Case Study

ACHIEVING NIST CSF MATURITY WITH VERVE SECURITY CENTER

Verve Industrial Protection offers a comprehensive solution for the NIST CSF via the Verve Security Center platform and VIP Services

Abstract: Industrial companies are beginning to realize that their manufacturing or processing facilities are under threat from targeted and untargeted cyber-attacks. While awareness is growing, many struggle with how make a difference in protecting these assets. The NIST Cybersecurity Framework is one method of measuring maturity in cyber defense and protection. Over the past several years, Verve Industrial Protection has helped a range of companies significantly increase their maturity against the NIST standard by deploying the Verve Security Center on clients’ OT or Industrial Control Systems. Verve technology and talent enables a dramatic, rapid increase in maturity as well as provides a foundation on which to build future maturity increases. This whitepaper provides one example of a customer’s journey to greater cyber maturity leveraging the Verve Security Center and VIP Services.
The Situation

An integrated energy company with a mix of heavily regulated and less regulated assets was searching for a way to improve cybersecurity on the OT assets in its portfolio. The company had successfully enhanced the security of its IT assets, but it did not feel that the frameworks and guidelines for the protection of information assets was applicable to the industrial control system assets.

The CEO and CFO demanded a way to measure the ROI of any investment in cybersecurity. It was not enough to say that tools were deployed or no intrusions were discovered or that any intrusion that was discovered was resolved in a certain window. They were seeking a maturity model that could provide a holistic and rigorous measurement system to track progress. The team knew they would need a “defense in depth” approach, but they were looking for a path and way to begin.

The first choice was to build off the NIST CSF standard as a way to measure current status and monitor progress against specific areas of cybersecurity. The NIST CSF provides a set of control guidelines more targeted at control systems rather that pure information systems. The team established a set of guidelines or “profiles” or target states of maturity against each of the primary categories of the NIST framework as seen below.

The NIST CSF Framework:

![NIST CSF Framework](image-url)
As they began, the company had little data on current procedures and even less data on individual assets and networks. Therefore, to get a read on their initial “baseline” profile, they conducted interviews and a quantitative survey of employees to assess where the maturity level of their OT networks and procedures.

Several key findings emerged:

1. The scores were relatively low across the board as these systems had not been subject to the traditional cybersecurity advances that the information systems had.
2. The scores were particularly low in the asset management, protective technology and processes, detection of threats, and recovery.
3. There were gaps in both process and technology
4. The organization needed better information on its assets and potential vulnerabilities to generate momentum for the program

The company set an objective that within 18 months they would see significant improvement across these dimensions.
The Solution

The company evaluated multiple technology solutions to address the technology components of the maturity gaps. They set forth a set of criteria for any solution:

- OEM Platform independent
- Scalable architecture across plants
- Robust asset management across OS, Networking, and embedded devices
- Single interface across endpoints
- Event logging, correlation & storage
- File integrity and configuration change monitoring
- Endpoint protection: AV & application whitelisting
- Patch management
- Backup and restore management
- Strong ICS-experienced support

After reviewing five or six different vendor options, the company chose the Verve Security Center (VSC) supported by VIP Services to ensure that the system was deployed, configured and serviced appropriately.

VSC includes 6 critical elements which are clearly aligned to the NIST components:

Verve Security Center Capabilities Map to NIST CSF
1. Verve Asset Manager: A proprietary OT-specific asset inventory solution that integrates data from OS devices using a safe and tested agent-based solution, networking devices using Verve’s network agentless solution, and all the OT embedded devices such as protective relays, controllers, etc. using Verve’s proprietary agentless OT communication stack.

VAM includes a low-cost, scalable architecture leveraging proprietary software to reach remote locations efficiently – and one that enables auto-identification of new devices as they are added to the network.

2. Verve Patch and Vulnerability Manager. An OT-focused closed-loop vulnerability & patching solution that allows for safe discovery of vulnerabilities without the need for risky scanning of these sensitive OT networks and integrates patch, configuration, account, software and other remediation actions in the same platform.

3. Verve endpoint protection: Verve has been deploying end point protection for over a decade on industrial control systems. This includes anti-virus and application whitelisting as well as host intrusion detection. Verve leverages leading solutions such as Symantec or McAfee for AV and has custom-tuned CarbonBlack’s Bit9 whitelisting solution for the specific needs of different OEM vendor equipment.
4. Verve SIEM for log & netflow management and correlation: Verve has dedicated significant investment to build a SIEM aggregation tool that can parse data from OT devices, network behavior, asset behavior, DCS alarms, etc. and provide meaningful insights as necessary for the challenging embedded devices in a control system.

5. Verve backup & restore: Verve’s platform is open and can integrate a range of backup solutions, but the most effective in an OT environment leverages the Avamar platform from Dell/EMC which can scale across networks and provide much lower bandwidth solution which is critical in these sensitive networks.

6. Verve Reporting and Analysis: One of the most critical features was the ability to aggregate all the underlying elements into a single database and user interface to reduce the cost and labor burden on an already taxed cybersecurity team. The solution had to have an integrating or orchestration layer to simplify the monitoring and compliance reporting. Verve Security Center leverages a NoSQL database and a modern stack user-interface which brings together all of this information into a searchable and automated asset management system to provide full visibility and actionability.

The Impact:

Over the next 18 months, the client saw significant improvements in its cybersecurity maturity as defined by the NIST CSF. 18 months after deploying Verve, the company reassessed their maturity against the same NIST CSF profiles as it had done at the beginning. The results were significant. Overall the company doubled its profile scores across all dimensions of NIST. The
greatest increases were in the areas of technology such as asset inventory, protection technology, detecting technologies as well as backup/restore.

Most importantly, the management was able to clearly demonstrate the ROI of cybersecurity tools with a very specific yardstick of metrics and measurements.

There is still work to be completed and the company is now focused on continuing to evolve and mature their security as they fine tune technology, install improved processes and training programs, and increase awareness overall.
Verve Security Center Capabilities Map to NIST CSF

***

We would be happy to provide more material or a demonstration of VSC and its capabilities at any time.