



SecureVue®: Operational Security for the Good Practice Guide: Protective Monitoring for HMG ICT Systems

Solution Brief

The following table provides a complete summary of how eIQnetworks' SecureVue platform provides operational security capabilities mandated by the CSEG National Technology Authority for Information Assurance, "Good Practice Guide: Protective Monitoring for HMG ICT Systems", Issue 1.3 (October 2009).

Good Practice Guide Requirement	How SecureVue Implements this Capability
PMC 1: Accurate Time in Logs	<ul style="list-style-type: none"> ■ SecureVue monitors hosts (including Windows, UNIX, and network devices) to ensure that they are configured to synchronize time to an atomic clock source; ■ SecureVue monitors hosts to ensure that they are utilizing the Network Time Protocol (NTP); ■ SecureVue monitors network traffic and reports on all NTP traffic via flow data; ■ SecureVue normalizes all log data collected from hosts, network devices, applications and databases to a standard format (UTC), regardless of whether the native time signature was recorded in UTC.
PMC 2: Recording Relating to Business Traffic Across a Boundary	<ul style="list-style-type: none"> ■ SecureVue collects, correlates, and reports on all malware activity at the boundary of networks, including malware detection, and changes in the status of boundary antimalware programs; ■ SecureVue captures all network-based and host-based data and file ingress and egress activity as reported by both network devices and hosts, including allowed and denied (blocked) web browsing activities, file download and import/export attempts, and file access attempts.
PMC 3: Recording Relating to Suspicious Behavior at a Boundary	<ul style="list-style-type: none"> ■ SecureVue reports on all information provided by boundary network devices (such as firewalls, routers, and intrusion detection and prevention devices), including packets passed and dropped at the boundary, all console messages of any criticality, all commands issued to network devices, user authentication failures, and active user sessions; ■ SecureVue reports on all network device change activity, including changes to boundary device rulesets and access control lists, as well as changes to device signatures, and monitoring and alerting policies (including changes to SecureVue's own policies); ■ SecureVue reports on all automated responses that occur at the boundary, such as automated actions conducted by intrusion prevention systems (IPS); ■ SecureVue includes a comprehensive workflow engine, and maintains bi-directional communication with major third-party workflow and service desk applications, to track all manual actions invoked by users in response to an external attack notification.
PMC 4: Recording of Workstation, Server, or Device Status	<ul style="list-style-type: none"> ■ SecureVue reports on all event information provided by workstations, servers and devices, including all messages of any criticality, user authentication and access control failures, and active user sessions; ■ SecureVue collects, correlates, and reports on all malware activity on workstations, servers, and devices, including malware detection, and changes in the status of antimalware programs (such as signature updates); ■ Unlike log management or SIEM tools, SecureVue natively captures detailed configuration data regarding servers, workstations, and network devices, and provides detailed reports around key system changes, including changes to file and Windows registry access control lists, connected and disconnected devices (including removable media devices, such as USB storage), installed applications, Windows registry settings, and running processes/daemons; ■ SecureVue's native file integrity monitoring provides comprehensive change detection for operating system and data files on Windows, Linux, and UNIX-based hosts servers and workstations.



Good Practice Guide Requirement

How SecureVue Implements this Capability

PMC 5: Recording Related to Suspicious Internal Network Activity

- SecureVue reports on all information provided by internal network devices (such as firewalls, routers, and intrusion detection and prevention devices), including packets passed and dropped inside the network, all console messages of any criticality, all commands issued to network devices, user authentication failures, and active user sessions;
- SecureVue reports on all network device change activity, including changes to internal network device rulesets and access control lists, as well as changes to device signatures, and monitoring and alerting policies (including changes to SecureVue's own policies);
- SecureVue reports on all automated responses that occur on the internal network, such as automated actions conducted by intrusion prevention systems (IPS).
- SecureVue includes a comprehensive workflow engine, and maintains bi-directional communication with major third-party workflow and service desk applications, to track all manual actions invoked by users in response to an internal attack or threat notification.

PMC 6: Recording Related to Network Connections

- SecureVue reports on all information related to network activity and connectivity, including user authentication failures for remote access methods, authentication failures for local attempted logons of network devices, all activity (including failed node registrations) on VPN networks, all messages of any criticality, all commands issued to network connectivity devices, user sessions on network connectivity devices, and any changes to device signature databases.
- SecureVue collects detailed information from wireless access points, including logs indicating suspected wireless attacks and all wireless connections to the device;
- SecureVue collects network-related configuration information, including dynamic IP addressing tables (such as DHCP), as well as changes to IP addresses for specific servers, workstations, and network devices;
- SecureVue includes a comprehensive workflow engine, and maintains bi-directional communication with major third-party workflow and service desk applications, to track all manual actions invoked by users in response to an internal attack or threat notification.

PMC 7: Recording of Session Activity by User and Workstation

- SecureVue reports on all information related to workstation and server user activity, including user network sessions, use of specific applications and database facilities, local user sessions, and the invocation of any applications or executables.
- SecureVue's native configuration and asset data collection from workstations and servers provides complete reporting and alerting for any user account status changes, such as when accounts are created/enabled/disabled, passwords are changed, user accounts are locked out, or user privileges and/or group memberships are changed.

PMC 8: Recording of Data Backup Status

- SecureVue can collect detailed information regarding backups from both operating systems and enterprise backup application software, including the success or failure of backups, file catalogue details, and site reference and version information.

PMC 9: Alerting Critical Events

- SecureVue's comprehensive alerting capability allows the creation of virtually unlimited alerts, ranging from the most simple alerts (e.g., "show me all systems with more than 3 failed logons in a row"), to most complex, correlated alerts to that provide intelligence beyond signature-based systems and visibility into broad-based, zero-day attacks (e.g., "show me all systems with more than 3 failed logons in a row, where the system has experienced an unauthorized change in the last 30 days, and the system has been communicating using unapproved protocols.");
- SecureVue alerts are forwarded to a real-time graphical dashboard within the SecureVue security manager console, which presents a continuous, real-time stream of alerts for immediate evaluation and action;
- SecureVue alerts provide comprehensive notification options, including e-mail, SNMP, and SMTP proxy-based services such as SMS, pager, and others;
- SecureVue provides detailed reporting and alerting on changes within the product itself, including notification when alerts are created, modified, deleted, enabled or disabled;
- SecureVue alerts can be viewed by multiple users, across multiple SecureVue consoles within a distributed implementation.

PMC 10: Reporting on the Status of the Audit System

- SecureVue's native asset and configuration data collection provides detailed information regarding logging sources, including log size, threshold, and status information, and complete timestamping;
- SecureVue's log management capability provides centralized, secure control of all log-based and other security data sources across the organization, and provides consistent time-stamping and trending information over time;
- SecureVue maintains complete confidentiality and integrity of all collected data (including log data), from the point of collection and both in-transit and at-rest. SecureVue is fully accredited under NIST FIPS-140-2, and NIAP (Common Criteria) EAL 4+;
- SecureVue's integrated ForensicVue component allows users to quickly retrieve specific log (and other) data, using a straightforward, regular expressions-based query. Comprehensive filtering capabilities allow users to selectively report only relevant information, such as logs associated with a specific host, device, event, or user.

Good Practice Guide Requirement

How SecureVue Implements this Capability

PMC 11: Production of Sanitised and Statistical Management Reports

- SecureVue includes a comprehensive reporting system that contains over 1,500 out-of-box reports, all of which are customizable. In addition, users can create additional reports, or modify existing reports to ensure sanitization of proprietary data such as IP addresses and user identifiers.
- As a solution designed *specifically for situational awareness*, SecureVue is uniquely positioned to provide interoperability of reporting between vendors and security technologies. SecureVue, unlike log management or SIEM tools which are typically used in support of the Good Practice Guide for Protective Monitoring, is capable of **collecting, correlating, analyzing, and reporting** on data from many different sources, not just log-based sources. The breadth of data collected by SecureVue is unparalleled in the security monitoring industry, and includes the capability to natively collect: log and event data; asset data (such as OS information, installed applications, and running services/daemons); configuration data (including device rulesets, Windows registry settings, password policies, and user privileges); network flow data; known vulnerabilities; performance metrics; native file integrity monitoring; and native removable media (USB) device detection.

PMC 12: Providing a Legal Framework for Protective Monitoring Activities

- SecureVue captures system configuration data, and can ensure that servers, workstations, and network devices are configured to utilize a logon warning banner consistent with organizational requirements.
- SecureVue collects all logged events related to user system acceptance, including sign-up acceptance/refusal, use of digital signatures, and use of multi-factor authentication technologies (e.g., smartcard, hardware token).



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