VERVE

ACHIEVING NIST CSF MATURITY WITH VERVE SECURITY CENTER

CASE STUDY

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

SUMMARY

Industrial companies understand their manufacturing or processing facilities are under threat from targeted and untargeted cyber attacks. While awareness grows, many struggle to protect their assets in a meaningful way.

The NIST Cyber Security Framework is one method for 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 case study provides one example of a customer's journey to greater greaterging the Verve Security Center and VIP Services.

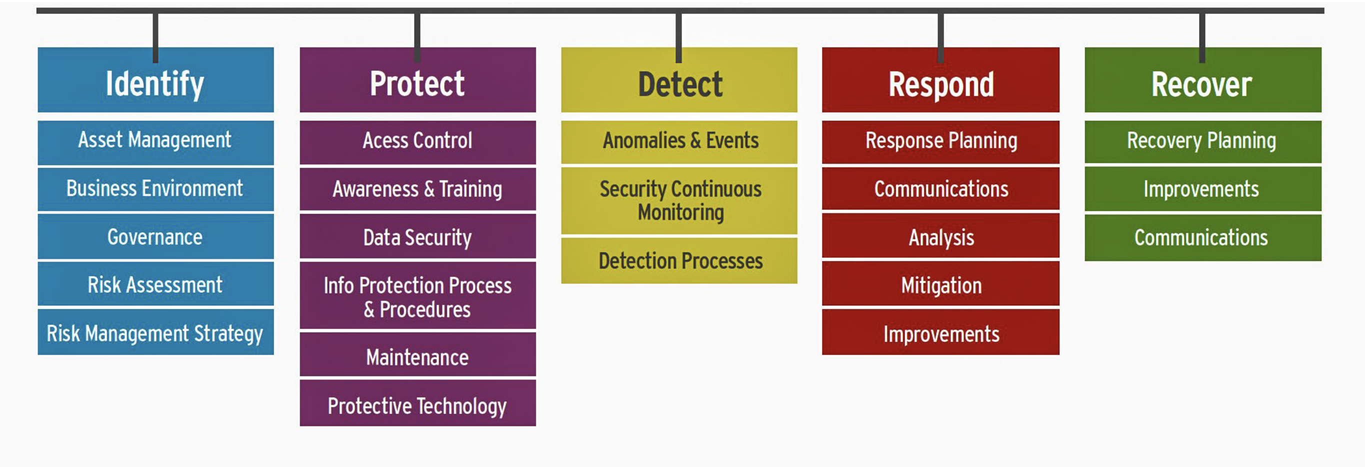
THE SITUATION

An integrated energy company with a mix of heavily regulated and less regulated assets wanted to improve cyber security on the OT assets in its portfolio. The company successfully enhanced the security of its IT assets, but 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 their investments in cyber security. 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 needed a robust "defense in depth" approach, so they started looking for a path and way to begin.

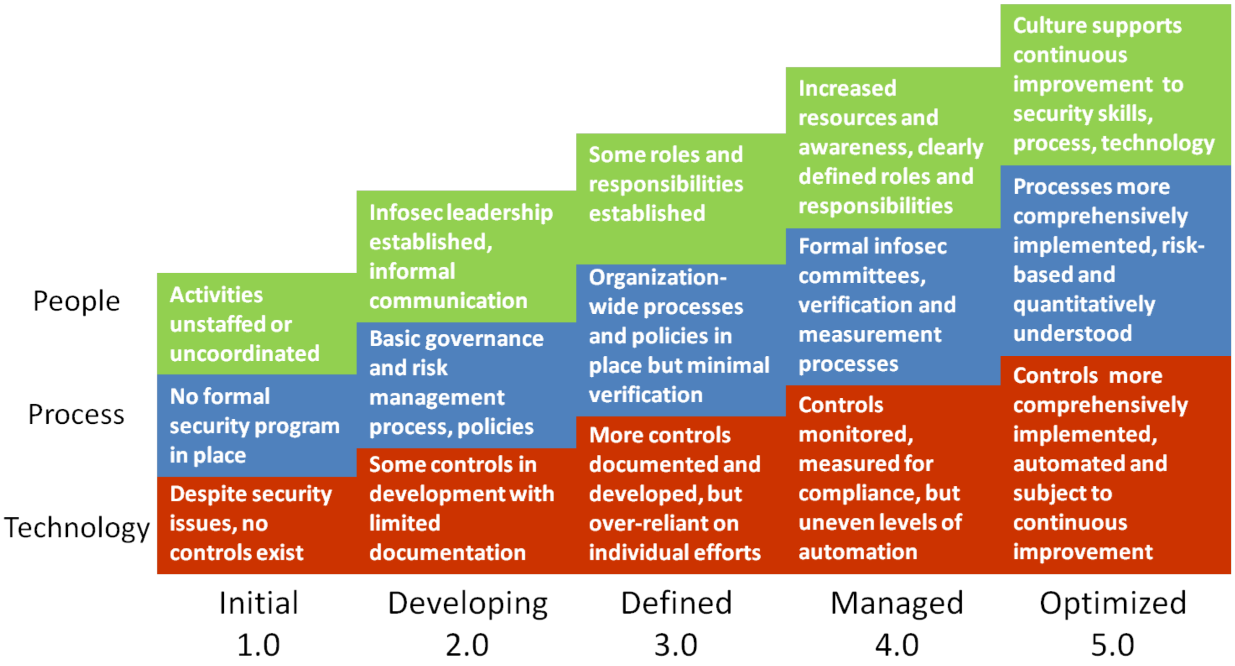
The first choice was to build off the NIST CSF standard to measure their current status and monitor progress against specific areas of cyber security. The NIST CSF provides a set of control guidelines more targeted at control systems, rather that pure information systems. The team established a set of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

NIST Cyber Security Framework



Identify	Protect	Detect	Respond	Recover
Asset Management	Acess Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Process & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Example Profiles or Maturity Levels



	Initial 1.0	Developing 2.0	Defined 3.0	Managed 4.0	Optimized 5.0
People	Activities unstaffed or uncoordinated	Infosec leadership established, informal communication	Some roles and responsibilities established	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
Process	No formal security program in place	Basic governance and risk management process, policies	Organization-wide processes and policies in place but minimal verification	Formal infosec committees, verification and measurement processes	Processes more comprehensively implemented, risk-based and quantitatively understood
Technology	Despite security issues, no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement

As they began the process, the company had little data on current procedures and even less data on individual assets and networks. To get a read on their initial "baseline" profile, they conducted interviews and a quantitative survey of employees to assess the maturity level of their networks and procedures.

Several key findings emerged:

1. The maturity scores were relatively low across the board as these systems had not been subject to the traditional cyber security 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 to see significant improvement across these dimensions within 18 months.

THE SOLUTION

The company evaluated multiple solutions to address the technology components of the maturity gaps. They set forth the following criteria:

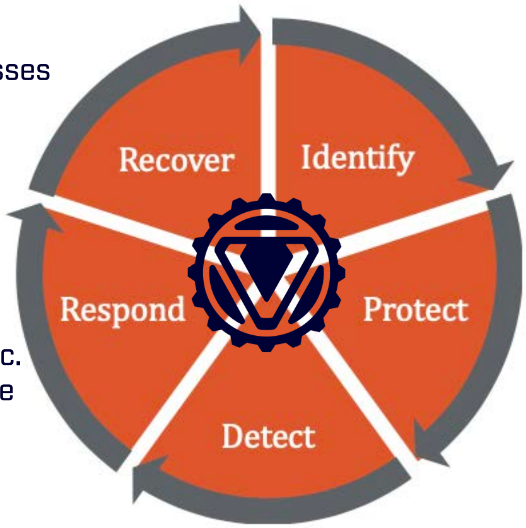
- OEM platform independent
- Scalable architecture across plants
- Robust asset management across OS, networking and embedded devices
- Single interface across endpoints
- Event logging, correlation and storage
- File integrity and configuration change monitoring
- Endpoint protection: antivirus and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

After reviewing five-to-six vendors, the company selected the Verve Security Center (VSC), supported by VIP Services, to ensure the system was deployed, configured and serviced appropriately.

VSC includes six critical elements, which are clearly aligned to the NIST components.

- Backup & restore all systems
- Remediate software malware
- Recovery procedures & processes

- Asset management
- Access control
- Software inventory
- Configuration baselines
- Network connectivity & rules
- Vulnerability assessment



- Incident troubleshooting
- Remove software, malware, etc.
- Kill chain analysis to root cause threat
- Communications

- Patch
- Standard secure configurations
- Antivirus
- Application & device whitelisting
- Network segmentation
- Identity management & authentication controls
- Change control procedures

- Monitor device performance
- Monitor account behavior
- Monitor and manage configuration changes
- Monitor device logs
- Monitor network traffic (flows & packets)
- Analyze anomalies: single and correlations

Verve Asset Manager (VAM): 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 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. It enables auto-identification of new devices as they are added to the network.

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

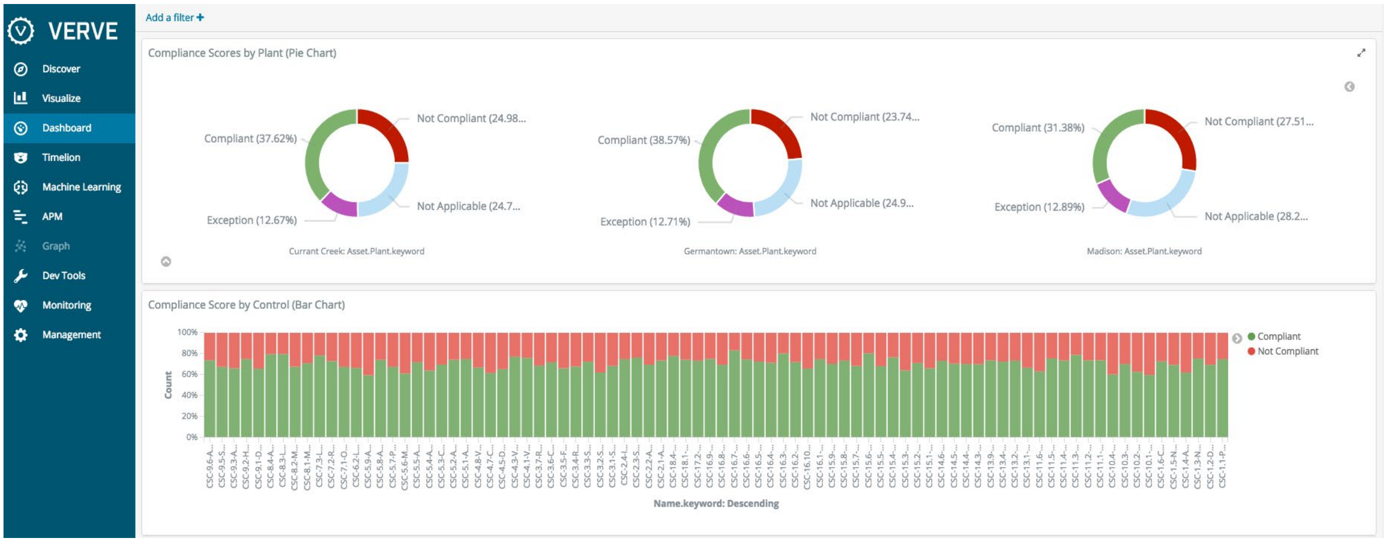
Verve Endpoint Protection: Verve has deployed endpoint protection for over a decade on industrial control systems. This includes anti-virus and application whitelisting, as well as host intrustion detection. Verve leverages leading solutions, such as Symantec or McAfee for AV and custom-tuned CarbonBlack's Bit9 whitelisting solution for the specific needs of different OEM vendor equipment.

Verve SIEM for log and netflow management and correlation: Verve has dedicated significant investment to build a SIEM aggregation tool that parses data from OT devices, network behavior, asset behavior, DCS alarms, etc. to provide meaningful insights for the challenging embedded devices in a control system.

Verve Backup and Restore: Verve's platform is open and integrates a range of backup solutions, but the most effective in an OT environment leverages the Avamar platform from Dell EMC to scale across networks and provide much lower bandwidth - which is critical in sensitive networks.

Verve Reporting and Analytics: One of the most critical features is the ability to aggregate the underlying elements into a single database and user interface to reduce the cost and labor burden on an already taxed cyber security team. The solution had an integration layer to simplify the monitoring and compliance reporting.

Verve Security Center leverages NoSQL database and a modern stack user interface to bring the information into a searchable and automated asset management system for full visibility and actionability.

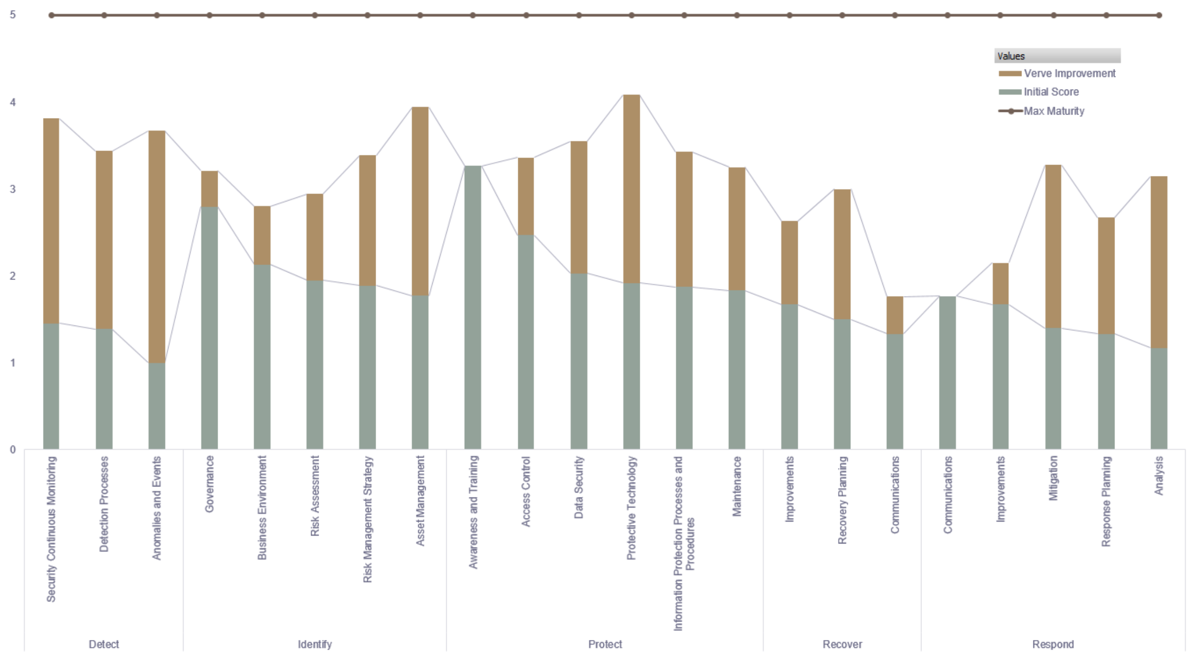


THE SOLUTION

Over the course of 18 months, the client saw significant improvements in its cyber security maturity as defined by the NIST CSF. After deploying Verve, the company reassessed their maturity against the same NIST CSF profiles as it had done in the beginning.

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 and backup/restore.

Most importantly, the management team could clearly demonstrate the ROI of its cyber security investments with very specific metrics and measurements.



There is still work to be completed. The company is continuing to evolve and mature their security program as they fine tune technology, install improved processes and training programs, and increase overall awareness.