

Overview

CentraComm's Security Information and Event Management (SIEM) solution is built with integrated key elements from several best-of-breed products to provide an extremely robust cloud-based SIEM service. The service offers different tiers of network monitoring and management for a customized fit to match your secure networking requirements.

What is SIEM and How Can It Benefit You?

CentraComm's cloud-based SIEM solution, known as CentraVUE, adheres to all network security compliances and is your central management tool for log management and vulnerability scanning. With our qualified network engineers monitoring security and network events – no matter where in the world they occur – you can rest assured you'll get the most comprehensive coverage throughout your entire network. With nearly 12 billion attacks averted so far, we're keeping the bad at bay every single day.

CentraVUE correlates disparate logs from multiple sources... “We have seen reductions of one million events to a single actionable item.”

-Patrick Foxhoven, CIO

Why CentraVUE?

With increasing regulatory compliances, it's more important than ever to identify and monitor events and trends that can indicate bad behavior. CentraVUE has the capability of consolidating all of your vital network data into a central repository, providing advanced correlation and delivering actionable responses to any potential network threats.

Our team of certified network security engineers directly monitors your network equipment to neutralize threats before they materialize into a bigger issue. CentraVUE monitors your network around the clock. Events affecting network security can occur anytime – day or night. The cutting edge reporting capabilities of CentraVUE accelerate the detection of potential threats and delivers faster remediation of security issues.

CENTRAVUE

- ▮ SIEM, and so much more
- ▮ Detects network attacks before they impact your business
- ▮ Provides situational awareness to proactively address enterprise threats
- ▮ Ensures quick and easy compliance reporting and documentation
- ▮ Significantly lower total cost of ownership than other compliance management solutions

SUPPORTED DEVICES

- ▮ Intrusion detection and prevention
- ▮ Firewalls
- ▮ Servers
- ▮ Switches
- ▮ Routers
- ▮ IP phones
- ▮ Server logs
- ▮ Application logs
- ▮ Workstation logs

Benefits of CentraVUE

CentraComm's infrastructure as a Managed Security Services Provider allows us to offer a robust, fully correlated 24/7, cloud-based SIEM solution.

CentraVUE offers zero capital cost and increased speed of deployment. CentraVUE is a cloud-based (meaning: hosted, scalable and resilient) security information and event management system capable of operating without the purchase, installation or maintenance of any on-premise equipment. It enables small and mid-market business who previously could not afford SIEM solutions access to fully correlated threat protection, compliance reporting, performance reporting, and much more.

Similarly, CentraVUE allows enterprise organizations the ability to quickly and easily deploy SIEM without all the integration headaches or a learning curve, scaling seamlessly throughout all branches of the organization.

CentraVUE provides companies with a custom solution that reduces total cost of ownership and allows your IT personnel to focus on mission critical projects. CentraComm's Security Operations Center staff is second to none when it comes to network diagnosis and remediation. With their ability to monitor devices around the globe, security threats and vulnerabilities are identified before they can disrupt your network operations.

The CentraVUE solution provides situational awareness with a more holistic view of the network by taking in all security and network events: asset and configuration data, logs and events, known vulnerabilities, performance metrics, and network flow data. CentraVUE has the ability to take 100MM events and boil it down to 100 actionable items, which will give you and your CIO peace of mind.

Our cloud-based SIEM can operate in a hybrid scenario for clients that require onsite log storage but still want to take advantage of the benefits of outsourcing the monitoring and management of the solution.

CentraVue Options

To best match your needs CentraVUE is available as a "self-service" On-Demand model or in Monitored Service mode where CentraComm's engineers are actively involved with monitoring your network.

On-Demand (Self Service)

With the CentraVUE On-Demand platform, you'll enjoy access to CentraComm's proven security infrastructure remotely through our cloud-based SIEM, providing your organization with the advanced tools needed to keep your network secure, including automated log correlation and analysis, asset-based security reporting, threat intelligence and automated affiliate risk management.

CentraVUE's On-Demand service puts CentraComm's cutting edge technology and security tools at your fingertips, ensuring you're getting the best of the best tools in network security to keep your network running smoothly. You have ultimate control, using your own dedicated IT team to monitor and manage your devices, without the added cost of purchasing this technology platform for yourself.

Enjoy top-notch cloud-based network security with no strings attached, with CentraComm's On-Demand Security platform.

Service Details / Technical Specs

Automated Alerts

You may choose from numerous auto-notification templates.

Ability to Build Customized Alerts

You may tailor automated alerts specific to your needs, building custom business logic.

Visibility and Reporting

Powerful real-time and historical reporting capabilities provide insight into usage trends, performance baselines and security events. Use of CentraComm's web-based monitoring tools allows the monitoring of throughput, performance, and intrusion analysis.

Customer Portal

Access to web interface to view real time information on devices being managed with a variety of graphical and visual views of the data.

Online Reporting Portal

A secure web portal offering 24/7 access to dynamic reports and flexible query tools to help identify and prioritize security-related events.

Event Archives

Security event logs are stored at CentraComm's Security Operations Center for reporting and forensic purposes.

Daily and Monthly Reports

These reports break down your event logs, tying events back to the specific PCI DSS requirements, highlighting critical issues, quiet data sources, and provide aggregate trend analysis.

On-Demand Access to Reports

Robust library of reports that may be scheduled or run in real-time.

Security Escalation

CentraComm assistance with escalation of severe or intrusive attacks to third party civil and governmental agencies.

Monitored Services

CentraVUE's Monitored Service offerings are highly scalable, allowing us to monitor your entire network, or just a single device from virtually any vendor. The choice is yours. With our cloud-based Monitored Service platform you get all the features of the On-Demand package, as well as our security expertise. We sift through the noise to focus your attention on the most pressing issues and aide you in your remediation efforts.

Our team of certified network security engineers are always accessible, working around the clock to make sure your network is secure at all times. Operating within our state-of-the-art Security Operations Center (SOC), they have the proven tools and cutting edge systems to go hand-in-hand with their industry-leading knowledge and experience. Our SOC monitors networks around the globe using continually expanding threat intelligence to better protect all CentraComm customers. We'll notify you of direct threats to your network and will offer advice on how to remedy any issues.

Service Details / Technical Specs

Along with the specs listed under "On-Demand," Monitored Services also includes the following:

Real-time Analysis

CentraComm's network security engineers will manually review and respond to security alerts, as they happen, 24/7, following the customer's own Incident Response and Escalation Policy. Our team of network security engineers are monitoring networks across the globe, which allows you the utmost viable knowledge which further increases your own network security.

Service Level Agreement

CentraComm is proud to offer our industry leading 15 minute service level agreement.

Daily Review and Analysis

Review and analysis of your logs by CentraComm's experienced Security Operations Center (SOC) will occur daily.

24/7 Telephone and Email/IM Support

Access to CentraComm's SOC for questions about escalated events, requests for up/down scoring and other concerns.

Adaptive Security and Countermeasures

CentraComm manages a set of policy-based actions to be implemented when attacks are recognized within other security and network devices.

SAMPLE OF SUPPORTED DEVICES WITH ON-DEMAND AND SUPPORTED SERVICES

Barracuda	BlueCoat Proxy	Check Point NGX
Cisco ASA, CatOS, IOS, IDS, Ironport	Enterasys Dragon Network IDS/IPS	Extreme Alpine
Fortinet Fortigate	Foundry BigIron, FastIron, NetIron	H3C (3Com)
HP Procurve	ISS Proventia	Juniper ISG, Netscreen
Linux	McAfee EPO, Intrushield	Microsoft Exchange, ISA, SQL
Secure Computing Sidewinder	SNORT IDS Sensor	SonicWall
SourceFire	Symantec Gateway Security	TippingPoint Unity
TopLayer Attack Mitigator	VMware	Windows Desktops, Servers, IP Phones

For a full list of support devices visit <http://www.centracomm.net/centravue>. If your device is not on this list, contact us, it can be setup as new device support, sometimes in as little as one hour.

NETWORK & SECURITY DEVICES - SERVICE ATTRIBUTES	ON-DEMAND	MONITORED
24/7 Real Time Analysis by Security Expert		✓
24/7 Real Time Alerting	✓	✓
Automatic Off-site Configuration Backup	✓	✓
Automated Performance Monitoring	✓	✓
Real-time Portal Access	✓	✓
Automated / Advanced Correlation of Security Events by SIEM Platform	✓	✓
Escalation of Events to Third Party Authorities		✓
Device Polling	✓	✓
Alert / Event Resolution & Consultation		✓

PREMIUM SERVICES & REPORTING AVAILABLE AT A NOMINAL FEE

- ▣ Compliance reporting (PCI, SARBOX, NERC, HIPAA, or GLIB)
- ▣ Vulnerability scanning
- ▣ Network behavior anomaly detection

REPORTS - INCLUDED	SERVERS, APPLICATIONS, IDS/IPS	ROUTERS, SWITCHES, FIREWALLS
Log-based	✓	✓
Configuration	✓	✓
Asset	✓	✓
Flow		✓
Performance	✓	✓
Availability	✓	✓
Executive	✓	✓

CONTACT CENTRACOMM

CentraComm Communications
 323 South Main Street Findlay, OH 45840
 419.423.2666
info@centracomm.net

CONNECT ON SOCIAL MEDIA

LinkedIn www.linkedin.com/companies/centracomm
twitter www.twitter.com/centracomm
facebook www.facebook.com/centracomm