve management of cybersecurity incidents that impact industry.
- CISA have Cybersecurity-based threat vector scenarios including ransomware, insider threats, phishing, and Industrial Control System compromise.
- The European Union Agency for Network and Information Security have various ICS/OT resources such as the Good practice guide for CERTs in the area of Industrial Control Systems.
- The US National Institute of Standards (NIST) has resources to support Incident Response such as its Computer Security Incident Handling Guide and its Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)

CAF IGP Summary

This article discusses measures that contribute to the following CAF (v3.2) IGPs:

- **A3.a Asset Management** - Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).
- **B4.b Secure Configuration** - You securely configure the network and information systems that support the operation of essential function(s).
- **B4.d Vulnerability Management** - You manage known vulnerabilities in your network and information systems to prevent adverse impact on the essential function(s).
- **B5.a Resilience Preparation** - You are prepared to restore the operation of your essential function(s) following adverse impact.
- **C1.c Generating Alerts** - Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.
- **C1.e Monitoring Tools and Skills** - Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential function(s) they need to protect.
- **D1.a Response Plan** - You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function and covers a range of incident scenarios.
- **D1.b Response and Recovery Capability** - You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function. During an incident, you have access to timely information on which to base your response decisions.
- **D1.c Testing and Exercising** – Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.
- **D2.a Incident Root Cause Analysis** - When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.
- **D2.b Using Incidents to Drive Improvements** - Your organisation uses lessons learned from incidents to improve your security measures.

Statement of support

This guidance has been produced with support from Dragos, SSEN, Bridewell Consulting, Airbus and members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Interconnected Cyber-Physical Systems (RITICS), with support from the National Cyber Security Centre (NCSC). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable. This document is provided on an information basis only, Dragos, SSEN, Bridewell Consulting, Airbus, ICS-COI members and NCSC have used all reasonable care in

verifying the guidance contained within using the data sources available to it, they provide no warranty as to its accuracy or completeness. To the fullest extent permitted by law, Dragos, SSEN, Bridewell Consulting, Airbus, the NCSC and the ICS-COI accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using this document. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances. Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by Dragos, SSEN, Bridewell Consulting, Airbus, the ICS-COI or NCSC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.