ARC VIEW

OCTOBER 27, 2016

RKNEAL Verve Security Center Supports Effective, Efficient Cybersecurity Management

By Sid Snitkin

Keywords

Industrial Cybersecurity Management Solutions, RKNEAL Verve Security Center, Asset Inventory Management, Patch Management, Incident Response, Compliance Support

Summary

The risk of cyber incidents remains high for industrial plants and critical infrastructure. Many operators have invested in sophisticated cyber defenses, but most struggle to sustain them. Staffs are overwhelmed with the complexity of managing a never-ending stream of product patches and updates for a multitude of assets and security products. They likewise struggle to collect information to demonstrate ongoing compliance with regulations like NERC CIP.

A recent ARC briefing with RKNEAL executives on the company's Verve Security Center focused on how it can help companies sustain plant cybersecurity defenses. Product features also reflect the company's deep understanding of automation systems and industrial cybersecurity.

Overcoming these challenges is critical. Too many companies are operating with a false sense of security. Plants are living with latent vulnerabilities that leave them open to intentional and unintentional cyber incidents. The resulting risks to safety and operations are real and need to be addressed.

These challenges were the focus of a recent briefing that RKNEAL executives provided for ARC. Their company has been providing control system engineering services to critical infrastructure organizations for over twenty years. In recent years, it has also provided its clients with cybersecurity assessments, implementations, and solutions management. This work led to the development of the Verve Security Center, a platform for cybersecurity management that integrates a range of best-in-class cybersecurity management tools and supports a wide range of control system devices and manufacturers.

Industrial Cybersecurity Management Is Challenging

ARC end user research consistently shows that many industrial companies struggle to maintain plant cybersecurity defenses. Key reasons for this include lack of resources and lack of effective cybersecurity management tools.

While cybersecurity is generally viewed as an IT issue, most industrial companies rely upon control system engineers to manage plant cybersecurity solutions. They have a vested interest in control system security and a deep understanding of operational constraints and control system equipment. But they also have other, high-priority responsibilities that limit the time available to maintain cybersecurity. Available time is further reduced in regulated industries, like electric power, where these same people are tasked with collecting compliance information.

While modern control systems include a lot of commercial IT-based products, they operate in an environment with unique constraints. This requires special care when selecting and using system maintenance tools, particularly those that perform network scans or automatic updates and reboots. Control systems also include many cybersecurity-related assets, from many different automation suppliers, with special operating systems and protocols. Traditional IT management tools lack the functionality and coverage to support all these needs in operational environments.

Recognizing this situation, some vendors have worked with security software to modify and support these tools for operational deployment. While these are helpful, their scope is generally limited to the specific vendor's products. Thus, a typical industrial plant needs a portfolio of security tools to cover all its needs. This creates additional management problems and a proliferation of costly licenses. Also, these tools are often incompatible with one another, so collecting compliance requirements remains a major effort. Lack of a single, integrated view of cybersecurity status also limits visibility into a plant's total cybersecurity risks.

Industrial Cybersecurity Management Selection Criteria

ARC has conducted numerous surveys and one-on-one discussions with industrial end users to understand the kinds of tools they need for cybersecurity management. Based on this research ARC has defined a detailed set of criteria for selecting industrial cybersecurity management solutions.

These selection criteria include:

- Asset Inventory Management
- Product Configuration Support
- Backup Management
- Change and Patch Management
- Compliance Reporting Support
- Single, Comprehensive Platform

The RKNEAL Verve Security Center

RKNEAL, which has been providing automation and cybersecurity services to industrial plants for many years, appears to have a clear understanding of the challenges that control engineers face in maintaining cybersecurity technology. Much of the company's work has been in the demanding power industry, so it is familiar with a wide range of DCS, PLC, and SCADA systems, as well as specialized control devices like IEDs and smart relays. The company also has ten years of rich experience dealing with NERC CIP requirements.

Verve Security Center Capabilities

RKNEAL's Verve Security Center reflects extensive automation and cybersecurity experience. This comprehensive platform for cybersecurity management integrates a range of best-in-class cybersecurity management

tools and supports a wide range of control system devices and manufacturers. While ARC did not perform a detailed product review, RKNEAL executives provided an in-depth demo of the solution that impressed us with its usability and coverage across ARC's selection criteria for industrial cybersecurity management solutions.

Asset Inventory Management

Verve enables users to structure all control system assets into understandable hierarchies. This enables data to be rapidly filtered using a variety of parameters (plant area, type of device, geography, etc.) and device roles (engineering workstation, operator station, controller, relay, etc.).

Verve provides automatic collection of asset data from all control system assets. It uses a best-in-class tool for Windows, Unix, and Linux devices that have been customized for use within plant control systems. Additionally, the company provides an internally-developed FDI (Foreign Device Interface) tool for a wide range of unique control system devices from popular suppliers like ABB, Emerson, Schweitzer, etc. With these tools, control engineers can automatically collect data for every connected device, including unmanaged devices for which agents cannot be deployed. Collected data identifies the device and a library of device-specific templates are provided for intelligent parsing of configuration information so that data can be used to evaluate patches and automatically detect changes.

Product Configuration Support

While we didn't have an opportunity see the solution operating on a client's system, RKNEAL described the extensive work it has done to customize and extend best-in-class cybersecurity products for the needs of industrial operations and users. For example, the company noted how it has developed specific rules for application whitelisting for a variety of control system assets. This greatly reduces the time engineers need to spend identifying valid applications in every cyber asset. It also enables rapid rollout and management of whitelisting on new devices. The company also noted how SIEM customization also saves engineers' time by integrating alerts with other asset information.

Backup Management

Verve uses Acronis or other backup tools to perform system backups. These tools have been tightly integrated with other Verve capabilities. For

example, backups can be scheduled directly from the asset hierarchy, using a common interface that is also used for scheduling patches. This association with the asset hierarchy provides asset-specific records of when backups are performed and convenient restoration of assets on a selective, granular basis. Because these are full-image backups (even for agentless devices), customers can get back up on line much faster should a device fail.

Change and Patch Management

Patch management capabilities was a key focus of the demo and ARC was advised that change management is handled in an analogous manner.

Patch management starts when the company receives an alert from any source. This information includes vendor, product, profile, category, severity, and release date, which are updated within Verve. The interface also enables users to associate alerts with affected assets in the system, and fields are provided to track actions taken.

Verve includes capabilities to schedule deployment of patches. These can be automatically implemented for PC-based assets with an appropriate agent installed. Instructions for implementing patches can be defined at the Verve console. Automatic patching is managed by agents that poll the Verve Security Center periodically for required patches and downloads and manage the implementation as per the specified directions. Significantly that does not require automatic rebooting of the device, which is critical in industrial environments. Non-agent devices need to be manually patched, but Verve still provides fields for communicating instructions and recording when patches have been completed.

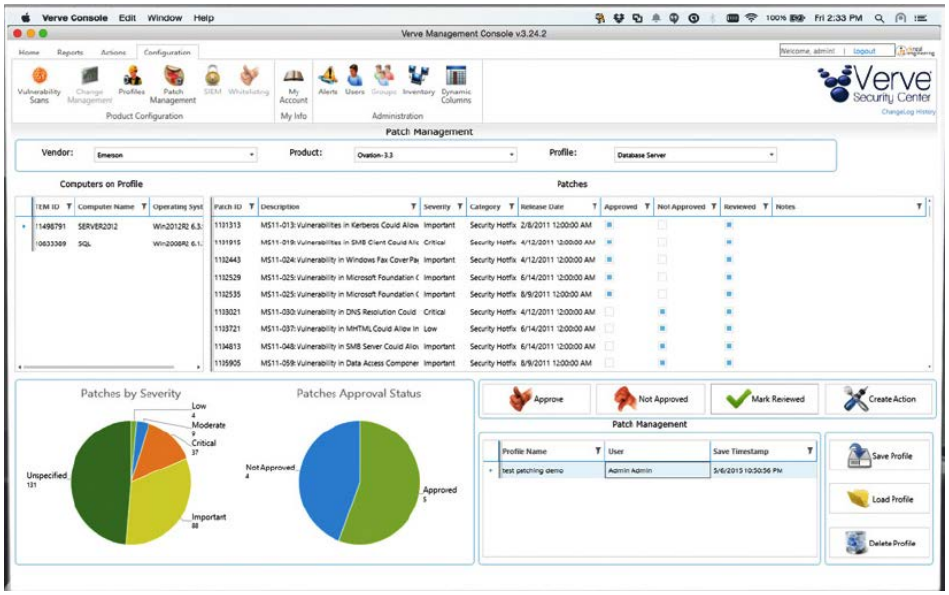
Verve also includes the capabilities to detect unexpected changes and anomalous behavior in cyber assets. It makes use of advanced configuration change tools such as Tripwire to monitor supported assets and its FDI service automatically scans controllers, IEDs, PLCs, etc. to alert for graphic, ladder logic, or other changes. Any differences in control configuration is then fed to configuration management tools for action/investigation by the user. The solution also supports use of Nessus to scan assets for known vulnerabilities. This is integrated with SIEM alerts to provide users a single list of issues on the system dashboard, linked with the asset hierarchy.

Compliance Reporting Support

Verve supports compliance reporting through its other capabilities. These include the ability to automatically collect and organize configuration information in a convenient asset hierarchy. Patch management records provide evidence to demonstrate ongoing care and maintenance.

Single Comprehensive Solution

The Verve platform provides a single dashboard to help manage cybersecurity for all plant assets. RKNEAL has selected and customized best-in-class tools with an eye toward ensuring a supplier-agnostic solution that covers the needs of plants with multiple automation vendor products. The broad list of supported vendors and products helps demonstrate Verve's comprehensiveness and broad applicability.



Verve Manages All Plant Assets Through a Single Dashboard

Recommendations

Every industrial company needs a strong program to maintain cyber defenses. Lack of resources prevent many companies from achieving this basic goal. Automating these activities is the best way to lessen the load. ARC recommends that all industrial companies consider software like Verve as a key element in their cybersecurity strategy.

For further information or to provide feedback on this article, please contact your account manager or the author at srsnitkin@arcweb.com. ARC Views are pub-