VERVE
INDUSTRIAL PROTECTION

Case Study

ACHIEVING CIS TOP 20 MATURITY IN OT SYSTEMS

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

Abstract

Recently, a client of Verve Industrial asked us to help them dramatically improve their cybersecurity 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 thought to be too high a bar for application to these systems. This client wanted to maintain consistency between IT and OT and, hence, established the same objective for all of their assets. Over an 8-month period-of- time, this client with Verve's help not only achieved their objective, but also 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 decided that it should become a leader in securing all of their assets from possible cyber threats. This company has a range of operational assets – from power generation of all sorts (coal, gas, wind, hydro, etc.) to transmission to distribution. In addition, 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 large as well as small, remote locations. In all, there were tens of thousands of computing assets across all of the company's operating businesses. These computing assets were under a range of different regulatory requirements from PII to NERC CIP of different levels.

Managing security, as a result, was a complex task requiring different rule sets for different assets and a lack of clarity of what the overall level of real cybersecurity was. As a leader in the industry, the company decided it needed to establish a high bar and require all areas of the company to reach it.

Instead of spending months or years conducting assessments across all of their different asset and computing types or debating which standards were the best, the management team decided to select a very robust standard – the CIS CSC 20, which mapped to other standards such as NIST CSF and NERC CIP in many areas – and execute it across all of their assets, both IT and OT. This was a controversial decision as no company had ever applied the CSC 20 to a set of Operating Technology assets at scale. And many argued that it could not be accomplished without risking the integrity of the operational assets themselves. But management persevered in its aspiration.

The CSC20 allowed the company to establish 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 time to a clear set of milestones. It also provided the specificity necessary to give teams clarity of the objectives they were expected to achieve. Instead of proscribing the "means" of achieving the objective, the leadership team targeted the "ends" and let the business units define how they would achieve it.

They established a firm goal: achieve a specific maturity level across all computing assets within a year. This required that 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 – all be completed within

an approximately nine-month period-of-time. For many companies, they may still be assessing at that time frame. This company wanted action – fast.

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 that not only did they have to know what needed to be resolved and how to measure it, but the controls and updates all had to 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 did the solution need to address all stages of a maturity improvement program, but it also 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 also 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. To achieve 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 & 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 alternative options, the client chose Verve Industrial to partner with for the solution for their multi-OEM fleet and their transmission & substation assets. Verve offers an integrated software & services solution necessary to achieve true maturity step-change in the time required. The software also is vendor-agnostic and provides a single-pane-of-glass for the management and reporting of all the necessary components of CSC 20 compliance. The approach we took had 4 key steps:

1. Deploy the assessment tools
   As discussed, the first step is to assess at a very granular level what the gaps are between the current state and the target maturity level against all the 120+ sub-controls of the CSC 20. To accomplish this requires a robust assessment tool set deployed on an asset-by-asset, network-

by-network level to give 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 to gather a robust set of information on every asset. It has to reach 100% of the assets to meet the maturity requirements.
- Verve's End Point manager: This end point solution gathers 1000+ pieces of information on all Windows/Unix/Linux assets such as installed software, ports, services, accounts, etc. as well as reaches all of the embedded assets gathering firmware and other configuration information
- Vulnerability assessment: The Verve solution leverages the data in the Verve asset inventory 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: The Verve solution 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 8 months to touch thousands of assets and many thousands of remediation requirements, we needed a clear plan of attack with all of the necessary components mapped out. This is even more critical in an industrial controls environment where changes need to 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 that the team understand not only cybersecurity, but also 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 not only monitor for threats or vulnerabilities, but must also allow for actions and remediation such as software removal, password changes & management, configuration change, etc. This step included the following items, among others:
   - Leverage Verve tools 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
   - Creation/revision of procedures for areas such as patching, change management, etc.

- Lockdown application whitelisting
- Leverage the assessment tools installed in phase 1 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 cybersecurity 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 cybersecurity posture by taking a standards-based approach. By applying the CSC20 as their standard, they were able to quickly move from theory and assessment to action. By partnering with Verve, they had an integrated solution provider that could provide not only the critical software elements, but also the necessary services to not just monitor for threats but to 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. Our client instead chose to base its actions on a clear set of standards as established by a broad group of cybersecurity experts driven out of the US DOD and NSA. This standard allowed them to have a robust roadmap from day one of the goals and objectives to achieve.

Now they 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 cybersecurity across their system. And because they chose an integrated approach, they were able to achieve this much more quickly, and more cost effectively than piecemeal efforts might have allowed.

For more information please contact us at www.verveindustrial.com or info@verveindustrial.com