tenable™

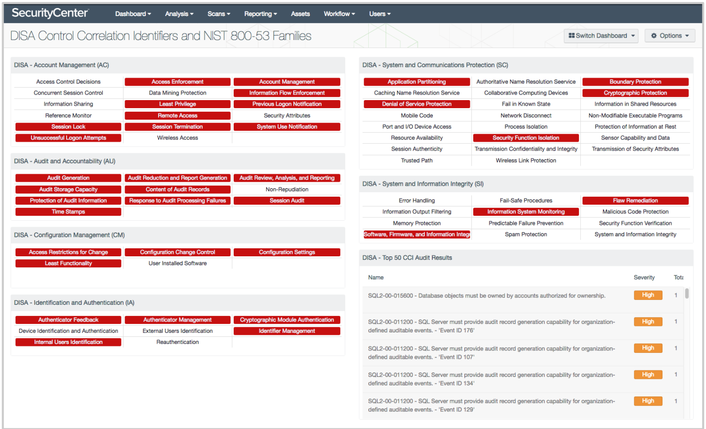
Solutions for
Special Access Programs (SAPs)

Protecting DoD Special Access Program Sensitive Information

Special Access Programs (SAPs) represent some of the Department of Defense's (DoD) most sensitive information, and therefore, must be protected accordingly. Reliance upon physical isolation as a primary risk mitigation strategy is no longer sufficient. Threats and risks often outpace the ability to implement robust, multidisciplinary countermeasures. Additionally, costs and timelines to develop new attacks typically pale in comparison to the costs and effort required to implement counter measures.

Joint Special Access Program Implementation Guide (JSIG) Provides Policy, Procedures and Implementation Guidance

The Joint Special Access Program Implementation Guide (JSIG) serves as a technical supplement to NIST SP 800-53 and CNSSI 1253, and is used in concert with the applicable volume of DoDM 5205.07 in the application of the Risk Management Framework (RMF). JSIG provides standardized cybersecurity/information assurance-related policy, procedures and implementation guidance for managing all networks, systems and system components at all classification levels under the purview of the cognizant SAP Authorizing Official (AO).



DISA Control Correlation Identifiers and NIST 800-53 Families

DISA - Account Management (AC)

Access Control Decisions	Access Enforcement	Account Management
Concurrent Session Control	Data Mining Protection	Information Flow Enforcement
Information Sharing	Least Privilege	Previous Logon Notification
Reference Monitor	Remote Access	Security Attributes
Session Lock	Session Termination	System Use Notification
Unsuccessful Logon Attempts	Wireless Access	

DISA - Audit and Accountability (AU)

Audit Generation	Audit Reduction and Report Generation	Audit Review, Analysis, and Reporting
Audit Storage Capacity	Content of Audit Records	Non-Repudiation
Protection of Audit Information	Response to Audit Processing Failures	Session Audit
Time Stamps		

DISA - Configuration Management (CM)

Access Restrictions for Change	Configuration Change Control	Configuration Settings
Least Functionality	User Installed Software	

DISA - Identification and Authentication (IA)

Authenticator Feedback	Authenticator Management	Cryptographic Module Authentication
Device Identification and Authentication	External Users Identification	Identifier Management
Internal Users Identification	Reauthentication	

DISA - System and Communications Protection (SC)

Application Partitioning	Authoritative Name Resolution Seervice	Boundary Protection
Caching Name Resolution Service	Collaborative Computing Devices	Cryptographic Protection
Denial of Service Protection	Fail in Known State	Information in Shared Resources
Mobile Code	Network Disconnect	Non-Modifiable Executable Programs
Port and I/O Device Access	Process Isolation	Protection of Information at Rest
Resource Availability	Security Function Isolation	Sensor Capability and Data
Session Authenticity	Transmission Confidentiality and Integrity	Transmission of Security Attributes
Trusted Path	Wireless Link Protection	

DISA - System and Information Integrity (SI)

Error Handling	Fail-Safe Procedures	Flaw Remediation
Information Output Filtering	Information System Monitoring	Malicious Code Protection
Memory Protection	Predictable Failure Prevention	Security Function Verification
Software, Firmware, and Information Integ	Spam Protection	System and Information Integrity

DISA - Top 50 CCI Audit Results

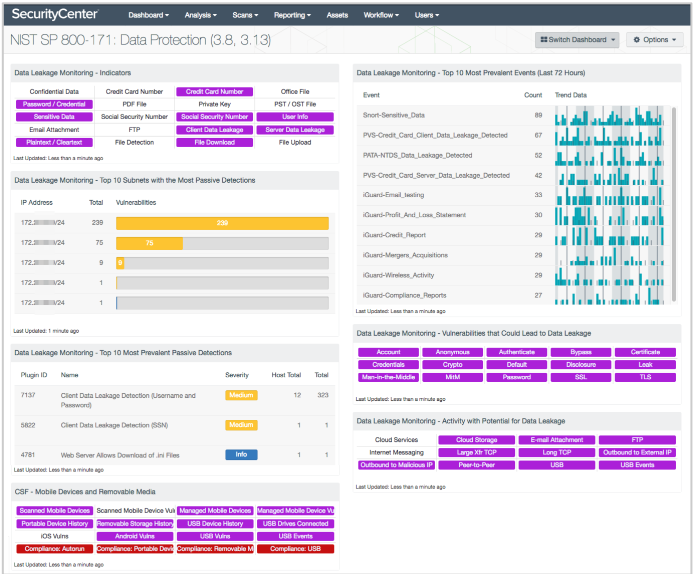
Name	Severity	Tota
SQL2-00-015600 - Database objects must be owned by accounts authorized for ownership.	High	1
SQL2-00-011200 - SQL Server must provide audit record generation capability for organization-defined auditable events. - 'Event ID 176'	High	1
SQL2-00-011200 - SQL Server must provide audit record generation capability for organization-defined auditable events. - 'Event ID 107'	High	1
SQL2-00-011200 - SQL Server must provide audit record generation capability for organization-defined auditable events. - 'Event ID 134'	High	1
SQL2-00-011200 - SQL Server must provide audit record generation capability for organization-defined auditable events. - 'Event ID 129'	High	1

Further, the Joint SAP Cybersecurity Working Group (JSCS WG) was established to provide DoD SAP cybersecurity implementation guidance. One key function of the JSCS WG is to promote DoD SAP Community coordination in methodologies for assessing and authorizing SAP information systems and related areas (e.g., documentation, tools, assessment methods and processes).

Tenable Solution Delivers Situational Awareness and Adherence to JSIG Security Controls

SecurityCenter Continuous View® (SecurityCenter CV™) from Tenable is an out-of-the-box solution uniquely positioned to assist in delivering situational awareness to SAP information systems, thus enabling consistency in the measurement, visualization and communication adherence to JSIG security controls. SecurityCenter CV automates the assessment of technical controls from ISO/IEC 27001/27002, the NIST Cybersecurity Framework, JSIG, NIST SP 800-171 and CIS Critical Security Controls to ensure they are in place and operating effectively.

SecurityCenter CV fits JSIG specific needs by supporting "air-gapped" networks, as well as larger enterprise networks. It delivers broad and continuous coverage across physical, virtual, cloud and mobile devices used in IT and industrial control networks. Dynamic asset lists enable you to logically segment, manage and report on the status of specific systems. Intelligent connectors to existing IT and security products audit configurations and analyze events to identify control weaknesses.



NIST SP 800-171: Data Protection (3.8, 3.13)

Data Leakage Monitoring - Indicators

Confidential Data	Credit Card Number	Credit Card Number	Office File
Password / Credential	PDF File	Private Key	PST / OST File
Sensitive Data	Social Security Number	Social Security Number	User Info
Email Attachment	FTP	Client Data Leakage	Server Data Leakage
Plaintext / Cleartext	File Detection	File Download	File Upload

Last Updated: Less than a minute ago

Data Leakage Monitoring - Top 10 Subnets with the Most Passive Detections

IP Address	Total	Vulnerabilities
172.[redacted]/24	239	239
172.[redacted]/24	75	75
172.[redacted]/24	9	9
172.[redacted]/24	1	
172.[redacted]/24	1	

Last Updated: 1 minute ago

Data Leakage Monitoring - Top 10 Most Prevalent Passive Detections

Plugin ID	Name	Severity	Host Total	Total
7137	Client Data Leakage Detection (Username and Password)	Medium	12	323
5822	Client Data Leakage Detection (SSN)	Medium	1	1
4781	Web Server Allows Download of .ini Files	Info	1	1

Last Updated: Less than a minute ago

CSF - Mobile Devices and Removable Media

Scanned Mobile Devices	Scanned Mobile Device Vul	Managed Mobile Devices	Managed Mobile Device Vu
Portable Device History	Removable Storage History	USB Device History	USB Drives Connected
iOS Vulns	Android Vulns	USB Vulns	USB Events
Compliance: Autorun	Compliance: Portable Devic	Compliance: Removable M	Compliance: USB

Last Updated: Less than a minute ago

Data Leakage Monitoring - Top 10 Most Prevalent Events (Last 72 Hours)

Event	Count	Trend Data
Snort-Sensitive_Data	89	
PVS-Credit_Card_Client_Data_Leakage_Detected	67	
PATA-NTDS_Data_Leakage_Detected	52	
PVS-Credit_Card_Server_Data_Leakage_Detected	42	
iGuard-Email_testing	33	
iGuard-Profit_And_Loss_Statement	30	
iGuard-Credit_Report	29	
iGuard-Mergers_Acquisitions	29	
iGuard-Wireless_Activity	29	
iGuard-Compliance_Reports	27	

Last Updated: Less than a minute ago

Data Leakage Monitoring - Vulnerabilities that Could Lead to Data Leakage

Account	Anonymous	Authenticate	Bypass	Certificate
Credentials	Crypto	Default	Disclosure	Leak
Man-in-the-Middle	MitM	Password	SSL	TLS

Last Updated: Less than a minute ago

Data Leakage Monitoring - Activity with Potential for Data Leakage

Cloud Services	Cloud Storage	E-mail Attachment	FTP
Internet Messaging	Large Xfr TCP	Long TCP	Outbound to External IP
Outbound to Malicious IP	Peer-to-Peer	USB	USB Events

Last Updated: Less than a minute ago

SecurityCenter CV Provides Ability to Communicate Security Status

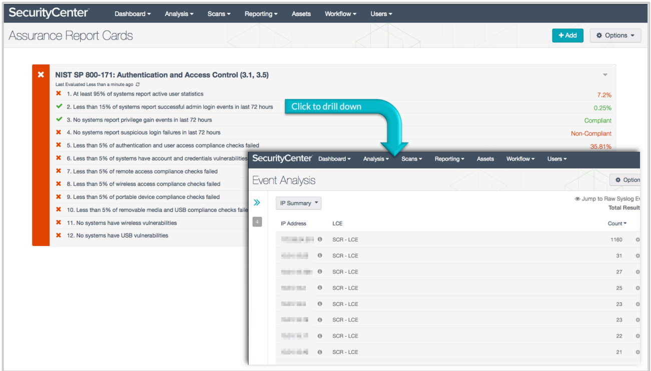
SecurityCenter CV provides fully customizable reports, dashboards and Assurance Report Cards® (ARCs) specific to the leading security frameworks – all out of the box. You can use them "as-is" or easily tailor them to meet your specific security and mission needs. For example, you can easily create specific reports, dashboards and ARCs for individual SAP Programs information systems, as applicable.

The data that SecurityCenter CV gathers and analyzes for security frameworks is often the same data you need for compliance reporting. You can use compliance report templates to present the data in the formats required by multiple compliance standards. As a result, redundant controls are eliminated, and the work required by each audit is reduced.

Tenable reports, dashboards and Assurance Report Cards demonstrate adherence with best practice security controls to external mission partners, as well as large customers that may have the right to audit your security program.

ARCs complement the comprehensive Tenable data collection approach, which uses a combination of active scanning, agent scanning, intelligent connectors to your third-party systems, passive listening and host data monitoring to assess the security posture of your complete infrastructure. Together, these capabilities enable you to:

- Measure, visualize and effectively communicate the technical security controls that help you manage risk
- Communicate security status to internal and external stakeholders
- Understand the context you need to prioritize remediation



Assurance Report Cards

NIST SP 800-171: Authentication and Access Control (3.1, 3.5)

Last Evaluated Less than a minute ago

✗	1. At least 95% of systems report active user statistics	7.2%
✓	2. Less than 15% of systems report successful admin login events in last 72 hours	0.25%
✓	3. No systems report privilege gain events in last 72 hours	Compliant
✗	4. No systems report suspicious login failures in last 72 hours	Non-Compliant
✗	5. Less than 5% of authentication and user access compliance checks failed	35.81%
✗	6. Less than 5% of systems have account and credentials vulnerabilities	
✗	7. Less than 5% of remote access compliance checks failed	
✗	8. Less than 5% of wireless access compliance checks failed	
✗	9. Less than 5% of portable device compliance checks failed	
✗	10. Less than 5% of removable media and USB compliance checks faile	
✗	11. No systems have wireless vulnerabilities	
✗	12. No systems have USB vulnerabilities	

Event Analysis

Total Result

IP Address	LCE	Count
[redacted]	SCR - LCE	1160
[redacted]	SCR - LCE	31
[redacted]	SCR - LCE	27
[redacted]	SCR - LCE	25
[redacted]	SCR - LCE	23
[redacted]	SCR - LCE	23
[redacted]	SCR - LCE	22
[redacted]	SCR - LCE	21

About Tenable

Tenable 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 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses 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.

For more information, visit tenable.com or contact federalsales@tenable.com for a demo.

tenable™