ACAS, POWERED BY TENABLE®
ACHIEVE AND EXCEED DOD COMPLIANCE

Over the past few years, the sophistication and frequency of cyberattacks has increased exponentially. In parallel, the evolution of the IT landscape has exploded to include much more than physical and virtual machines, and the landscape continues to transform. As more assets, systems, devices and users come online, more complexity, uncertainty and reactive security are sure to follow. Poor visibility into the IT environment, data overload and a lack of effective communications put your missions at risk.

To address these challenges, in 2012, the Defense Information Systems Agency (DISA) awarded the Assured Compliance Assessment Solution (ACAS) contract to HP Enterprise Services (now Perspecta) and Tenable®. The ACAS mission is simple: Assess DoD enterprise networks and connected IT systems against DoD standards, as well as identify any known system vulnerabilities.

With ACAS and Tenable, you can both meet and exceed DoD compliance while also participating the Cyber Exposure revolution. As the network and threats to it grow, Tenable solutions grow in parallel, enabling you to anticipate, prioritize and neutralize threats across any infrastructure, any device and at any time – helping you know and respond to your Cyber Exposure. It’s that powerful.

THE TENABLE ACAS SOLUTION

ACAS provides complete visibility and prioritized, actionable data through customized reporting. Recently, new capabilities were added to the ACAS contract with the addition of Nessus® Agents and LCE® (Log Correlation Engine), supporting even more compliance capabilities at no further cost to the government.

The solution today includes the following IT security platform necessities: Tenable.sc™ (formerly SecurityCenter®) for on-prem Vulnerability Management, Nessus® scanners controlled by Tenable.sc, Nessus Network Monitor® (formerly Passive Vulnerability Scanner® or PVS), Nessus® Agents, and LCE® (Log Correlation Engine). The Tenable solution is Security Content Automation Protocol (SCAP) 1.2 compliant and provides advanced capability to configuration compliance and auditing.

Information on additional solution components and enhancements can be found at https://www.ask-acas.info/

SOLUTION COMPONENT

<table>
<thead>
<tr>
<th>Solution Component</th>
<th>ACAS Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.sc™ (formerly SecurityCenter) – now with LCE</td>
<td>YES</td>
</tr>
<tr>
<td>Nessus® (scanners controlled by Tenable.sc)</td>
<td>YES</td>
</tr>
<tr>
<td>Nessus Network Monitor® 1GB</td>
<td>YES</td>
</tr>
<tr>
<td>Tenable Research Team</td>
<td>YES</td>
</tr>
<tr>
<td>Nessus Agents</td>
<td>YES</td>
</tr>
</tbody>
</table>

SOLUTION COMPONENT

<table>
<thead>
<tr>
<th>Beyond ACAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable Industrial Security</td>
</tr>
<tr>
<td>Nessus Network Monitor 10GB</td>
</tr>
</tbody>
</table>

KEY BENEFITS

With ACAS and Tenable.sc, you have the resources needed to harness the IT security transformation and meet and exceed DoD compliance.

- Complete Vision: The most comprehensive view of deployed assets and potential weaknesses in the IT environment
- Situational Awareness: Contextual insight and actionable intelligence so you can prioritize targets and destroy threats
- Fast Communications: Share customized reports, statuses, assessments and discoveries easily and quickly
- Risk Measurement: Measure risk against mission objectives with powerful reporting for total operational excellence
- Continuous Compliance: Know the network you’re responsible for, achieve DoD compliance and then exceed it.

TENABLE.SC: ANTICIPATE, PRIORITIZE AND CLOSE THE CYBER EXPOSURE GAP

The Tenable.sc platform provides the most comprehensive and integrated view of security posture to reduce risk and exceed DoD compliance. This next generation vulnerability analytics component for ACAS includes: Assurance Report Cards, Advanced Analytics/Trending, Customizable Dashboards/Reports and Cumulative Scan Results.
UNDERSTANDING CYBER EXPOSURE WITH TENABLE.SC

Cyber Exposure is an emerging discipline for managing and measuring cybersecurity risk in the digital era. Cyber Exposure transforms security from static and siloed visibility into cyber risk to dynamic and holistic visibility across the modern attack surface. Cyber Exposure translates raw vulnerability data into business insights to help security teams prioritize and focus remediation based on business risk. Just as other functions have a system of record, including ITSM for IT and CRM for Sales, Cyber Exposure solutions will provide Security with a system of record to help them effectively manage and measure cyber risk.

Tenable.sc is the on-prem solution that brings together unique sensors for vulnerability management, all of which are now available to the DoD as part of ACAS. Starting with active scanning (Nessus), passive network monitoring (Nessus Network Monitor), Agent scanning and event data (LCE), unit commanders are able to visualize up-to-date vulnerability and threat intelligence information. With Tenable.sc, you have even more power to continuously discover all assets, identify all vulnerabilities, monitor all networks in real time for advanced threats, gather contextual insight to rapidly respond to security breaches and ensure compliance.

NESSUS AGENTS: CLOSE THE CYBER EXPOSURE GAP

The ACAS solution now includes Nessus Agents which enables you to deploy clients across the enterprise, extending the coverage for the DoD mandated vulnerability scanning, assessment and management capabilities. Nessus Agents close the gap in reporting for assets on the move or removes the requirements for credential management. Nessus Manager collects the Agent vulnerability data and reports back to Tenable.sc’s advanced vulnerability analytics engine. Tenable.sc retrieves agent results, and correlated the data so you can accurately assess risk and prioritize remediation workflows.

Nessus Agents used via Tenable.sc enable you and your teams to achieve:
- Effective resource allocation to improve efficiency
- Expanded scan coverage across the entire IT environment
- Improved risk analysis by integrating context from existing infrastructures and partner framework

NESSUS NETWORK MONITOR: MODERN VIEW FOR THE MODERN CYBER SECURITY PROFESSIONAL

Periodic scanning is no longer an acceptable IT security defense tactic given the nature and proliferation of threats. Point in time scanning leads to uncertainty and gaps in coverage, which is the Cyber Exposure Gap. Tenable Nessus Network Monitor (NNM) exposes these problems by delivering real-time asset discovery and network monitoring for continuous scanning and assessment of DoD enterprise-level networks. NNM is a critical element to effectively creating and managing a more modern view of the IT infrastructure you’re tasked with defending. Information on additional solution components and enhancements can be found at https://www.ask-acas.info/

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