Case Study: A Standards-based Approach to ICS Cybersecurity

Applying the CIS Top 20 Security Controls in Industrial Control Systems

In 2017, a client of Verve Industrial asked us to help them dramatically improve their cybersecurity readiness by achieving a Level 2 maturity across the CIS Top 20 Critical Security Controls[1]. 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. However this client wanted to maintain a consistent program across both IT and OT and, hence, established the same objective for all of their assets.

[1] https://www.cisecurity.org/controls/

During the 8 month project Verve worked hand in hand with our client to not only establish a comprehensive CSC20 program in their OT environment, but to also build a sustainable, dynamic compliance and security management platform. This platform provides visibility into measurement, alerting or discovery/investigation as needed and is dynamically updated by a multitude of supporting sources. This platform ensures compliance but also captures value from their investment, speeds resolution of emerging events and provides unparalleled visibility into otherwise disconnected practices.

The Situation

Recently, the leadership team of a major US-based energy company decided that it should become a leader in securing all IP-enabled 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 all over 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 in scope for this effort.

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 real need for clarity on what the overall level of existing 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[2]. And many argued that it could not be accomplished without risking the integrity of the operational assets themselves. But management persevered in its aspiration.

They established a firm goal: achieve a certain maturity level across all computing assets with a firm deadline This required that the entire security program – from assessment, to detailed vulnerability profiles, to remediation of inadequate security practices like patching, access management, to development of ongoing monitoring and compliance management, to revised

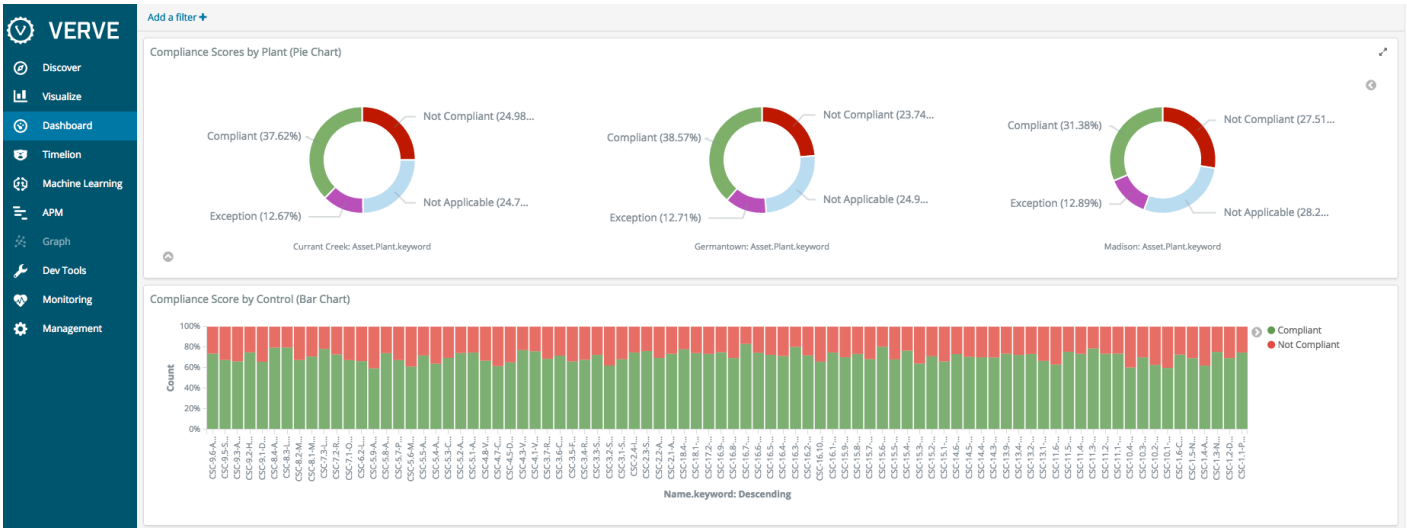
[2]Since the first publication of this case study the CIS has released an OT specific interpretation of its standards which align quite well to the method deployed at this operating company during this project - to learn more go here: https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/

procedures and training – all be completed within an approximately nine-month period-of-time. For many companies, they may still be assessing and planning in that sort of a time frame. This company wanted action – fast.

The Solution

To achieve the step-change increase they were looking for, the company needed a comprehensive asset profile/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. And since this was targeted at control systems, the solution provider needed to be as competent in the DCS/SCADA world as they were in cybersecurity.

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 and to the level dictated by the CISO office. Passwords needed to change to meet the new standard. Patches on OT assets had to be deployed to resolve vulnerabilities. Configurations needed to be hardened to be 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.

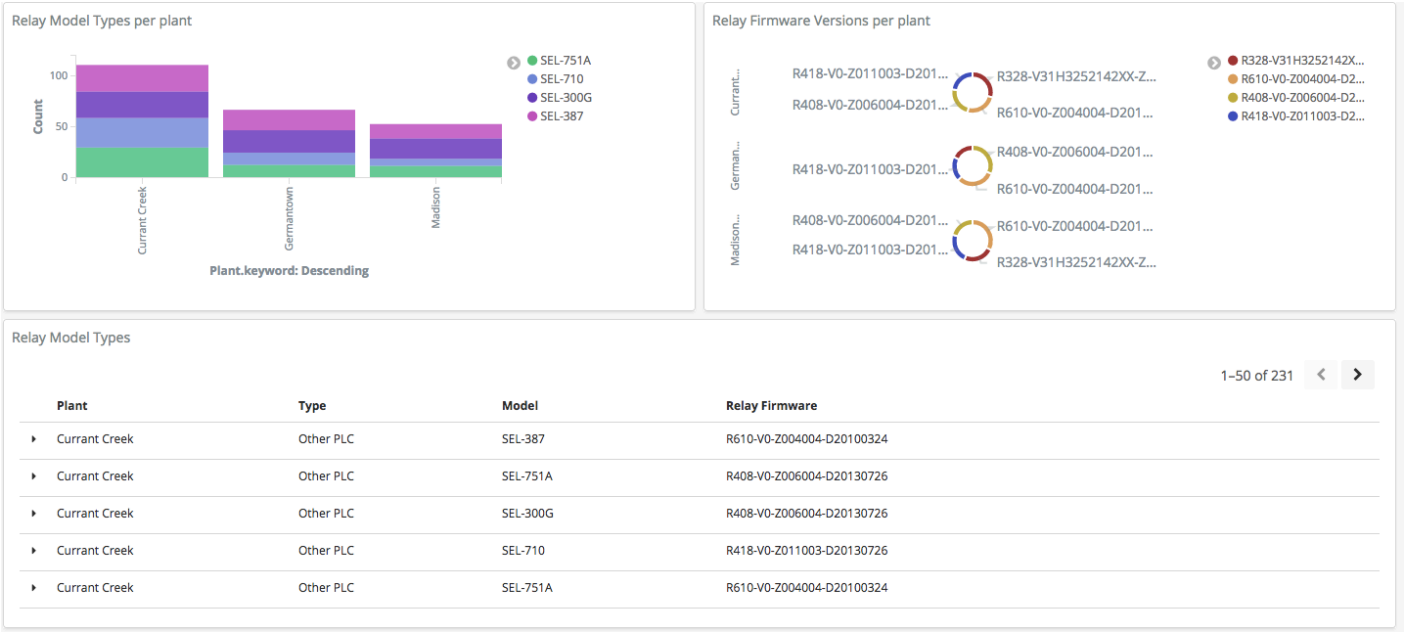


Not only did the solution need to address all stages of a maturity improvement program, but it also had to work across all OEM vendor equipment. Because all OT assets were in scope and the company has a range of control system vendor equipment in their fleet, the solution had to work equally well on 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. Most importantly, the project required ingenuity,

Copyright RKNeal LLC December 2017

flexibility, detailed knowledge of security and operational technology and the ability to ‘negotiate’ between security controls and operational needs.

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 offered an integrated software & services solution necessary to achieve true maturity step-change in the time allowed. Verve’s software and solutions are vendor-agnostic and our Verve Security Center software provides a single-pane-of-glass for the management and reporting of all necessary components of CSC 20 compliance. The approach we took had 4 key steps:

VERVE INDUSTRIAL PROTECTION

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 element in scope. The key 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 solution leverages leading vulnerability scanning tools for OS-devices such as workstations and servers, tuned for safe operation on ICS devices. It combines that with a review of known vulnerabilities on embedded devices to deliver a vulnerability profile across 100% of assets in the OT space – not just OS enabled systems
- Network diagrams: The Verve solution provides robust mapping of network connectivity to enable views of paths and potential segmentation gaps.
- A thorough review and, as required, revision of all policies and procedures against CSC20 and Verve best practices built-up over our quarter-century of experience with control system procedures.

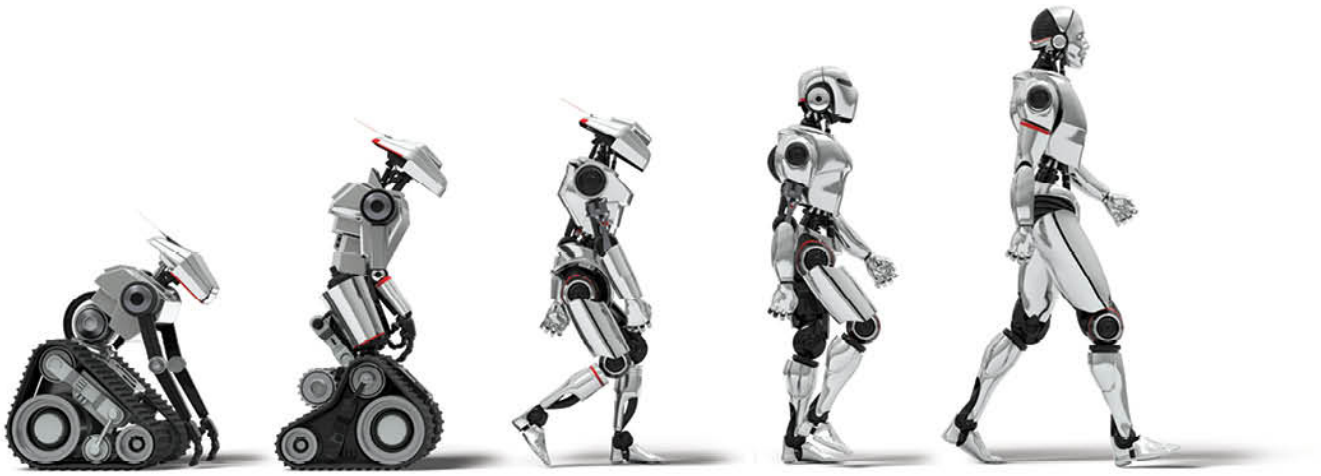
2. Build roadmap of necessary remediation steps to reach required maturity levels.

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 – eg., 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 expected operations during any system or security changes. Further the tools deployed must not only monitor for threats & vulnerabilities, but must also allow for actions towards remediation to be taken such as software removal, password changes & management, configuration change, etc. Once our base platform and its components were in place we were able to automate most and track all tasks towards remediation. This step included the following items, among others:
   - Leverage Verve tools to make changes to assets and networks – e.g., removal of decommissioned/unnecessary 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 partner 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. Perhaps most importantly, by housing this entire effort into a single, security portal that ties together multiple disciplines they ensure value for their investment, provide an unparalleled level of visibility into the entire program at a glance and greatly speed remediation and protection tasks.

VERVE
INDUSTRIAL PROTECTION

VERVE
INDUSTRIAL PROTECTION