Protecting Critical Infrastructure

SCADA Network Security Monitoring

March 20, 2015

Table of Contents

I. Introduction

SCADA Systems

The term SCADA stands for Supervisory Control and Data Acquisition. It represents a family of protocols that can be used to monitor and manage a variety of machinery and equipment involved with many activities, including power generation and distribution, manufacturing processes, large-scale chemical processes and transportation of materials.

SCADA systems are used for many different types of processes that require monitoring, reporting or control from a computer system. SCADA devices are managed and report information to control centers through a variety of protocols including DNP3, ICCP and MODBUS protocols. SCADA systems are used for control of systems requiring both human and automated interaction.

Because SCADA systems are typically used in private and public organizations that provide critical services to the general population such as water, power, telecommunication and other services, they are often a part of critical infrastructure. Various studies and assessments have revealed that there is a lack of security in SCADA systems due to their fragile nature and their susceptibility to disruption with traditional vulnerability assessment techniques. Private and public organizations have placed more reliance on the internet and commercial off-the-shelf software that expose SCADA networks to new vulnerabilities.

In This Paper

This paper discusses a variety of SCADA security issues, including an analysis of how active vulnerability assessments can disrupt older networks, and how continuous network monitoring can help avoid this issue. In addition, this paper discusses how Tenable's solutions can be used to facilitate the Department of Energy recommendations to improve SCADA networks.

SCADA Security

The reality is that the actual SCADA protocols are subject to the same sorts of attack techniques that email, web servers and file transfer protocols are subject to. These include denial of service, buffer overflows and more. Any vendor who sells a SCADA device may have made the same sort of programming errors that any number of other vendors make.

To make matters worse, the SCADA devices themselves may reside on networks that have other types of traditional vulnerabilities. For example, the servers that run a SCADA protocol may also be running an unauthorized web server or have an unpatched kernel. Any vulnerability in an underlying device on a SCADA network may ultimately result in the potential to control or disable the entire SCADA network.

Assessing the Security of SCADA Networks

From a technology point of view, SCADA networks (that run over routed protocols like IP) are like any other network. They have various nodes and communicate over various protocols. Nodes are added and removed over time as well. However, there are two significant technical differences.

First, many SCADA networks tend to make use of older equipment. This is not to say a new SCADA network built today would use Windows XP as compared to Windows 2012, but a SCADA network built in 1995 may not have seen a need to upgrade to Windows 2012. This can also be true of the network infrastructure. Second, SCADA networks also run the DNP3, ICCP and MODBUS protocols. These protocols are just like any other type of protocol such as HTTP, DNS or SMTP in that they have their own expectations and rules for client and server communication, timing, data encoding and data formatting.

Besides the technological differences, there are also much larger political differences. SCADA networks often need to run 24x7 or account for a process that directly generates revenue to the organization. Because of this, any notion of a security issue can become politicized. This can directly impact how often security assessments are performed, what is done with the information once it is discovered and how corrective actions are implemented.

Network vulnerability scanners are a standard tool for quickly and actively discovering all hosts on a network, which services they are running, and which vulnerabilities are present. However, the techniques of port scanning, service fingerprinting and rapidly probing hosts to determine the present vulnerabilities can negatively impact SCADA networks.

Tenable™ offers continuous network monitoring for SCADA networks. Using Tenable SecurityCenter Continuous View® (SecurityCenter CV™), organizations can not only detect vulnerabilities through the SCADA-specific audits available to the Tenable Nessus® component of SecurityCenter CV, but also monitor network traffic for vulnerabilities using the Passive Vulnerability Scanner® (PVS™) component of SecurityCenter CV.

Many organizations have adopted network policies and procedures that forbid traditional vulnerability assessments on production networks because they may cause a repeated outage. These policies and procedures are usually adopted because it is too difficult to actually remediate the root cause of the security issues. In these cases, Tenable recommends using PVS through SecurityCenter CV for passive network monitoring. This allows discovery of not only SCADA specific information, but also all network vulnerabilities.

II. SCADA Network Attacks

Different Types of Attacks

This section of the paper discusses various attack scenarios against SCADA networks. They vary in complexity, intent and require access vectors for execution. The purpose in this section is to give the reader a sense of the many different types of security issues that a vulnerable SCADA network represents.

Affecting Display and Status Screens

Many SCADA networks have a type of master control panel or command center. For reliability and redundancy, most networks have multiple control centers. Attackers that gain access to a SCADA network can use a variety of techniques to alter the information consumed by the control center. Insiders to the network may be able to compromise servers on the network and change their data. Outsiders to the network may be able to exploit a vulnerability that gives them similar access to that of an insider. In both cases, information about key processes can be altered at the source of the data to present different information to operators and control systems.

Taking Over the Command Center

If the command center is not protected by security patches, firewalls, intrusion prevention and other mechanisms, it may be possible for an intruder to gain complete control over the SCADA networks. Modern control centers use a combination of Unix, Windows and web-based SCADA management tools. Each of these tools may be installed on any number of operating systems and applications such as Apache or Microsoft IIS web servers, which can introduce vulnerabilities into the organization.

An attacker who has control over the SCADA network may not even need to understand the underlying SCADA protocols. Instead, they will likely be presented with any user interface that a normal control center operator would use. These displays often include documentation and procedures for emergencies and change control. This information can be used by a remote attacker to understand how to control the SCADA network.

Using the Nessus SCADA checks and the PVS component, SecurityCenter CV can identify a variety of SCADA management applications and diagnostic software. These checks can be used to help create asset lists of important devices and then monitor them for attack and access.

Disrupting Processes

Any SCADA system that manages a real-time or 24x7 operation can be used to prevent that operation from occurring. Attackers, intruders and malicious insiders can use network vulnerabilities to send shut down and power off messages to equipment performing a variety of processes resulting in denial of service.

If direct manipulation of the SCADA devices is not possible, it may also be possible to prevent communication from a control center to the SCADA devices. This may be all that is required for a hostile agent to prevent normal operations of a SCADA network device.

Since SCADA devices are usually physically inconvenient to get access to, an intruder may be able to keep the key systems powered off or out of commission and override any commands sent.

These effects can also manifest in the case of a malware outbreak. Increased bandwidth usage, support systems being infected and overloading CPUs can keep a control center from managing SCADA equipment.

One of the SCADA probes supported through Nessus is to test if a system that speaks the DNP3 protocol supports an unsolicited response. Typically, DNP3 is used much like SNMP in a polling mode. However, a remote device may be configured to send new information in real time to the management node via a DNP3 unsolicited response. If this is the case, it may be possible for an adversary to remote to the management station or console, to flood it with messages that may consume CPU resources, have false data or prevent legitimate messages from being received.

Damaging Equipment and Property

Since SCADA devices control many different physical processes, it may be possible to not only disrupt or disable operations, but it may also be possible to create permanent damage.

There are simply too many combinations of physical processes and any safety controls that may be in place to truly assess this vulnerability. Most SCADA environments do not have a self-destruct sequence seen in the movies. Instead, most high availability or 24x7 plants have a variety of physical and electronic safety precautions. For example, anything that physically moves at all likely has a governor on it that limits a top speed, regardless of what the SCADA control unit says. Similarly, ovens, power generators and power relay stations all have physical safety limitations built into them for what they can and cannot do.

However, an insider who knows where the safety mechanisms are and has malicious intent to affect some sort of damage inside those parameters can still present a threat to organizations. Examples include disabling air conditioning in a data center or allowing chemical processes to occur longer, which can require physical cleaning before the equipment can be recovered.

III. Active Assessment Considerations

Quick Review of Active Scanners

A network vulnerability scanner generates a wide variety of IP packets to discover other active nodes, what services they are running and what vulnerabilities are present. They are often targeted against a broad range of IP addresses and methodically sweep through the range until each IP has been assessed. Scanners have different techniques for determining if a host is alive and for choosing which methods should be employed to discover running services.

Impact to SCADA Protocols

There is nothing inherently insecure about the core SCADA protocols; DNP3, ICCP and MODBUS. The issue can be how various SCADA manufacturers have implemented these protocols.

During a port scan, a vulnerability scanner may attempt to open up a port listened to by one of the SCADA protocols. If the implementation of the SCADA protocol is not robust, it may lead to a crash or a denial of service. The specific failure mode results in the combination of implementation flaws and scan method. Some failure modes cause immediate crashes and some may take several queries to result in a crash. Other failure modes result in slow performance or cutting off access to other services. Poorly written network daemons or implementation issues on embedded devices may also lead to unexpected behavior.

This is extremely relevant to SCADA protocols. A majority of SCADA devices operate on embedded devices. If any of these devices have implemented their SCADA protocols in such a way that errors are not handled gracefully, they could open themselves up to inadvertent denial of service attacks. During a network vulnerability assessment, port scans and network probes of SCADA protocols can cause the devices to lock up or become unavailable.

Impact to Older Operating Systems and Network Infrastructure

Similar to issues with SCADA devices, older operating systems have a variety of denial of service issues that can occur during network vulnerability assessments. Older versions of Cisco routers and switches also have similar issues.

Many of these attacks have been well documented and are understood by the operating system vendors and the security community. However, for whatever reason, these systems are often present on older SCADA network implementations.

Although the technology involved is not particular to SCADA, if one of these older operating systems is running a SCADA client or server application, any impact to the underlying system will also impact the SCADA application.

Specific Nessus SCADA Checks

Nessus and SecurityCenter CV customers have access to many SCADA specific plugins. These plugins were developed for Tenable by Digital Bond Consulting to specifically test and identify a wide variety of common SCADA devices.

Performing Active SCADA Assessments with Nessus

When performing active vulnerability assessments with Nessus and SecurityCenter CV, organizations should take the following precautions:

- Assess a SCADA test lab before assessing a production environment to identify any potential impact from active scanning.
- When assessing operational SCADA devices, ensure that a second device is available for fail over and ensure that the device operators are informed of the scheduled assessment.
- To be safe, make sure Nessus scan polices have Safe checks enabled and Thorough tests disabled. Tenable has previously blogged about safe checks usage for Nessus at tenable.com/blog.

Political Sensitivity

If an organization responsible for operating SCADA devices feels that vulnerability assessments may impact their operation or show that the operation is running vulnerable applications, they may implement political and technical mechanisms to prevent scanning.

They may simply ask the security organization or the security organization's management to not scan them. In these cases, there is usually some other form of assessment done such as physical inspections, reference server configuration reviews or even test lab auditing. Tenable has observed organizations where these techniques are effective, but have also observed organizations where these techniques were really delay or avoidance tactics.

In cases where there has been a prior incident that an assessment or an attack did impact SCADA operations, some organizations have chosen to implement routing and firewall policies to segment the networks. These are effective as long as the perimeter does not change, and Tenable has worked with many different companies running SCADA networks that did not realize other network connections existed outside the firewall.

IV. Tenable Solutions for SCADA Security Monitoring

Tenable provides enterprise-class solutions for continuous network monitoring, including vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure USGCB, FISMA and PCI compliance. Tenable is uniquely positioned to detect vulnerabilities with active and passive assessments and analysis, and host-based patch monitoring for enterprise networks. Key product lines include: Tenable SecurityCenter Continuous View, for enterprise security management, continuous network monitoring, log aggregation and analysis and Nessus, the leading global technology utilized for vulnerability assessments. More information can be found on these products by visiting tenable.com.

The next sections will discuss how Tenable's products can be implemented to audit, verify and protect SCADA networks and the benefits that each Tenable module provides.

SecurityCenter Continuous View

Tenable SecurityCenter Continuous View (SecurityCenter CV) provides a continuous network monitoring platform that brings information from around the network to a single management console. SecurityCenter CV uses Nessus, the Passive Vulnerability Center, and the Log Correlation Engine® to create a comprehensive, continuous view of the network.

SecurityCenter CV is used to manage the information collected by the Log Correlation Engine, Passive Vulnerability Scanner and Nessus in a single web-based, role-based security management console. It can control and manage active assessments and credentialed patch audits with Nessus, and combine this with passive continuous network monitoring from the Passive Vulnerability Scanner. This makes auditing SCADA networks much easier. New devices can be quickly identified and devices operating with unauthorized protocols or attempting unauthorized communications can be managed.

SecurityCenter CV has the ability to automatically discover parts of an organization and identify them as an asset group. For example, an asset group could be a list of any devices that speak the SCADA DNP3 protocol. This group could then be used as an access control mechanism. Only certain users of SecurityCenter CV would have access to this asset list, and only they would be able to analyze, report or manage the vulnerabilities.

In addition, Tenable customers utilizing SecurityCenter CV can build many different types of asset group hierarchies. SecurityCenter CV groups can overlap. For example, if all SCADA network addresses can be mapped to a physical plant or building, then groups can be created and named after these physical locations. Similarly, if network addresses can be mapped to a specific SCADA function, then groups can be created for those functions. Having multiple asset groups allows a manager to view large amounts of security data and quickly identify trends.

Passive Vulnerability Scanner

The Passive Vulnerability Scanner (PVS) component of SecurityCenter CV is a network-monitoring product that reports a wide variety of security data including active hosts, protocols in use, and any vulnerabilities associated with them. It monitors network traffic 24x7 and reports on any observed vulnerabilities.

PVS is ideally suited for monitoring SCADA networks. It passively determines any device that speaks client or server SCADA protocols including DNP3 and MODBUS. While performing this discovery, PVS can also look for thousands of vulnerabilities in non-SCADA applications such as Apache, BIND and Exchange.

As PVS discovers what hosts are active and which applications with vulnerabilities they are using, it also catalogs how each host communicates. For any given host, PVS will log what ports the device browses on. This is an excellent way to discern firewall rules or access control policies. For example, PVS can be used to identify each host on a SCADA network that also uses TCP port 80 for web browsing.

For more intensive analysis, PVS can also log which unique hosts are communicated with. Continuing the previous example, PVS can also be configured to not only detect that TCP port 80 is browsed by a host, but also log which other hosts that host connects to on TCP port 80. The same process can be used to identify which hosts communicate on SCADA protocols as well as which other hosts they communicate with.

Since PVS passively monitors network traffic, there is absolutely no network impact. As long as PVS can observe network traffic, it will create an accurate report of all known SCADA devices and vulnerabilities associated with the monitored network.

Log Correlation Engine

SecurityCenter CV uses the Log Correlation Engine (LCE®) component to aggregate, normalize and correlate logs from various devices. Any application that generates logs can be aggregated by the LCE. These consumed logs can be used for correlation rules as well as analyzed for deviations from previous behavior.

The LCE accepts logs from many applications and operating systems associated with SCADA networks. It also accepts SCADA client and server events from the PVS component of SecurityCenter CV. Tenable has written a correlation rule set for the LCE that can specifically alert when a new SCADA client or server is active.

The LCE can also accept input from NetFlow and direct network traffic monitoring. These logs can be used to keep a forensic record of every transaction on a SCADA network. If an outage or incident occurs, the LCE can be used to analyze any traffic or activity that occurred prior to the event.

Finally, LCE can analyze both network logs as well as firewall and application logs to summarize remote access sources. This can help identify connections that are originating outside of the SCADA network. These connections may not be secured and could require additional monitoring or access control.

Nessus

Nessus can be used to identify many different types of applications and vulnerabilities. When managed by SecurityCenter, it can effectively be used to monitor the security of SCADA networks.

In high-availability environments, Tenable recommends a combination of active, passive and host-based continuous network monitoring. Nessus performs both network assessments as well as host-based patch and configuration audits.

Tenable’s Support for Intrusion Detection Systems

SecurityCenter CV accepts logs from leading network IDS solutions. Combining IDS events with logs allows for deeper correlation to reduce false positives as well as to more accurately detect a compromise or denial of service incident.

This also reduces the workload of any staff dedicated to network security monitoring. By using only one console, security staff only needs to become familiar with one set of tools for reporting, analyzing logs and correlating events.

V. 21 Steps to Improving Cyber Security of SCADA Networks

Introduction

The U.S. Department of Energy has provided guidelines on how to secure SCADA networks in a paper titled "21 Steps to Improve Cyber Security of SCADA Networks". The paper describes recommendations for how the security of SCADA networks can be improved. This section highlights how Tenable's solutions can be applied to facilitate a majority of these recommendations. For each of the items, how Tenable's solutions can help is specifically discussed.

1. Identify all connections to SCADA networks

SecurityCenter CV and its PVS component can be used to identify all active SCADA devices through passive network analysis. The Nessus component of SecurityCenter CV can also perform assessments of SCADA devices with specific SCADA plugins.

This information can be used to create an asset group within SecurityCenter CV. This asset group can then be used to analyze network traffic, access logs, firewall logs and other types of data collected by the LCE component of SecurityCenter CV. This analysis will identify any network activity and report on all connections to the SCADA devices.

Since larger networks often have a certain degree of complexity in them, SecurityCenter CV allows for many different types of asset groups to be defined or discovered. For example, PVS might identify a SCADA client, but it might also identify it as a running a Windows operating system. These two pieces of information can be used to help build a specific list of Windows servers running SCADA client applications.

2. Disconnect unnecessary connections to the SCADA network

If an access control policy is put into place that forbids connections from certain networks to other SCADA networks, SecurityCenter CV can help monitor to enforce this policy.

Network devices such as firewalls generate tremendous amounts of logs. SecurityCenter CV can be used to process the logs from these network devices. It can also be configured with the network addresses that are to be denied access and alert accordingly.

Similarly, many of the logs processed by SecurityCenter CV can also be modified to alert when an access control violation has occurred. For example, simple log events such as a valid web password can be correlated with the source IP address to find evidence or alert when unauthorized networks connect to the SCADA network.

3. Evaluate and strengthen the security of any remaining connections to the SCADA network

For connections that are authorized, solutions to strengthen these points usually involve combinations of firewalls, web proxies, intrusion prevention and virtual private networks. SecurityCenter CV can help aggregate the various logs generated by these different devices and provide a common report about which assets are accessing the SCADA network.

4. Harden SCADA networks by removing or disabling unnecessary services

SecurityCenter CV can manage multiple PVS and Nessus instances. The data collected by each of these technologies can be used to build different types of asset lists. These lists can then be analyzed for common services and devices running additional services can be highlighted for analysis. Also, devices not part of any particular business asset may also not be needed anymore and can be identified for removal.

5. Do not rely on proprietary protocols to protect your system

SecurityCenter CV can be used to identify several SCADA clients and servers. The protocols for SCADA devices have been published in several different computer security venues and more information is being disclosed as time goes on.

With Tenable's solutions, a security manager for a SCADA network can easily discover all of their active SCADA devices and identify when new devices are added.

6. Implement the security features provided by device and system vendors

Many core operating systems and network devices include fairly good auditing, securing and logging options. SecurityCenter CV can be used to log in to these devices and ensure that basic security parameters have been enabled. Tenable calls these checks compliance checks.

Tenable has many customers who use these checks to ensure their devices are configured according to a corporate policy. For example, all event logging should be enabled on all Windows servers and all passwords should be changed every 30 days. Policies to take advantage of the basic security features of underlying operating systems can be used to harden SCADA networks.

7. Establish strong controls over any medium that is used as a backdoor into the SCADA network

The compliance checks alluded to in the previous step can be used to ensure that servers have been locked down. Modern operating systems can be configured such that non-admin users do not have access to insert CDs, USB drives or other peripherals.

8. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring

SecurityCenter CV can correlate events from a wide variety of IDS. The correlation includes real-time vulnerability to event correlation, such that only IDS events that target vulnerable servers are alerted on.

It also includes per-asset analysis such that all IDS events going to or from a particular asset group are considered. This makes analysis of any threat to a specific SCADA network much easier.

In addition, the LCE component of SecurityCenter CV can also accept logs from many different IDS as well as other sources of data including NetFlow, network monitoring, firewall logs and application logs. SecurityCenter CV can also perform anomaly detection on the logs and search for changes in behavior that traditional IDS may miss.

9. Perform technical audits of SCADA devices and networks and any other connected networks to identify security concerns

SecurityCenter CV can use Nessus and PVS to identify a wide variety of security concerns in any network that connects to the SCADA network.

For the actual SCADA devices themselves, the ideal method to discover them without any impact to operations is to monitor the network with the PVS component of SecurityCenter CV. This allows 24x7 continuous discovery of current and new SCADA devices.

Once these devices are discovered, a manual analysis of their configuration can be used, or if the devices are modern, a direct vulnerability assessment can be launched with Nessus. These assessments include several dozen SCADA-specific checks written for Tenable by Digital Bond.

10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security

Although SecurityCenter CV and each of its managed components do not specifically perform physical inspections, it can gather a great deal of information that can make a physical inspection much easier. For example, SecurityCenter CV can provide the following information for assessors:

- Internet and intranet traffic usage
- Which computers are managed (part of a domain) and which may have been part of the network unchanged for years
- A good idea of the usernames, accounts and frequency of use of various administrator and end user activity
- The operating system and running applications of all active hosts on a remote network
- If the remote network is a source of network attacks, malware outbreaks or unauthorized activity such as P2P file sharing

In addition to gathering such useful knowledge, SecurityCenter CV can also be used to gather logs from a variety of physical access control devices.

11. Establish SCADA Red Teams to identify and evaluate possible attack scenarios

For an existing Red Team, having the knowledge of what actually is in use on the network can help them identify more realistic attack scenarios. SecurityCenter CV can be used to gather intelligence about a remote network prior to physical inspection. Those same methods can be applied to gather information about the entire network. For example, SecurityCenter CV can provide the following information a Red Team:

- The frequency devices are patched or upgraded
- What ports firewalls are allowing though
- Trust relationships between separate asset groups
- Where attackers may have broken out inside or outside the SCADA network
- A list of all software in use on the network
- Which computers are used for administration

12. Clearly define cyber security roles, responsibilities and authorities for managers, system administrators and users

SecurityCenter CV is ideally suited to provide the correct level of access to vulnerability, log, compliance, risk and patching information. Almost any hierarchy of security roles and responsibilities can be configured to ensure the right level of attention, reporting and monitoring is given to security issues.

13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection

Through active and passive analysis, SecurityCenter CV can be used to identify the network architecture. The combination of groups of like devices into business-level assets as well as knowing how the network is connected makes SecurityCenter CV ideal for disseminating this information.

In addition, once critical assets are either discovered or manually added into SecurityCenter, they can be monitored at a closer level. For example, SecurityCenter CV can be used to identify all computers as a control center for a coal burning power plant. Any changes to these devices or new types of security threats and vulnerabilities can be highlighted specifically for the control center.

14. Establish a rigorous, ongoing risk management process

A key element of risk management is to monitor the network for new vulnerabilities or evidence of intrusions. SecurityCenter CV is ideally suited to gather this sort of information and produce asset based risk management reports.

Once the various types of assets are added into SecurityCenter CV, many different types of assets can be reported on. For example, one view can show how all physical buildings as part of a SCADA network compare against each other. Another view can highlight how various devices such as desktops, SCADA clients and servers compare. SecurityCenter CV can present this trend data in such a way that small changes can be used to identify increased risk to key assets.

15. Establish a network protection strategy based on the principle of defense-in-depth

When deploying defense in depth, most solutions will employ different types of security and access control technology. SecurityCenter CV and its LCE component are ideally suited to gather logs from many different devices and report on how that information affects each asset.

16. Clearly identify cyber security requirements

For organizations that have outlined their specific cyber-security requirements, solutions from Tenable can be used to implement a variety of policies. Tenable has helped customers implement a wide variety of programs that reflected an organization’s overall desire for a uniform security policy. At a high level, Tenable’s products can help identify:

- Unauthorized devices, applications and networks
- Network activity that is harmful
- Unauthorized information access
- Devices that are not configured to a gold standard

17. Establish effective configuration management processes

SecurityCenter CV can be used to log into a variety of systems to audit their configuration. Tenable includes many of these audits out of the box with SecurityCenter CV, but they are also flexible enough to create new policies particular to any organization’s needs. Non-compliant devices can have their specific configuration issues reported on.

For general network configuration management, SecurityCenter CV and its Nessus component can be used to detect network and host changes such as new hosts, new applications and new vulnerabilities.

18. Conduct routine self-assessments

As with step 11 and 14, organizations that have SecurityCenter CV deployed can perform a wide variety of routine self-assessments. These include:

- Identification of all new devices and applications

- Performing patch audits of all operating systems
- Identifying changes in communication behavior of SCADA networks
- Identifying new trust relationships between various asset groups

19. Establish system backups and disaster recovery plans

SecurityCenter CV can be used to ensure that systems are configured correctly to participate in backup and fail-over operations. Any type of data storage or fail-over technologies will also need their vulnerabilities and security events managed. SecurityCenter CV can accomplish this with existing technologies.

20. Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance

SecurityCenter CV can be used to display a variety of security data. The data can be presented by business unit, technology, physical locations, protocols and more. By using SecurityCenter CV to distill information out of raw security data, senior management can be better informed about what is occurring on their SCADA networks.

21. Establish policies and conduct training to minimize the likelihood that organizational personal will inadvertently disclose sensitive information regarding SCADA systems design, operations or security controls

Tenable has made partnerships with companies that can monitor communications for sensitive information. Monitored devices can be configured to detect when inappropriate communications containing human resources, customer data, SCADA configuration information, etc. has been sent outside of the network. SecurityCenter CV can correlate these events with known asset groups or intrusion detection events.

VI. Conclusion

Tenable Network Security is ready to help answer any of your questions regarding your specific SCADA security concerns. Our solutions offer a very robust and accurate way to discover and report all security issues on your SCADA network, without any adverse effects.

VII. About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.