



United States Army Trusts eIQnetworks' SecureVue to Combat Key Security and Compliance Challenges

Case Study

SecureVue from eIQnetworks provides the US Army with a common operating picture (COP) of their global environment through a combination of next-generation SIEM, DISA STIG assessment, forensic analysis, and a true situational awareness.

"SecureVue provides a number of critical security and compliance capabilities in a single information platform."

-Brian Crawford, former Deputy G5 US Army NETCOM/9th Signal Command

Challenge

U.S. Army installations and Network Operations and Security Centers (NOSCs) around the world encounter a variety of challenges related to security and compliance issues. Specifically, ensuring prescriptive, system-level compliance with DISA STIGs has been a significant challenge for the Army, since to date this has been largely a manual effort. Additionally, as required by FISMA, DIACAP and other mandates, installations are required to collect, store and review security log event information on a continuous basis. In Army installations, this is generally accomplished by a SIEM or log management solution, but unfortunately, many installations do not have this capability.

Army Network Enterprise Centers (NECs) and NOSCs utilize multiple tools to help with overall security and network operations. These tools do not "talk" to one another, each operating within its own silo and almost always within its own console. Each tool is generally managed by one of three teams – Server Operations, Network Operations or Information Assurance (IA). When a situation arises that requires the sharing of information between two or more teams, a manual request is required from one branch to another, typically an email or phone call – a resource intensive exchange.

Security alerts are triggered every day in the Army. NECs, Theater Network Operations Security Centers (TNOSCs), and Army Global Network Operations Security Center (AGNOSC) environments can trigger security alerts that affect the other organization and the root cause of these alerts must be identified to ensure that threats are mitigated quickly. NEC, TNOSC and AGNOSC security operations teams must be able to effectively conduct root cause analysis across all security data, using a single source of information and a single, comprehensive console; as importantly, TNOSC and AGNOSC operations personnel require theater-wide and global command-and-control views into security threats that provide a "roll-up" view of activity across multiple NEC environments.

Solution

SecureVue, the unified situational awareness platform from eIQnetworks, is being used today by multiple Army installations to meet these many challenges, while simultaneously reducing risk and improving overall security and compliance operations. As stated by, Brian Crawford former Deputy G5 of the US Army's NETCOM/9th Signal Command, "SecureVue provides a number of critical security and compliance capabilities in a single information platform."

SecureVue provides an in-depth view of an organization's security and compliance position via a single console through comprehensive, real-time security monitoring, compliance automation, configuration auditing and forensic analysis. With its intelligent security and industry-leading single management console approach, SecureVue reduces complexity and minimizes the effort and operational overhead required to manage security and compliance.

Benefits

- **Comprehensive DISA STIG Compliance.** In addition to taking hours to audit a server against a DISA STIG, a traditional manual STIG process only provides a point-in-time view of compliance and does not provide an ongoing assessment against relevant STIGs. Further, the use of "statistical" evaluation – selecting a subset of only a few representative systems to evaluate against the STIG – means that many potential vulnerabilities are not being discovered. SecureVue is "a unique solution," said Crawford, because "SecureVue has the ability to look at the configuration information of all assets, measuring compliance over time." SecureVue solves the problem of system configuration evaluation through the ability to look at the configuration information of all assets – servers, network and security devices, desktops, applications, databases and other systems and measure their compliance over time against either pre-defined baselines or against DISA STIGs. From a single, straightforward and easy to navigate console, SecureVue quickly and easily measures and

identifies an installation's level of compliance against a broad range of STIGs, the level of compliance of each asset, the specific controls with which an asset is not in compliance and which configuration changes are required to make a device STIG compliant.

“A unique solution, SecureVue has the ability to look at the configuration information of all assets, measuring compliance over time.”

“Prior to the Army’s implementation of SecureVue, assessing the state of security required individuals to access each tool and manually extrapolate pertinent data.”

- **Enhanced, Next-Generation SIEM.** Before deploying SecureVue, Army installations did not have the capability of collecting, storing and reviewing security log event information on a continuous basis, let alone the broader set of security data that is required for STIG compliance. Although log management and evaluation might have been deployed at the theater level, it generally stopped there. As a unified situational awareness platform, SecureVue provides a number of critical security and compliance capabilities into a single tool, including a next-generation SIEM capability that goes far beyond traditional event-based data by natively collecting, correlating and analyzing not only logs and other event-based information, but network traffic information (via netflow), asset and configuration data, performance metrics, file integrity data and removable media data. This enhanced, next-generation SIEM capability does not require the acquisition of a separate SIEM tool or a separate set of licenses.
- **Unified Situational Awareness.** "Prior to the Army's implementation of eIQnetworks' SecureVue, assessing the general state of security and network operations required individuals to access each tool and manually extrapolate the pertinent data," stated Crawford. The data had to then be manually correlated with one another to provide a "best guess" of information security threats and risks. This approach was extremely resource intensive, and lacked real-time visibility into operations – the hallmark of true situational awareness. SecureVue provides a true situational awareness capability to NECs and TNOSCs by not only collecting data pertinent to security and operations, but by providing real-time cross-correlation across many different types of information security data. This cross-correlation capability, unique among security monitoring platforms, provides immediate, real-time and fully actionable information, greatly reducing the time to discover the true root cause of issues and anomalies.
- **True Common Operating Picture (COP).** Manual exchange of information is resource intensive and slowed the ability of NECs, TNOSCs and the AGNOSC to respond to incidents. If there were a common operating picture that could be leveraged by each group simultaneously with each team utilizing the information appropriate to their role, installations could deliver real-time response across multiple teams using a single platform and alleviating time-consuming manual exchanges of information. SecureVue provides NECs with a true common operating picture (COP) at the installation level, and TNOSCs with a roll-up view of activity at the entire theater level, and the AGNOSC with complete, command-and-control visibility across the enterprise through a single tool that provides contextually-relevant information that is appropriate to their role within the organization. SecureVue allows people to access the information they need at a moment's notice without the constant back-and-forth manual communication, and ensures that day-to-day operations at the NEC, TNOSC and AGNOSC level are significantly more productive.
- **Comprehensive Forensic Analysis.** SecureVue's integrated ForensicVue component provides a comprehensive, Google-like search engine across all security and compliance data, not just events. ForensicVue allows NEC, TNOSC and AGNOSC security teams to drill-down into alerts and quickly correlate events with system configuration changes, network traffic patterns, user data and other non-event information, rapidly providing the information necessary to quickly eliminate threats.

Summary

As a true unified situational awareness platform, SecureVue provides unparalleled visibility into security and compliance data by allowing the correlation of all security elements – including events, users, assets and configurations, network behavior, performance metrics, file integrity and others – to see the often complex inter-relationships between these pieces of data.

Specifically, eIQnetworks' SecureVue benefits the U.S. Army through:

- True situational awareness that collects all security and compliance data, not just events
- Highly granular role-based access control that ensures separation of duty
- Enterprise scalability that supports the largest global enterprises
- Low implementation and management costs

Want to know how SecureVue from eIQnetworks can help you? Contact us at +1 877.564.7787 or email sales@eIQnetworks.com to learn more.



eIQnetworks
31 Nagog Park
Acton, MA 01720
t. +1 978.266.9933
f. +1 978.266.0004
www.eIQnetworks.com