Meeting CJIS & FTI Compliance with Tenable

Continuous monitoring helps state and local government agencies discover, assess, report, and take action to manage risk and ensure compliance

Key Challenges

State and local government agencies face a constantly changing compliance landscape. Tenable's SecurityCenter Continuous View™ (SC® CV™) can help agencies fulfill requirements for meeting and demonstrating compliance with multiple standards, including the Criminal Justice Information Services (CJIS) Security Policy and IRS Publication 1075 – Tax Information Security Guidelines for Federal, State, and Local Agencies (FTI).

The CJIS policy was designed to provide a base-level security policy for all entities that have access to Criminal Justice Information (CJI). The policy outlines roles and responsibilities for organizations, proper handling of CJI, and the implementation of both technical and physical security policies. IRS Publication 1075 is largely based on NIST Special Publication 800-53, but with special considerations for additional sensitive information. IRS Publication 1075 provides thorough guidance for organizations that deal with Federal Taxpayer Information (FTI). Many agencies are required to meet the CJIS and/or FTI standards in order to handle sensitive information, so agencies need to take a comprehensive approach to securing this information.

Agencies face CJIS and FTI compliance challenges, such as:

- Detecting and reporting on unlawful, unauthorized, or inappropriate information system activity
- Tracing back an individual user's activity
- Limiting information system access to authorized users, processes of those users, and devices
- Identifying users, processes acting on behalf of users, or devices, and then authenticating their identities before allowing access
- Enforcing security configuration settings for information technology products
- Maintaining plans for emergency response, backup operations, and disaster recovery for organizational information systems
- Verifying that compliance has not been compromised after maintenance is done

Arm your agency with full network awareness that provides the information needed to take action in managing risk and ensuring compliance with the CJIS and FTI standards.

Where Tenable Can Help

SecurityCenter CV provides proactive continuous monitoring across the organization to help an agency respond to existing CJIS and FTI compliance requirements, as well as prepare for any requirement changes that may arise. SC CV assists with discovery, assessment, reporting, and responding to information about the network, providing vulnerability, risk, and compliance summaries and enabling agencies to easily meet many of the technical requirements for the CJIS and FTI standards.

Auditing & Accountability

The CJIS Security Policy specifies that organizations must create, protect, and keep information system (IS) audit records to enable the monitoring, analysis, investigation, and reporting of improper IS activity, and ensure that the actions of individual IS users can be traced back to those users. SC CV displays a pie chart of compliance checks related to an organization's auditing and accountability.

Access Control

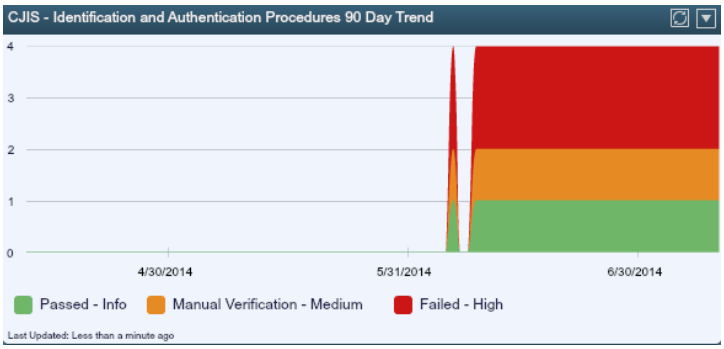
The CJIS policy requires that organizations limit IS access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), as well as to the types of transactions and functions that authorized users are permitted to exercise. SC CV displays a chart of compliance checks related to an organization's access control.

Key Advantages

- Identify the biggest security risk across your entire organization
- Receive alerts of threats on your network, in real time
- Isolate misconfigurations among managed assets
- Identify non-managed applications or systems
- View at-a-glance status of compliance checks with dashboards and reports
- Have the means to assess the severity of the above situations
- Communicate any issues found by SC CV via SMS or email

Identification & Authentication Controls

The CJIS Security Policy specifies that organizations must identify IS users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. SC CV displays an area trend chart of compliance checks related to an organization's identification and authentication controls. In the chart, green indicates that checks pass an audit of the control area, red indicates the checks that have failed a compliance audit, and orange indicates the checks that will require manual verification of the status of the audit check.



Configuration Management

The CJIS policy requires that organizations establish and maintain baseline configurations and inventories of organizational information systems, and establish and enforce security configuration settings for information technology products employed in organizational information systems. SC CV displays a table of hosts that have been checked for NIST compliance checks related to an organization's configuration management. The table displays the IP address, FQDN, and compliance check summaries.

Contingency Planning

NIST guidelines specify that organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations. SC CV displays a table of hosts that have been checked for NIST compliance checks related to an organization's contingency planning. The table displays the IP address, FQDN, and compliance check summaries.

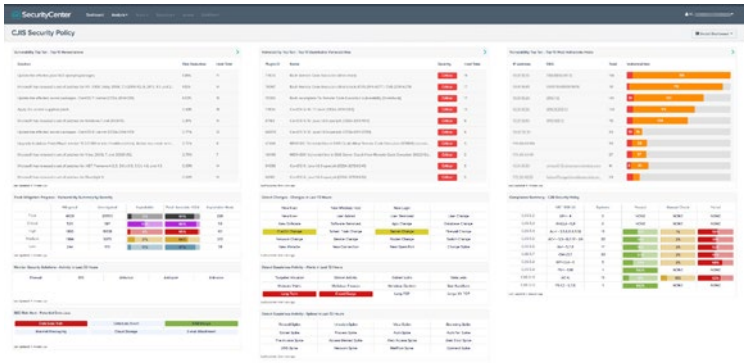
Maintenance

SC CV provides a ratio view of systems that have been checked for a variety of compliance standards. The ratio bar provides a visual of the number of compliance checks that have either passed, failed, or that require some manual verification. This component of SC CV can be used to verify compliance and configurations on systems that will be undergoing maintenance and then can be used to evaluate these systems after maintenance has finished verifying that compliance has not been compromised.

Dashboards & Reports

Tenable has created SecurityCenter dashboards and reports specifically designed to assist organizations with CJIS and FTI compliance. The dashboards display top vulnerabilities, suspicious activity or changes to the network, and a summary of an organization's CJIS or FTI compliance. The reports package the dashboard information so it can be easily distributed for analysis. Dashboards and reports include:

- CJIS Security Policy dashboard
- CJIS Security Policy report
- FTI Security Guidelines dashboard
- FTI Security Guidelines report



Take the Next Step

SecurityCenter Continuous View arms an agency with full network awareness, providing the information needed for managing risk and ensuring compliance with the CJIS and FTI standards. In addition to providing real-time threat detection, SC CV isolates misconfigurations among managed assets, identifies non-managed applications or systems, and delivers at-a-glance information through dashboards and reports. These capabilities give agencies the means to continually assess the severity of security risk, and communicate with these findings via SMS or email to prompt rapid response.

For a full listing of the CJIS and FTI requirements that Tenable can help organizations meet when using SC CV, see the appendix in the "Analysis and Compliance to Meet CJIS and FTI Security Standards" whitepaper. Please contact us if you have questions or need assistance.

tenable network security

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact