INDUSTRIAL
CONTROL
SYSTEMS
Community of Interest

Point in Time Asset Discovery at remote sites within Industrial Control System/Operational Technology environments - meet Admin Corp

Introduction

An initial step for any organisation that utilises Industrial Control System (ICS) / Operational Technology (OT) 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 generic 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 on Asset Management first introduced here. Further articles from the ICS/COI can be found here.

In this article we shall be focussing specifically on performing point-in-time automated asset discovery supporting limited physical survey efforts within difficult to reach areas of operational networks, it is aimed at both asset owners looking to purchase a point in time assessment, or to the specialists conducting that assessment.

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.

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, they must take steps to ensure the continued cyber security of the Adminox production process.

As a requirement of NCSC’s Cyber Assessment Framework, Admin Corp have embarked upon an ICS/OT asset discovery project to increase their visibility of the devices which assist with the production of their vital product.

Remote Sites

Admin Corp have as they have grown in size through mergers and acquisitions, developed a large number of remote sites that develop components used in the production process, these include both onshore and offshore sites.

Whilst Admin Corp have found the ICS/OT asset discovery project fairly manageable within their larger production site (predominantly situated alongside their administrative buildings), the significant number of smaller remote sites responsible for the production of various components has been more of a challenge.

Due to the highly volatile nature of Adminox, a number of these remote sites are located far from human civilisation to enable the safe extraction and processing of raw materials. Several of these sites were acquired as part of Admin Corp’s vertical integration strategy, and in many cases, limited documentation was transferred about the ICS/OT networks during the acquisition process. As these sites were not part of Admin Corp when the ICS/OT systems were initially designed and deployed, they do not adhere to Admin Corp's corporate standards, nor were many purchased from Admin Corp's preferred ICS/OT suppliers. In addition, there is in some cases very limited telecommunications bandwidth serving the site, or none at all. The result is numerous ICS/OT environments with disparate technologies and implementations about which relatively little accurate data is held.

Would a manual process work?

Admin Corp considered whether just a "limited" manual asset discovery process involving an engineer walking through these facilities making notes on assets would be suitable for their needs. Admin Corp have done a "detailed" manual method at some of their sites as a primary means of understanding their assets, in addition at some sites, both central and larger remote sites, they have permanently installed automated asset discovery. Admin Corp undertook a "limited" manual method trial on a small number of the "acquired" sites, noting the lack of knowledge and experience of these sites with their current engineering and operations teams, it resulted in unverifiable results with many key fields of asset metadata left undiscovered.

Admin Corp identified that the resources required to produce an accurate in-depth asset register manually at scale across all the 'acquired' sites, given the unknown nature of the sites, would again require individuals from various teams, some of them needing to be upskilled and trained on different vendors. This would have an impact on other business-as-usual activities. Admin Corp therefore assessed the cost of a full manual approach only in this case to be untenable and decided on a limited manual survey approach in combination with the use of automated asset discovery tooling.

Would the ICS/OT Network monitoring tools suffice?

Consideration was also made to the use of their larger ICS/OT asset management discovery and monitoring solution, implemented in their central sites. The solution they chose was ideal for their relatively modern main production central sites, as they could easily configure their networking equipment to output a copy of the network traffic, deploy hardware to capture the data in real-time, and access the data from their HQ IT network safely. The implemented tooling providing sufficient asset metadata. Unfortunately, Admin Corp have identified a few issues with rolling this out to their remote sites:

1. Due to the wide variety of networking equipment of various vintages in use across their remote sites, the ability to easily extract and centralise network traffic within a location is likely to be challenging if not impossible in some cases.
2. If they were able to extract real-time network traffic at remote sites, they would need to purchase expensive hardware to run the asset discovery software for each location.
3. Due to their geographical location, many of these remote sites have no external networking capability – there's no copper or fibre lines running to the properties, nor any cellular towers within distance. The budget for this project will not stretch to installing new infrastructure to support internet connectivity (the option of satellite communications connectivity was something that Admin Corp considered but given the lack of any funding ruled this option out also). Therefore, even if data could be easily extracted, centralised, and analysed by on-site hardware, it wouldn't be possible to automate getting this data back to HQ.

A Balanced Approach is Required

Due to the above constraints, Admin Corp decided a balanced approach needed to be undertaken. Considering the relatively static nature of ICS/OT systems (who's average lifecycle is measured in decades), Admin Corp decided that taking point-in-time captures of asset metadata on a semi-frequent basis is likely to yield significant value where real-time data is not accessible. Having point-in-time captures of asset metadata would then hopefully solve the issues that the trial of several sites using manual survey only had identified.

Whilst it may not solve other aspects of meeting CAF requirements (which more automated network monitoring tools would achieve), Admin Corp decided that a point-in-time capture of asset metadata of the wire, in parallel with a limited manual survey being conducted at each site at the same time, should be sufficient to meet their immediate needs of producing an accurate asset register. Admin Corp therefore decided to take advantage of Asset Discovery solution which can be deployed on portable hardware (in this case a laptop) to perform asset discovery in these difficult-to-reach ICS/OT networks, backed up by use free open-source software like Wireshark or Malcolm, to gather and analyse the data on site and also help centralise and analyse it back at HQ afterwards.

While the Asset Discovery solution chosen could take advantage of both passive and active scanning techniques to build up a picture of the assets communicating across their remote site ICS/OT networks, Admin Corp decided to not utilise the depth of the active scanning techniques until they better understood the environments from a passive asset discovery perspective.

Passive Asset Discovery

Starting with passive discovery, Admin Corp, extracted network traffic from the ICS/OT environments at their 'acquired' remote sites, either by making use of SPAN/mirror ports on every network switch (noting that not all switches had this capability), or temporarily deploying network taps to intercept traffic on a wire. They chose to deploy the temporary network taps in numerous locations, to ensure they got saturation cover, given the unknown status of the wired network. Many of the ICS/OT network devices were known to communicate infrequently, so the scanning capability was deployed for a full week, to ensure that infrequent communications were captured.

The traffic captured from a SPAN or tap, was fed directly to the asset discovery software running on a laptop, to help the engineers at site understand what was installed, and steer their work in real-time, and was also captured as PCAP files, for analysis using free open-source tools such as Wireshark or Malcolm.

Saving the traffic in a PCAP would also if necessary, enable the uploading of that data for analysis to a central instance of Admin Corps main automated asset discovery tool hosted in Admin Corp HQ, allowing for ease of data ingestion to the central asset register.

It is important to note that Admin Corp understand that the 'acquired' remote sites had no PLC point-to-point links installed within their ICS/OT environments, noting that their chosen method of passive discovery using network switches would not have captured these.

Active Asset Discovery

While Admin Corp chose a technical solution that did have an active scanning capability, they chose not to utilise it given the 'acquired' remote sites had not very well understood assets. Admin Corp did consider both very basic scanning and active intelligent interrogation but decided against both to minimise any potential impact to the operations of live systems. Admin Corp realised that undertaking active asset discovery would have enhanced the resulting data from the asset discovery tool, making the decision to consider possible deployment at a later visit to the ‘acquired’ remote sites, once they knew more about the vendors and technologies in use from the passive and ‘limited’ manual approach.

Next Steps

Following the limited physical survey and passive asset discovery activity undertaken at its ‘acquired’ remote sites, Admin Corp work to enrich the data within it, cross-referencing between any existing documentation or any notes captured by the engineer performing the survey and data extraction on-site. This is then used to factor into the consideration of if a return visit is required, to explore further, and gain deeper insights, either by just using passive asset discovery capabilities again or utilising Active asset discovery capability if deemed viable.

The results of an accurate and reliable asset register developed for each remote site enable Admin Corp to move forwards with their overall ICS/OT cyber security programme, giving them visibility into their attack surface, the vulnerabilities which may exist within their environments, and allow them to effectively plan for future changes to mitigate, reduce or terminate cyber risks where appropriate. In addition, it has also helped them to understand their ICS/OT environment from a legacy perspective and now also supports their upgrade and maintenance programme.

CAF IGP Summary

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

- **A2.a A01:** Your organisational process ensures that security risks to networks and information systems relevant to essential functions are identified, analysed, prioritised, and managed.
- **A2.a A04:** Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential function.
- **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.

- **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 A04**: You regularly review and validate that your network and information systems have the expected, secured settings and configuration.

Statement of Support

This guidance has been produced with support from Awen Collective 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.

This document is provided on an information basis only, and whilst Awen Collective, 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, Awen Collective, 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 Awen Collective, 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.