VERVE

ACHIEVING CIS TOP 20 MATURITY IN OT SYSTEMS

CASE STUDY

Leading power company used Verve Industrial Protection to achieve target CIS Top 20 maturity levels across their industrial control systems

SUMMARY

A Verve client asked for help improving their cyber security readiness by achieving maturity across the CIS Top 20 Critical Security Controls.

The CSC 20 had never been applied at scale across industrial control systems and was though to be too high a bar for application to these systems.

This client wanted to maintain consistency between IT and OT and establish the same objectives for all assets. Over an eight-month period, the client achieved their objective and built a lasting compliance management reporting toolkit to ensure ongoing maintenance of the hard-won levels of security.

THE SITUATION

The leadership team of a major US-based energy company wanted to become a leader in securing all assets from possible cyber threats. This company had a range of operational assets - from power generation (coal, gas, wind, hydro, etc.) to transmission and distribution.

Like most power companies, they also have a range of IT assets for employees, customers, billing systems, etc. These assets are spread across a very wide geography across North America with small and large locations.

There were tens of thousands of computing assets across the company's operating businesses under a range of different regulatory requirements from PII to NERC CIP of different levels.

As a result, managing security was a complex task requiring different rule sets for different assets. There was an overall lack of clarity as to what the cyber security levels were. As a leader in the industry, the company decided to set a bar of higher standard for all areas of the company to reach.

Instead of spending months or years conducting assessments across different assets and computing types - or debating which standards are the best - the management team selected the CIS Controls. It maps to other standards (NIST CSF and NERC CIP) and could be executed across all IT and OT assets.

This was a controversial decision as no company had ever applied the CSC 20 to a set of Operational Technology assets at scale. Many argued it could not be accomplished without risking the integrity of OT assets, but management persevered in its aspiration.

The CSC 20 established a very specific set of objectives in a short time-period because of its included guidance of maturity levels. Instead of starting from scratch to define tiers or profiles, CSC 20 enabled the company to edit from a starting standard.

This significantly accelerated the creation of a set of milestones and provided the specificity necessary to give teams clarity of the objectives they were expected to achieve.

Instead of prescribing the means to achieve an objective, the leadership team targeted the end and let business units define how they'd achieve it.

They established a firm goal: Achieve a specific maturity level across all computing assets within one year. This required the entire security program - from assessment, to detailed vulnerability identification, to remediation of areas like patches, access management, to development of ongoing monitoring and compliance management, to revised procedures and training - to be completed within about nine months.

This company wanted action and results quickly.

THE SOLUTION

To achieve the step-change increase they were looking for, the company needed inventory, assessment, remediation, and compliance monitoring all in an integrated solution. They needed a combination of software and services that could bring these elements together – a true solution provider, not just a software vendor or an assessment/consulting firm.

The objective was to have a network of assets that were compliant by the end of the project. “Compliant” meant they knew what needed to be resolved, how to measure it, and controls and updates would be completed. Passwords needed to change to meet the new standard. Patches on OT assets had to be deployed to resolve vulnerabilities. Configurations needed to be changed to standard secure ones in line with CIS standards. Networks needed to be segmented. Compensating controls needed to be installed where devices could not meet standards due to technical limitations.

Not only were they looking for a solution to address all stages of a maturity improvement program, but it had to work across all OEM vendor equipment. Because all OT assets were in scope and the company has a range of control system vendor equipment in their fleet, the solution had to work equally well on Siemens, Emerson, GE, ABB, Schweitzer, Rockwell, Honeywell and dozens of other controls systems products.

A single, integrated solution that could provide cross-vendor assessment and remediation was required. Finally, the desired solution would provide visibility to the corporate security team for monitoring of compliance across all the controls, and also the ability to include OT system data in their overall Security Operations Center analytics.
Achieving compliance with the CSC 20 requires a suite of tools. There is no single solution that provides best-in-class protection for all of the elements that include everything from application whitelisting, to configuration change management, to backup and restore, to access management.

Therefore, the preferred solution needed to provide best-in-class coverage for all of the required elements, but also aggregate all of that information and reporting into a single user interface to provide consolidated reporting and analysis for security and compliance monitoring.

THE APPROACH

After a lengthy review of options, the client chose to partner with Verve Industrial for their multi-OEM fleet and their transmission and substation assets. Verve offers an integrated software and services solution necessary to achieve true maturity step-change in the time required.

The software also is vendor-agnostic and provides consolidated insight for the management and reporting of all necessary components of CSC 20 compliance.

The approach included 4 key steps:

1. Deploy the assessment tools

The first step is to assess, at a very granular level, any gaps between the current state and the target maturity level against all the 120+ sub-controls of the CSC 20. This requires a robust assessment tool set deployed on an asset-by-asset, network-by-network level for transparency to each individual network element. The key components assessment components include:

- Verve's automated asset inventory: a solution that gathers all IP addresses across the OT network and fingerprints them in a safe way. Critical to this solution is gathering a robust set of information on every asset. It has to reach 100% of the assets to meet the maturity requirements.
- Verve's endpoint manager: This endpoint solution gathers 1,000+ pieces of information on all Windows/Unix/Linux assets (such as installed software, ports, services, accounts, etc.) and reaches all embedded assets gathering firmware and other configuration information
- Vulnerability assessment: Data in Verve's asset inventory is used to conduct a passive assessment on the software and firmware gathered. This avoids the need for risky vulnerability scans on these sensitive OT systems.

- Network connectivity: Verve provides robust mapping of network connectivity to enable views of risky connections and potential segmentation gaps.
- A thorough review of all policies and procedures against Verve best practices built-up over our quarter-century of experience with control system procedures.

2. Build roadmap of necessary remediation steps to reach required maturity levels

With only eight months to touch thousands of assets and many thousands of remediation requirements, we developed a clear plan of attack and mapped out the necessary components. This is critical in an industrial controls environment where changes should be carefully planned to avoid disrupting the operational integrity of the processes that the devices are controlling. This step had several components:

- Build robust baselines of configurations, software, password status, vulnerabilities, etc. across all devices and networks
- Build site-by-site remediation plan that fits with operational schedules
- Develop longer-term roadmap for changes requiring capital equipment changes – e.g., network device upgrades, etc.

3. Remediate as necessary to achieve maturity objective

Remediation in industrial control systems requires the team understands cyber security and the individual control systems to which the security control is applied. In most cases, this requires onsite presence to ensure the proper operations during any changes.

Further, the tools deployed must monitor for threats or vulnerabilities and allow for actions and remediation, such as software removal, password changes and management, configuration change, etc. This step includes the following items, among others:

- Leverage Verve to make changes to assets and networks – e.g., removal of Kaspersky software across all sites, elimination of unnecessary services and ports, implementation of complex passwords on devices where feasible, etc.
- Record technical feasibility exceptions for any devices where the control was not feasible, and develop compensating controls in their place
- Create/revision procedures for areas such as patching, change management, etc.
- Lockdown application whitelisting
- Leverage the assessment tools installed in phase one to provide ongoing assessment in real time – e.g., patch updates, new asset discovery, change management alerting, etc.
- Deploy patches to bring software up to the supported level on all devices

4. Ensure compliance and maintenance of maturity

Any program to increase cyber security must ensure that the standard, once achieved, does not fade away. This requires several critical supporting components which we deployed:

- Install a compliance monitoring system that aggregates all of the controls into a single reporting functionality so that there is transparency if individual assets are no longer compliant with the standard
- Train personnel on the critical new procedures as well as using the new security elements such as password management.
- Initiate an update process for new assets etc. that are deployed into the system to ensure maintenance of compliance going forward.

THE RESULT

Over eight months, our client saw a dramatic improvement in their cyber security posture by taking a standards-based approach. By applying the CSC 20 as their standard, they quickly moved from theory and assessment to action.

They leveraged Verve as an integrated solution provider to provide the critical software elements and necessary services to monitor for threats and address the vulnerabilities in their control systems.

So often we hear about companies that start with deploying “threat monitoring” solutions without doing the hard work of remediating the known threats or vulnerabilities that already exist in their networks. Instead, our clients chose to base its actions on a clear set of standards as established by a broad group of cyber security experts driven out of the US DOD and NSA.

This standard provided them a robust roadmap from day one of the goals and objectives to achieve. They now have a new set of procedures, an ongoing monitoring and reporting system that integrates across all the necessary underlying tools, and a set of defensive applications that significantly improve the underlying level of cyber security across their system. The integrated approach achieved this quickly and at a lower cost.