Maximize Outcomes for CDM and Much More with SecurityCenter™ Continuous View

You have to comply with CDM. With Tenable you can do more.

As federal cybersecurity programs have matured, agencies have moved from periodic assessment of static security controls to continuous monitoring of IT resources and activities. The Department of Homeland Security supports this evolution through the Continuous Diagnostics and Mitigation (CDM) program, which offers a collection of commercial off-the-shelf products to give agencies real-time visibility into networks and systems. CDM is a risk-based approach to government cybersecurity, intended to "provide federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impact, and enable cybersecurity personnel to mitigate the most significant problems first."

Tenable SecurityCenter™ Continuous View (SecurityCenter CV™), already the standard for public sector continous monitoring, now sets the standard for CDM. This solution combines end-to-end visibility with the critical context needed to support real-time risk-based decisions, giving agencies and organizations the agility to continuously enhance their security operations to stay ahead of threats. SecurityCenter CV is widely used and has a solid track record in government departments and agencies, including deployments within the Department of Defense and the National Institutes of Health. Its ability to provide advanced analysis of vulnerability and threat data, network traffic and event information from across an enterprise, including connected devices and ICS/SCADA equipment, also makes it the best solution for meeting CDM requirements. SecurityCenter CV enables you to easily know what and who is on your network, a critical building block for robust risk management.

Your CDM solution should not be a burden on the mission or the enterprise. It should increase security analyst efficiency and reduce operational overhead while delivering on requirements. Simply scanning only gets you so far. SecurityCenter CV takes you further. Only SecurityCenter CV delivers the breadth of functionality, combined with the best interoperability support on CDM, to enable you to not only see, but also understand, what is happening on your network. Single solutions give you data in silos. Tenable gives you centralized visibility and context to answer important security questions.

Key Benefits

Tenable SecurityCenter CV complies with CDM Phase 1 requirements, enabling you to know the desired state of your network security, know the actual state and identify the differences.

Know the desired state	SecurityCenter CV tracks changes in the authorized security configuration baseline. Vulnerabilities are detected and documented through active and passive scanning, passive listening and log analysis, and directions for remediation are provided.
Know the actual state	SecurityCenter CV assesses configurations on an agency-defined schedule and on an ad hoc basis, supporting a wide range of checks within a 72-hour window. It can return actual values, rather than simple pass-fail results. Vulnerabilities and weaknesses are discovered and mapped to authorized hardware and software assets.
Know and automatically act on differences between the desired and actual state	SecurityCenter CV enumerates deviations from the authorized configuration benchmark, including deviations that can provide increased protection. Deviations can be visualized from an enterprise level down to the individual user, and business rules are applied to provide accountability for the persons responsible for addressing deviations. Configuration assessments are stored to allow security posture reporting.

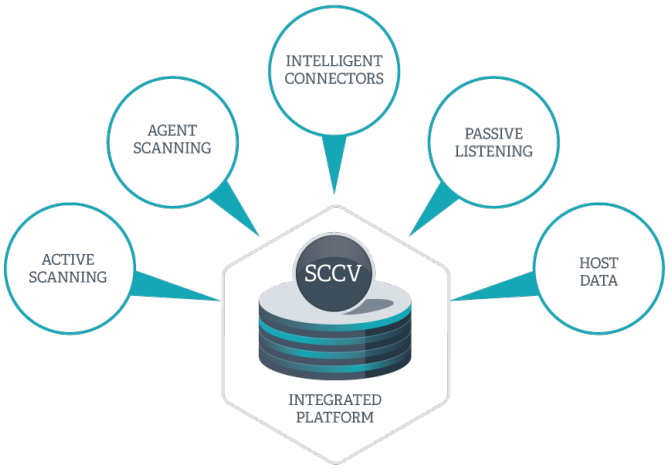
Proven Performance

SecurityCenter has demonstrated its past performance in programs of similar size, scope and complexit. For example, in the Department of Defense Assured Computing Assessment Solution (ACAS), Tenable delivers the technology solution that powers the ACAS Program. ACAS enables DoD elements to assess their networks and connected IT systems against department standards. Tenable leverages the same capabilities that are powering ACAS to support CDM, enabling you to prioritize and act on information to neutralize or mitigate threats across the enterprise.

Uniquely Tenable

Our Sensors

Tenable constantly analyzes information from our unique sensors, delivering continuous visibility and critical context, enabling decisive action that transforms your security program from reactive to proactive. Because Tenable integrates with existing infrastructure, it helps you to fully leverage your cybersecurity investments to realize the greatest return. The ability to see and to analyze data from all sources, including connected devices and non-traditional IT systems such as ICS/SCADA, creates the intelligence needed to counter sophisticated threats in a rapidly evolving landscape.



- **Active Scanning** - Periodically examine assets to determine their level of risk to the organization
- **Agent Scanning** – Rapidly audit assets without the need for credentials and capture transient assets that are frequently offline
- **Intelligent Connectors** – Leverage existing security investments and integrate security data from multiple sources to improve context and analysis
- **Passive Listening** – Monitor in real time to gather information on which assets are connected to the network and how they are communicating
- **Host Data** – Actively monitor host activities and events, including who is accessing them and what is changing to identify malicious activity and anomalous behavior

No Silos. Better Efficiency.

The traditional approach to solving security challenges is to deploy a purpose built tool, and in many cases that does the job. But in order to "identify cybersecurity risks on an ongoing basis and prioritize these risks based upon potential impact," as the CDM requires, silos of information are not helpful. The task requires a solution that can collect and analyze data from multiple sources in order to truly get the view you need of your hardware, software, vulnerabilities, threats and more. Tenable already delivers the richest set of data available. And by leveraging our open APIs and Log Correlation Engine (LCE), we also work with an entire ecosystem of third parties to expand that data set even further.

In addition, by automating and centralizing this data in one location, you gain not only better visibility and context, but you also reduce operational overhead by increasing security analyst efficiency and empowering them to answer important security questions quickly and proficiently. There is no other solution on CDM that can provide network visibility, network health and welfare, proactive vulnerability management, log management and so much more.

Key Features

- **Continuous asset discovery and network health monitoring** provides a complete picture of your network's status and identifies suspicious activity.
- **Real-time malware detection** leverages threat intelligence feeds that are built into the Tenable solution.
- **Anomaly detection** uses statistical analysis of external log sources to discover activity that deviates from the norm.
- **Customizable dashboards and reports** with a simple user interface to meet the needs of all stakeholders. This includes the industry's first Assurance Report Cards to measure effectiveness and identify gaps.
- **Advanced analytics and trending** provides contextual insight and actionable information, enabling rapid incident response with notification through a variety of media.
- **Unified reporting** of configuration, vulnerabilities, threats, and events allow you to measure security status and provide streamlined compliance with CDM, as well as other federal regulatory requirements.

tenable® network security

For More Information: Please visit tenable.com