INDUSTRIAL CONTROL SYSTEMS
Community of Interest

Exploring the "bake off" process and implementation of Industrial Control System / Operational Technology Asset Discovery Solutions - meet Admin Corp

Introduction

The initial step for any organisation that utilises an Industrial Control System (ICS)/ Operational Technology (OT) environment, in developing a cyber security programme is to produce an accurate and complete asset register to truly understand their potential attack surface. A reliable asset management system assists with the configuration change management, vulnerability management, and the Cyber Incident Response processes within the ICS/OT environment. This then supports the organisation with its understanding of the risks that it is managing.

NCSC has generalised asset management guidance which can be found here - https://www.ncsc.gov.uk/guidance/asset-management, while this article is part of a series of ICS/OT specific guidance articles on Asset Management first introduced in "Asset Management within ICS/OT Environments". Further articles from the ICS/COI can be found here.

Within this article we shall be focussing on the selection and implementation of automated ICS/OT Asset Discovery solutions/tooling. The article has been written for those

organisations that have ICS/OT environments, who are at the stage of their ICS/OT Cyber Security journey where they are considering if an automated solution for Asset Discovery/Management is right for them. The Admin Corp example supports those operators that have both central large site assets in addition to remote sites.

In this article we focus on a Asset Discovery solution that supports predominately the passive method of Asset discovery management. Further details on the other methods of Asset Discovery are covered here.

Meet 'Admin Corp'

Let's imagine we're following a fictional organisation who are responsible for managing the cyber security of a CNI processing plant.

Admin Corp runs a plant that produces Adminox, a highly volatile, refined form of administrative paperwork that is essential to every organisation in the country. It is created from volatile raw products using a continuous chemical process.

Admin Corp not only produces Adminox but also is responsible for the transmission and distribution of Adminox to a range of customers including both commercial and residential, and therefore is also classed as a utility company. It therefore has a range of sites, including those responsible for the production of Adminox, and those used to transport and distribute Adminox to its customers.

As an essential service, Admin Corp must comply with the UK NIS Regulation. This means that Admin Corp's assets needed to produce Adminox must be protected from cyber-attack. Also, because Admin Corp are regulated for safety by the UK Health and Safety Executive using OG86 , they must take steps to ensure the continued cyber Security of the Adminox production process.

Asset management and monitoring - Assurance Review

Although Admin Corp believe that their operations are secure and well managed, they have become increasingly concerned about reports in the news about cyber-attacks on industrial companies and, as a CNI operator and an essential service, they need to ensure that they are managing the risks to their operations.

Admin Corp's CISO and Operations Managers have agreed that they need to carry out a risk assessment of their networks and systems to understand how vulnerable they are to one of these cyber-attacks. The CISO receives threat briefings from a number of sources, including government departments, and is keen to ensure that Admin Corp can model the threats against their networks and operations.

The CISO's team have reviewed security good practice and agreed to work with field teams to assess how well they understand the ICS/OT systems and assets controlling their industrial processes. The CISO has a team that monitors the security and vulnerabilities in Admin Corp's IT assets and the Operations Managers have agreed that the review team should include monitoring coverage in their assessment of the ICS/OT systems.

The assessment team arrange a series of site visits to understand how the plant operators keep a record of their equipment. After a few visits, it is clear that the method for storing asset information is inconsistent: some sites are keeping ad-hoc records on spreadsheets, others simply refer to the design drawings and at others, the oldest sites, there are no records at all. The team identifies that the sites are protected by firewalls; some maintained and monitored by the CISO's security team and others that are maintained by site engineers but not monitored. The team concludes that overall, there are significant gaps in their knowledge of the assets that they need to protect.

The CISO creates a risk report and explains to the Operations Managers that the success of a cyber-attack on Admin Corp could be increased by having incomplete records of assets and limited monitoring of their ICS/OT systems and that this could lead to loss of production and associated revenue and, in extreme cases, injury or loss of life.

Developing the business case

Armed with the CISO's risk report, the Operations Managers have reviewed the financial and reputational value of the potential losses and conclude that they should develop a business case to improve their asset management and monitoring and, in turn minimise the risk to their operations. They call together experts from their engineering and security teams and instruct them to come up with a solution and include an indication of how much it will cost to implement and maintain.

The team agrees that the first thing to do is define an initial set of high-level requirements based on good practice guidance and market research. They refer to NCSC guidance and other guidance offered by the likes of NIST and the HSE.

They conclude that they have four high-level key requirements:

- **They need to know what assets are on the network, their components, and how and who they communicate with.**
- **They need to be able to maintain a record of the assets in a centralised system.**
- **They need to understand what normal activity looks like and be able to detect signs of threat behaviour in that environment**
- **They need unusual events to be reported to somebody who can investigate them.**

Delivering these requirements will put them in a far better position operationally, they will be better able to plan security improvements based on the tool's output and, in the event of a cyber incident they will be better placed to contain and eradicate the problem.

From their research the team understands that there are several companies offering products that will monitor networks and in doing so claim to identify the assets connected to it. They also notice that there are some tools available that are free to obtain and use - Admin Corp are keen to invest the right amount in the right places and the possibility of minimising cost is appealing to the Operations Managers.

As Admin Corp is also operating a utility company, it needs to follow procurement regulations to ensure that contracts are awarded to the most economically advantageous tender. They need to bear this in mind when talking to vendors and planning the implementation programme as there are extra stages that need to be considered before placing the contract.

After discussing the work with the Procurement team, they contact some of the key vendors and arrange for product demonstrations to understand more about what the systems are capable of. They ask each of the vendors for rough order of magnitude costs for the supply, implementation, and maintenance of each system.

The team also decides that it is worth investigating the solutions that are free to obtain and use.

Finally, the team agree that there may be some security tools already being used in Admin Corp that could deliver some of their requirements and decide to review them as well.

Operating the tools

The Admin Corp CISO and the Operations Managers have agreed that they need to implement security solutions/tools to identify and monitor assets, but the CISO is concerned that they have not yet discussed who will operate these solutions/tools. All the suppliers they have spoken to refer to tuning, false positives, validation and investigation activities that require somebody to do them but, for Admin Corp who would that be?

The team get together and make an initial list of concerns that need to be worked through:

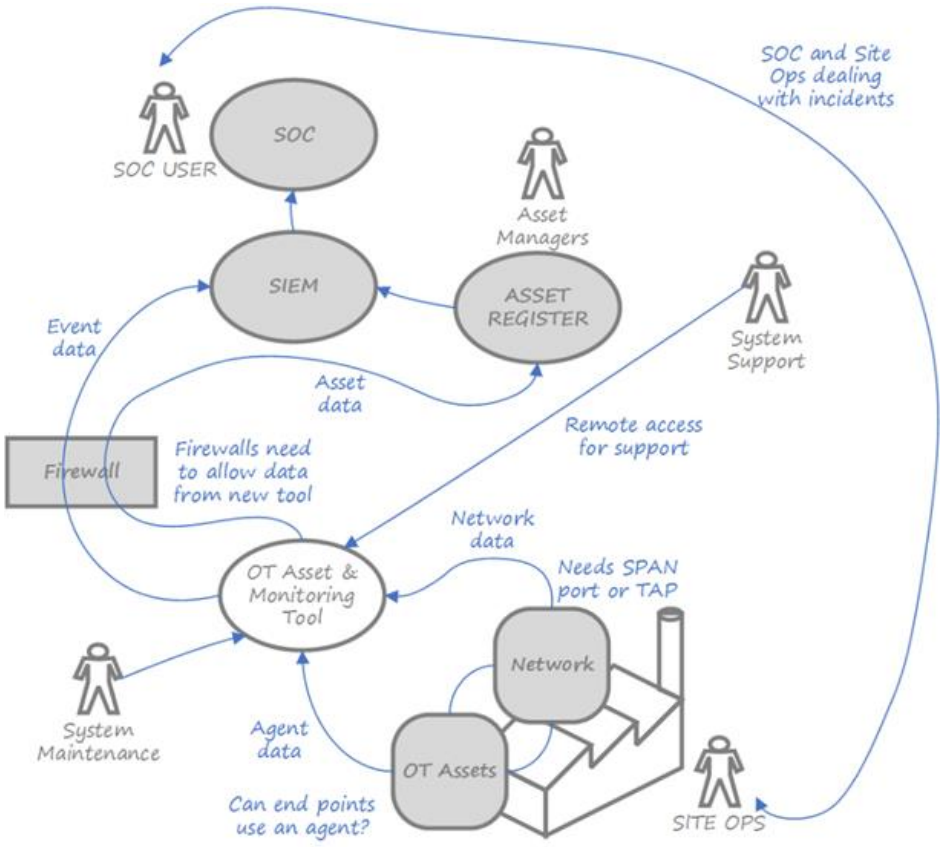
- **Who is going to use the solutions/tools?**
- **Who will manage the platform – patching, support, etc.?**
- **Who will validate the output – confirming if an asset is valid or rogue?**
- **Who will tune the monitoring tool to remove false positives?**
- **Who will receive and action security alerts? In hours? Out of hours?**

The CISO and the Operations Managers agree that before they commence procurement of the solutions/tools they will set out and agree the initial operating model; they do not want to be caught out buying a solution/tool and having nobody to operate it and there may be additional costs to consider beyond the price of the solutions/tools.

Designing the Implementation and Integration

Through research and conversations with suppliers, the Admin Corp team have started to build a greater understanding of what it means to implement and operate these asset discovery and monitoring solutions/tools. Almost all the suppliers have referred to taking data feeds from the networks and some have referred to putting agents on the ICS/OT system components. They agree to run a workshop and include Subject Matter Experts from the operational sites, IT, the CISO's team and group responsible for the communications network infrastructure.

They set to with a whiteboard and pens and sketch themselves a basic diagram of how the new tools will interact with the existing environment. This is shown below:



By sketching the target state, they can now understand whether and how the systems will be integrated.

- Admin Corp have an existing asset management system that can store the ICS/OT and networks assets discovered by the solution/tool. This will ensure that Admin Corp can develop a single source of truth that will be vital if they are ever subject to a cyber-attack.
- There is an existing Security Information and Event Management (SIEM) system already used by the outsourced IT Security Operations Centre (SOC) function and they agree that it should receive the events from the new tool. The SOC manager explains that having access to asset data is useful when dealing with incidents and that a link to the asset management system is useful.

They understand that most of the solutions/tools need to have a network connection that allows the traffic to be inspected without affecting it. The communications network support team agree to confirm that the switches can handle port mirroring; if they cannot there may be additional costs for network enhancements or Network TAPs to consider. In addition the network support team agree to explore if there will be a need to locally aggregate multiple mirror ports and then transport the mirrored data over a fibre link to the location of the new security tool or where additional network TAPs might be required/placed to provide additional visibility beyond the switch port mirroring capability (although these are limited to some of the larger sites). (further guidance on network TAPs can be found here).

It is important to note that Admin Corp understand that they have no PLC point-to-point links installed within their ICS/OT environments, noting that passive discovery using network switches would not have captured these, if they had them.

The team also realised that the new tool would need to be maintained by somebody and supported, possibly by a third party, and that access for these users' needs to be controlled and secure.

Considering how the tool will be implemented and integrated, even at a high level, helps Admin Corp to describe their requirements more clearly when they commence the formal procurement.

Requirements Analysis

The project team within Admin Corp having undertaken this work have developed technical functional and non-functional requirements to allow assessment of the market for potential product suppliers. In brief the technical functional requirement states that:

- The product must be able to gather a complete inventory of ICS/OT systems and its relative configurations, software installed, and firmware.
- The product should be able to perform automatic and manual asset discovery as well as manage all connected assets within the network.
- Zero Impact - The discovery of OT assets should not disturb plant operation and affect network or systems performance.
- Integration - The product must be able to integrate with the existing Admin Corp Configuration Management Database (CMDB) product and SIEM.
- ICS/OT Protocol support - The product must support all ICS/OT protocols used within Admin Corp. Both protocols with public specifications, and protocols with private specifications that require reverse engineering or partnerships with controller manufacturers to be handled.
- Alerting - The product should be able to alert when new ICS/OT assets are discovered.
- Vulnerability Management - The product should be able to analyse and prioritise all advisories and associate them with ICS/OT assets.
- Change Management - The product should be able to track all changes to the code, OS and firmware for all ICS/OT assets.
- Encryption support - The product should be able to manage encrypted protocols and ability to manage serial communications.

The team have also identified that most products available have a range of additional capabilities that they may wish to explore and have developed additional criteria, for these optional capabilities. This includes:

- Network Management
    - The product should be able to have real-time visibility to the industrial network
    - The product should be able to automatically or manually define the network topology including physical and logical connections (network mapping)
    - The product should be able to provide information about network administration such as user information

- The product should be able provide network fault diagnostics and network performance.

The project team task at this stage is limited to a documentary study and interviews with the product manufacturers, rather than engaging in a product test-bed exercise. The report they produce provides a clear picture of strengths and weaknesses against the functional criteria of a wide range of technical solutions/tooling and provides Admin Corp with a short-list of potential products. Admin Corp are aware some similar organisations to themselves have had this work undertaken by NCSC Assured Consultancies.

Admin Corp then request further briefings from the vendors highlighted in their shortlist.

Product Evaluation and Selection

Following the work detailed above, Admin Corp then decide to have a technical 'bake off' to further explore the capabilities of the selected technical solutions/tooling.

Admin Corp work to harmonise their requirements documentation for the solution providers, noting that various teams have provided requirements, including their IT infrastructure team, ICS/OT Operational team and their Security team (including the SOC), to ensure the same language, and a consistent theme of requirements is used.

Admin Corp discuss letting a contract to an NCSC Assured Consultancy to do this work on their behalf, but due to a pressing investment timeline due to regulation, decide to run the 'bake off' themselves using their own security and engineering teams.

The security and engineering team develop a Proof-of-Concept approach to facilitate the 'bake off' between the different solutions. The 'bake off' approach facilitates the connection of each solution in the short list to a switch (using the SPAN Port) within their Data Centre that their Supervisory Control and Data Acquisition (SCADA) servers are connected to. Best practice is to connect a Data Diode SPAN Aggregation TAP to the SPAN port of the switch to ensure data cannot be introduced from the systems being evaluated into the bi-directional Switch SPAN port. This specialist TAP can also be used to provide multiple copies of the mirrored traffic to each of the different solutions being evaluated ensuring each is evaluated with identical data and shortening the time needed for the proof of concept. Admin Corp team understand that this will only really capture SCADA to Remote Terminal Unit (RTU) traffic, and therefore also gather a packet capture from a remote field site that is also fed into each solution on the short list. The team are happy

that this is enough data for the solutions to be tested but are aware that due to some technical limitations they still have at remote sites that this is not complete.

Challenges faced in this approach include the fact that Managed Service Provider that they use to provide their data centre does not understand what is meant by ICS/OT traffic, and therefore has to have deeper explanation provided about the specific SCADA servers in question and the switch providing them with network capability, and the fact that while it was thought the networking at a remote site selected was provided by a hub it is found that it is provided by a switch without the facility to provide a port SPAN capability, and so has to be temporarily swapped out for one that does in order to undertake a packet capture.

Admin Corp also note that they may have some issues around the identification of some of its legacy hardware and software deployed in its ICS/OT environment and are keen to explore if the solutions selected can handle this. They also note that having access to a permanent lab environment to undertake this type of product evaluation would be very beneficial in the long term, given various other projects they have in mind to develop their cyber security maturity within the ICS/OT environment.

On reflection, Admin Corp, would also have liked the opportunity to have been able to utilise a consultancy/system integrator where they could see the shortlist of solutions already deployed on a test lab environment, so they could undertake a bake off in a more efficient and effective manner at a lower cost of entry.

The Admin Corp team developed an in-depth Scoring mechanism used to score each solution in a weighted manner during the ‘bake off’ process based on the MoSCoW approach shown against an initial functional catalogue of requirements.

Some of the more detailed requirement's criteria used by Admin Corp that are scored against are captured below (note this is not designed to be an authoritative list):

- Asset Management
    - Comprehensive near-real-time OT asset discovery
    - Identification of asset type (PLC, RTU, HMI, actuator etc.)
    - Identification of asset vendor for all assets
    - Identification of asset model (e.g. Foobar VT-13555-A RTU)
    - Identification of IP address
    - Identification of hostname
    - Ability to create network maps including routers, switches and firewalls
    - Identification of firmware version
    - Identification of OS & version where applicable
    - Identification of communication protocols between assets at all layers
    - Identification of TCP & UDP listening ports on identified assets
    - Identification of enabled USB & other mass storage ports on identified assets
    - Identification and highlighting of newly added assets
    - Identification of non-responsive assets/assets that have gone offline
- Threat and Vulnerability Management
    - Highlighting where firmware/OS is out of date and/or vulnerable
    - Providing CVE & summary for vulnerabilities with link
    - Providing CVSS or IVSS for vulnerabilities
    - Tool database is continuously updated with latest vulnerabilities and threat intelligence
    - Identification and highlighting of unencrypted traffic

    - Alerting when laptops, USB etc are plugged in and removed
    - NAC ability with an 'Allow List' and 'Block list' by MAC address of assets on the network
    - Ability to baseline normal network traffic profile
    - Identification and highlighting of active threats
    - Identification and highlighting of anomalous network traffic
    - Ability to highlight threats against the MITRE framework
- Usability of Application
    - Ability to filter by asset type (e.g. 'Show all PLCs only')
    - Event data is aggregated, searchable, filterable etc.
    - Able to secure with MFA
    - Application speed, responsiveness and usability/UX
    - Ability to configure different roles/granular permissions if required (RBAC)
    - Search facility to quickly find specific known assets or IP addresses
    - Ability to export asset register as CSV/other for import into another tool
    - REST API capabilities to pipe active and passive asset discovery data into a CMDB
    - Show numeric asset totals, overall and by type and by vendor
    - Provide risk dashboard with RAG, showing remediation priorities
    - Visual representation of discovered assets by asset type e.g. layered per Purdue
    - Ease of deployment
    - Ease of maintenance
    - Quality of support available

Admin Corp for the bake off, intentionally ruled out Active Scanning techniques given that they know that within their ICS/OT environment that they may have devices such as Programmable Logic Controllers (PLCs) and RTUs used to monitor the activity and state of machinery (e.g., pumps, valves and motors) and environmental factors (e.g., temperature, pH and vibration) in the production of Adminox, that may be too sensitive to withstand active scanning. They know this is especially true of older legacy devices. Specifically, they think their ICS/OT environment may be sensitive to Active Scanning techniques for some of the following reasons:

- **Limited CPU power:** ICS/OT devices could be overwhelmed when too many requests are added to their process control duties.
- **Real-time communications:** ICS/OT protocols involved often expect an unbroken stream of readings from a device. If they're delayed substantially, they may have

issues re-establishing communications. A full vulnerability scan probes many areas of a device very quickly, which can overly burden the limited CPU power and delay communications.

- **Custom operating system and software:** ICS/OT legacy devices generally do not run widely used and widely tested operating systems, such as Windows or Linux. They may include a small HTTP server, but it likely includes a limited feature set. When a vulnerability scanner attempts to check SSL, which may not have been implemented, the embedded HTTP server could crash. If actively scanned, these sensitivities may result in performance degradation or reboots – causing costly downtime and potentially unsafe working conditions.

Admin Corp do realise that some of the solutions they have chosen for the bake off but not all of them have an Intelligent Active Interrogation capability, that has gone through testing with OEMs, but still decide to rule out this capability in their scoring of the solutions.

Admin Corp also realise that visibility is key, with variation of use between TAPs and SPAN ports, but decide to develop the bake off purely based on the use of SPAN ports, noting that the operational implementation may be enhanced with an additional TAP fabric (further information can be found here on Asset Management visibility techniques).

At the end of the 'bake off' Admin Corp noted a significant difference between the scores of each solution tested, providing them with a clear leader for the solution to be progressed. They did, though, think that if the scores had been closer that the cost of the solution would also have been a major factor in final determination.

Admin Corp then utilised a "Procurement Advice Notice" (PAN) for the direct purchase of the solution chosen. This is a process whereby the standard procurement policy is not followed; however they noted that had they not used the internal approach taken, then they would have followed their standard procurement process with Invitations to Tender (ITT) and RFQ stages.

Implementation

Admin Corp then purchased the chosen solution, with a 3-year licence for the operation and professional services support. Their approach is to expand on a year-by-year basis on the number of instances deployed across their central and remote sites, Year 1 is focused on the data centres and some remote sites, year 2 will provide instances deployed at all remote sites, while year 3 will be full operational coverage. They have also purchased professional services support for this chosen solution for the full 3 years.

Admin Corp staff, then undertake a period of training/upskilling provided by the chosen solution provider, including elements of integration with the inhouse SIEM, which in turn is then monitored by their outsourced SOC provider. Currently they have no plans to provide direct access for the Outsourced SOC provider to the solution implemented, but this may be considered at a later date.

Admin Corp's first remote site installation will in fact be in a full representative environment lab to provide them with a further level of confidence and assurance that the tool will have asset visibility that it is expected, having noted some issues around legacy switches which may need to be swapped out to newer models to support SPAN ports. This is actually part of a bigger piece of work that Admin Corp are developing to test and research what a new ICS/OT network infrastructure would look like (including the likes of better separation between Purdue layers 1 and 2).

As part of the remote site implementation Admin Corp have also explored with the solution provider, the various physical forms the deployed instance can be, to ensure space compatibility. Admin Corp have also chosen for the solutions data to be provided back to the central monitoring site using existing in-band communications (Multiprotocol Label Switching Wide Area Network, with 3G/4G/Satellite Communication redundancy) from a cost perspective, noting that there was an option of a more expensive out-of-band solution.

Admin Corp note that adding in any new security control adds a new element of risk that needs to be considered, they have therefore conducted several levels of Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) with the solution provider, in addition to conducting a threat informed risk assessment process on the use of SPAN ports and existing in-based communications, to understand if this has had a negative or positive impact on the attack surface, especially if it has introduced any new vulnerabilities.

Cost at this stage is a major factor for Admin Corp, so they have avoided any re-architecture of their ICS/OT environments, only accepting that they may have to swap out some non-SPAN enabled switches/hubs for newer SPAN enabled switches. They do note that they will have to review the architecture of their ICS/OT environment, including out of band options for their security fabric as part of a future project as they progress on their Cyber Security maturity journey.

During the implementation Admin Corp and the solution providers professional services support team do face challenges on fine tuning and tweaking the solution on the live ICS/OT environment, which Admin Corp choose to document carefully to inform any potential re-architecting projects in the future.

Admin Corp also decided during the implementation period, while covering their main sites and major remote sites, that actually the cost/value benefit of some of their smaller remote sites was not as first thought and therefore reduced their requirement somewhat in year 3 for full operational coverage.

Final thoughts

Having achieved these steps, Admin Corp believe they now understand what they have implemented with regards to an ICS/OT automated asset discovery capability (along with logging and monitoring) that will provide them with the foundation they can build upon to achieve vulnerability management, good asset situational awareness, that helps them defend against both deliberate acts of cyber intrusion as well as incidental malware infections that might have an impact on the production process. Once they are mature and have implemented across all central and remote sites, Admin Corp will be looking to explore the value-added services that the chosen solution also has to offer (including the option of Intelligent Active Querying).

Admin Corp understand that this solution will identify a range of vulnerabilities and will be also developing a risk driven process so that they can manage and understand the risk of vulnerabilities within their ICS/OT environment.

They also understand that they need to build better governance on their change management control process, supported by their chosen solution, to ensure they maintain better asset inventory. They also need to look to start their thinking about the options of having a dedicated out of band cyber security fabric across their sites ICS/OT environments, in addition to enhancing their ICS/OT network security (given they have put

smarter/newer managed switches in place, and now could implement switch port security and deploy an Network Management System (NMS) for switch port monitoring, which could limit the connection of unauthorised devices, alert them to attempted connections by an unauthorised device, and better monitor the performance of their ICS/OT network, and where redundancy is built into the network, monitor for component/link failures that may not otherwise be observed (because the network is still functioning).

CAF IGP Summary

This case study discusses measures that contribute to the following CAF IGPs:

- **A3.a A01**: All assets relevant to the secure operation of essential functions are identified and inventoried (at a suitable level of detail). The inventory is kept up to date.
- **A3.a A02**: Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded.
- **A3.a A03**: You have prioritised your assets according to their importance to the operation of the essential function.
- **A3.a A04**: You have assigned responsibility for managing physical assets.
- **A3.a A05**: Assets relevant to essential functions are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.
- **B4.b A01**: You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of the essential service.
- **B4.b A02**: All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment.
- **B4.b A04**: You regularly review and validate that your network and information systems have the expected, secured settings and configuration.
- **B4.d A01**: You maintain a current understanding of the exposure of your essential service to publicly known vulnerabilities.
- **C1.c A03**: Alerts can be easily resolved to network assets using knowledge of networks and systems.
- **C1.e A07**: Monitoring staff are aware of essential services and related assets and can identify and prioritise alerts or investigations that relate to them.
- **C2.a A01**: Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting

malicious activity (e.g. You fully understand which systems should and should not communicate and when).

- **C2.a A04**: The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.

Statement of Support

This guidance has been produced with support from SSEN, Wales and West Utilities, Bridewell, Garland Technology, Yorkshire Water and members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected 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.