



Full-Context Forensic Analysis Using the SecureVue® Unified Situational Awareness Platform

Solution Brief

- **ForensicVue provides - for the first time - fast access to the root cause of information security incidents and anomalies by evaluating *all* security data in context**
- **Advanced threats, including insiders, APTs and other cyber attacks, can sometimes leave only very light "fingerprints" that take detailed security information to detect**
- **ForensicVue is an integrated component of the SecureVue unified situational awareness platform**
- **ForensicVue provides complete, full-context analysis, correlation and reporting on security data across any period of time**

Finding Security "Fingerprints"

Today's headlines don't promote a strong sense of confidence among consumers, business owners, or even information security professionals. Organizations across the public and private sectors are being successfully hacked -- both from outside and within - at what seems like an exponentially increasing rate, and the result is a series of data breaches that include cardholder and other financial data, private healthcare information, classified government data, confidential intellectual property, and more. Why are these attacks becoming so much more prominent and attackers apparently more bold?

Historically, organizations previously relied entirely on signature-based technologies to detect threats to their environment. Tools such as firewalls, anti-virus, intrusion detection sensors, and others were responsible for protecting the perimeter of the network. These signature-based tools were a giant "fingerprint database" for attackers and malware.

Unfortunately, today's malicious attackers and programs are very intelligent, and rely on tactics such as evading signature detection and disabling security tools to provide stealthy access to critical business data. That means the "fingerprint databases" provided by signature-based technologies are no longer sufficient; organizations need to look beyond signatures to discover the new "fingerprints" left by attackers, both inside the organization and out. The way to achieve that visibility is through full-context forensic analysis.

What Is Full-Context Forensic Analysis?

Full-context forensic analysis differs from other, more simplistic security activities such as scanning or monitoring log files. Forensic analysis requires:

- **Visibility Across All Security Data.** In order to truly see the full context of information -- for example, how security events relate to the configuration state of the system on which the events were triggered - it's critical to have access to all security-related information. This includes not only event-based data (such as logs from devices, hosts, applications and databases) but also asset and configuration state, network traffic analysis, known vulnerabilities, performance metrics, file integrity changes, and more. Without access to all data, it becomes difficult or impossible to piece together activity to discover the true root cause of anomalies and other security issues.



- **ForensicVue searches are done using a fast, Google-like user interface with support for both point-and-click and regular expressions**

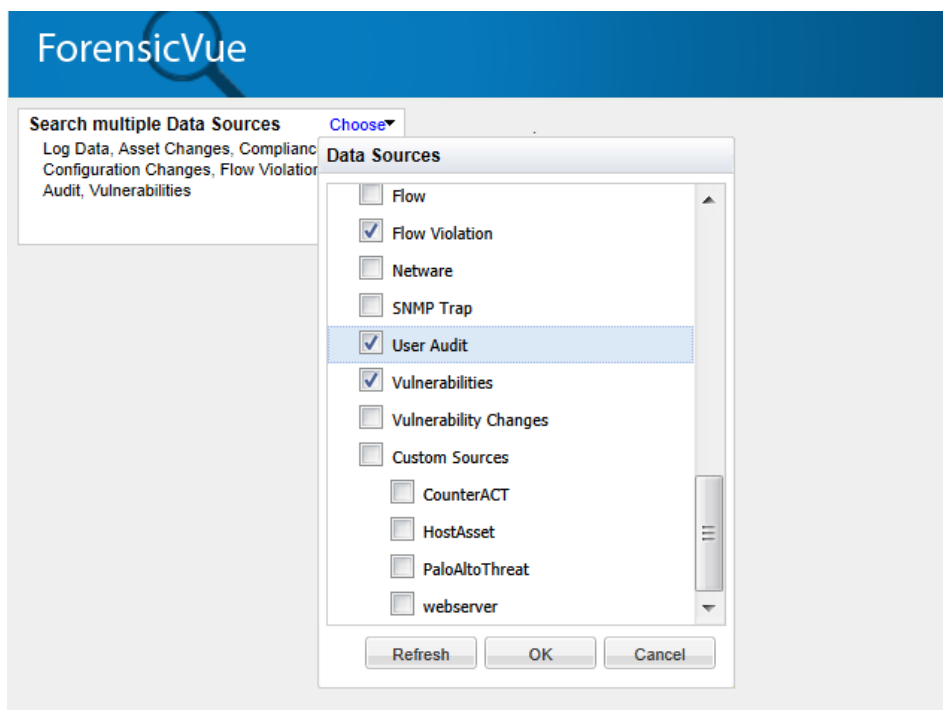
- **ForensicVue reduces the time to root cause discovery with fast, autonomic searching and categorization of security information**

- **Using the same proprietary, performance-driven database as the rest of SecureVue, ForensicVue maintains unparalleled speed when searching across days, weeks, months, and even years' worth of data**

- **Automated Visualization.** A full-context forensic analysis solution must provide access to all security-related information, but present it in a highly visual, uncluttered and minimally complex manner in order to significantly reduce the time to discover the root cause of security-related issues. This is typically achieved through automated normalization and categorization of security data to make it easier to view similar activity, as well as via dynamic visualization of large quantities of data through dashboards and other visual elements.
- **User Context.** Almost all security activity -- from network traffic, to running processes and system changes - can be tied back to the context of a specific user. For this reason, it is critical to ensure that security analysts can identify the users associated with specific actions. As importantly, this means being able to mine and normalize user accounts not only across individual systems and databases, but also directory services and identity management systems.

ForensicVue: Deep Analysis Across All Security Data

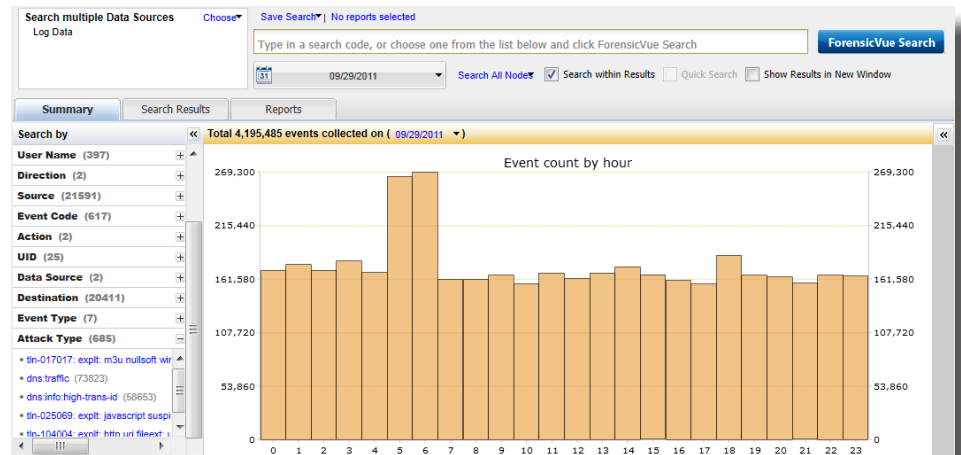
ForensicVue from eIQnetworks is an integrated component of SecureVue, the industry's first unified situational awareness platform. ForensicVue provides unparalleled visibility into the complete chain of security activity across the enterprise. Unlike forensic and other analytic components in log management and SIEM tools, ForensicVue provides analysis of **all** security data, not just event-based activity. ForensicVue's range of support data is vast, and includes events, asset and configuration changes, network traffic data (including both raw connection information and profiled data), known vulnerabilities, performance metrics, system availability, file integrity changes, and much more. Using ForensicVue, security analysts and other stakeholders can quickly identify the true root cause of security problems.



ForensicVue supports enterprise forensic analysis across all security data, including events, asset and configuration changes, network traffic data, known vulnerabilities, performance metrics, system availability, file integrity changes, and much more

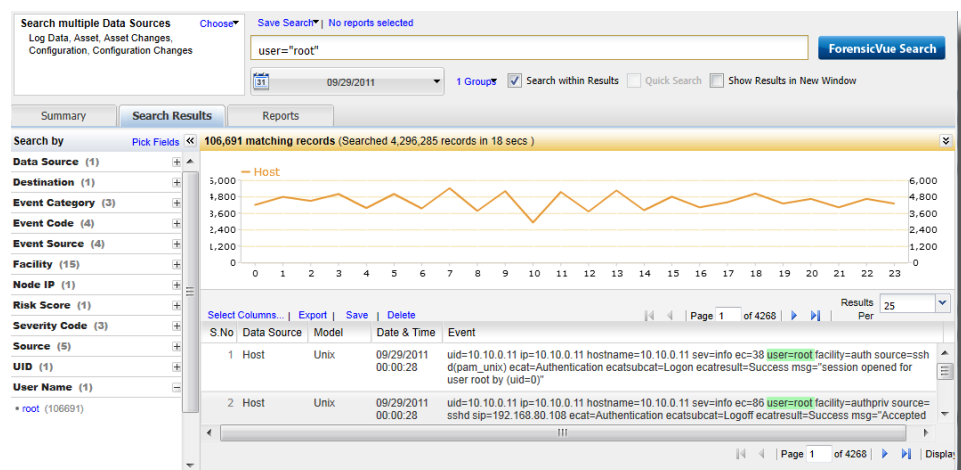


ForensicVue completely visualizes security data, providing a clear, simple and straightforward understanding of collected data. ForensicVue's normalization engine provides dynamic results of searches across unlimited periods of data, allowing security analysts to quickly determine their next course of action. Simultaneously, ForensicVue provides comprehensive "drill-down" support for rapid access to raw data. ForensicVue's autonomic capabilities ensure that security professionals minimize the time required to find their target.



ForensicVue's autonomic capabilities include dynamically normalize data elements within search criteria (on the left), as well as visualization of security data over time.

ForensicVue collects and identifies the context of users across all security activity. Working in seamless concert with the rest of the SecureVue platform (including UserVue, which can normalize multiple accounts into a single identity), ForensicVue provides comprehensive evaluation of users who are responsible for activity across the enterprise, and can be used to profile whether a potential data breach or other attack is the responsibility of a malicious insider, or an outsider who has compromised user accounts.



ForensicVue helps security professionals quickly identify all activity associated with a specific user, including activity that spans multiple operating system, database, and application accounts

ForensicVue: The Fast and Efficient Workhorse of Unified Situational Awareness

ForensicVue gives information security professionals the fast access they need to correlate **all** information security data, identify the sometimes complex relationships between security-related activities across the enterprise, and act immediately to ensure that unauthorized activity and incorrect security controls are addressed without delay.

Based on eIQnetworks' proprietary database, which provides the fastest search times in the industry, ForensicVue dramatically reduces the time required to discover the true root cause of anomalies and other security activity. Coupled with comprehensive autonomic capabilities and support for complete user context, ForensicVue represents the most advanced security monitoring analysis tool available on the market today.

Best of all, ForensicVue is an integrated component of SecureVue, the first situational awareness platform, providing additional capabilities beyond forensic analysis including continuous security monitoring, configuration auditing and assessment, and compliance automation -- all within a single, unified console!

Discover how ForensicVue, an integrated component of the SecureVue Unified Situational Awareness platform, delivers full-context security analysis across all security data. 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