Learn About Secure Analytics

This *Learn About* introduces you to the fundamentals of security information and event management (SIEM) and Juniper Secure Analytics (JSA). It explains these essential network security technologies and shows why they are essential in today's networks. For those of you who need field knowledge, this *Learn About* also reviews each of the core functions of a SIEM and JSA implementation and describes how a SIEM and JSA are used.

Secure the Network

Networks are growing larger and more complex than ever before. At the same time, multiple threats to the security of those networks are emerging and spreading rapidly. As shown in Figure 1, there are also more possible points of entry into any given network because of the increase in user mobility, the number of remote locations that might exist, and the sheer number of devices accessing the network.

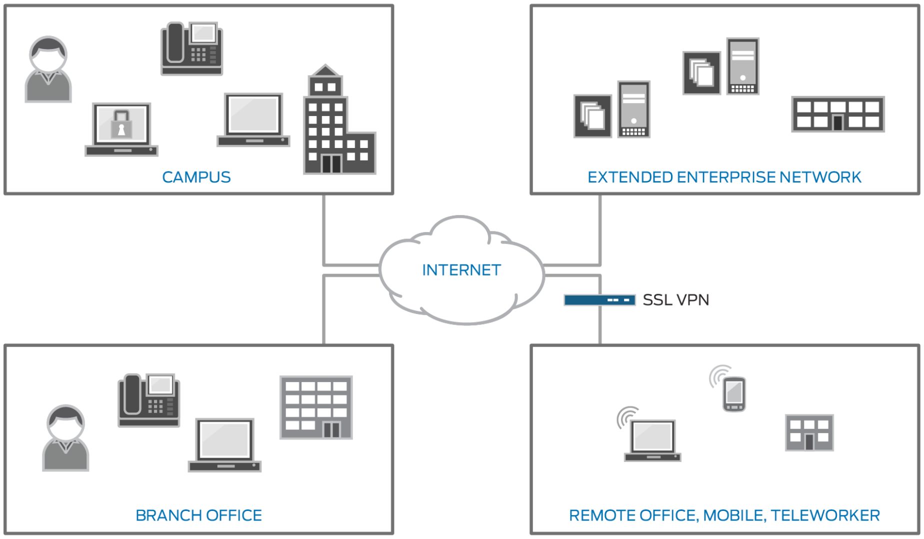

CAMPUS
EXTENDED ENTERPRISE NETWORK
INTERNET
SSL VPN
BRANCH OFFICE
REMOTE OFFICE, MOBILE, TELEWORKER

Figure 1 *Enterprise Network*

A security breach is one of the earliest stages of a security attack by a malicious intruder, such as a hacker, cracker, or nefarious application. Security breaches happen when the security policy procedures are violated or there is an intruder in the system. Depending on the nature of the incident, a security breach can be anything from low risk to highly critical.

The digital market economy, with its continual barrage of new applications and technologies, also creates additional risks and invites a slew of new attacks on networks. In some organizations *security breaches* can go completely undetected for months, while others have IT departments with staff dedicated to protecting a network against malicious activity. They must analyze data from a multitude of sources in order to understand what threats are facing a network, then they must determine what actions to take to address those threats.

What IT staffs need is a complete, holistic solution that provides layered security to protect from threats that occur at all layers and at every location of a network, including branch offices, campuses, and extended enterprises. Without such a solution, IT professionals cannot fully manage all the threats a network can incur. They need:

- Comprehensive visibility that can analyze everything happening in the network.
- Analytics that will analyze and investigate potential threats in near real time.
- Actionable intelligence that will identify targets, threats, and incidents.

IT departments also need to keep abreast of compliance requirements, providing:

- Accountability that can survey the reports on who did what and when.
- Transparency that can provide visibility into the security controls, business applications, and assets that are being protected.
- Measurability that can provide metrics and reporting around IT risks within a company.

Introduction to SIEM

SIEM software provides a powerful way for organizations to detect the latest security threats to their networks before they can cause damage. SIEM provides a holistic view of an organization's IT security by providing real time reporting coupled with long-term analysis of security events.

SIEM software logs event records from sources throughout a network. Those logs provide important forensic tools to an IT staff, which the software then helps to analyze. Complete log collection also helps address many compliance reporting requirements.

Parsing and normalization maps log messages from different systems into a common data model, enabling IT professionals to better connect and analyze related events, even if those events are initially logged in different source formats. Additionally, correlation links log events from disparate systems or applications, which greatly speeds not only the detection of, but the reaction to, security threats.

SIEM aggregation can also reduce the volume of event data by consolidating duplicate event records and then reporting on the correlated, aggregated event data in real time, comparing it to long-term summaries.

How SIEM Works in an Attack

Let's begin with a look at a basic network attack as shown in Figure 2.

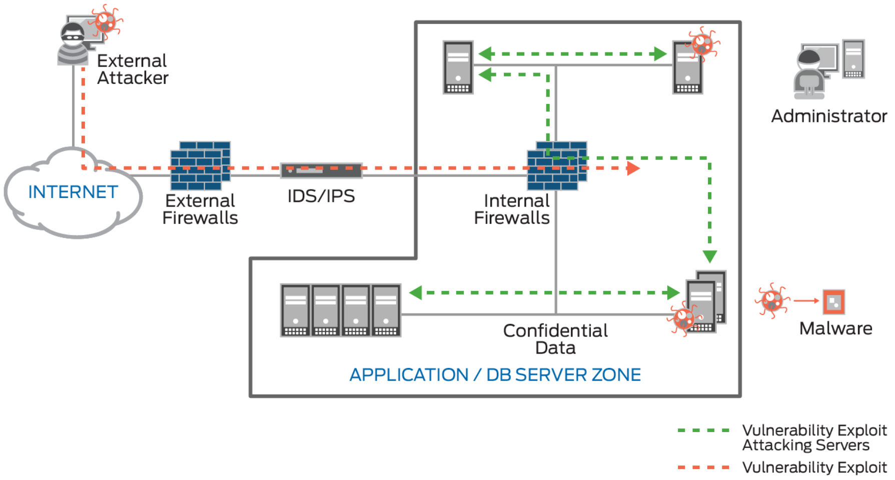


Figure 2 *Example of a Basic Attack to a Network*

In Figure 2, the attacker on the left scans the perimeter defenses to find a hole in the network. The attack bypasses network defenses and compromises web servers using a vulnerability exploit. From the web server the attack pivots to the database server, which holds confidential data and installs malicious software that opens a backdoor for the attacker to steal data.

How would one detect such an attack without using SIEM? Figure 3 shows the steps in a traditional network defense.

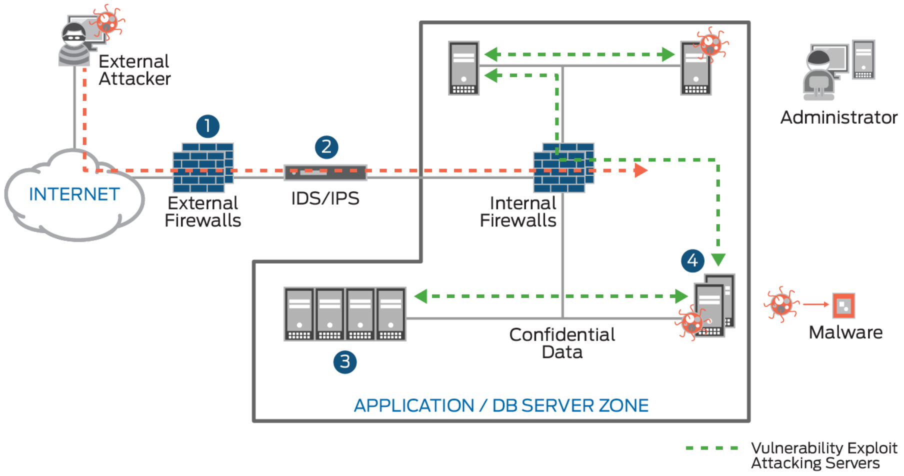


Figure 3 *Analyzing the Basic Attack Without Using SIEM*

You can see, in Figure 3, that the network uses:

- Firewall logs with events for reconnaissance, scanning, and so on.
- Intrusion detection service (IDS) or intrusion prevention system (IPS) logs have exploit signatures triggering (both behavior and anomaly).
- There will be web or application server logs (access inbound or outbound traffic).
- And of course, database logs.

In Figure 4, when the same attack occurs in a network using SIEM, the software provides insight into all the IT components (gateways, servers, firewalls, and so on).

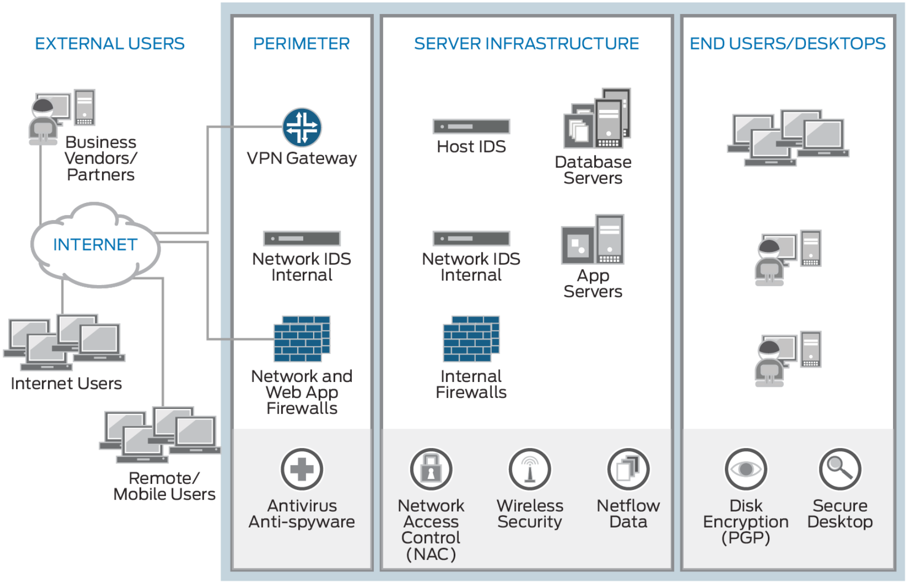


Figure 4 *SIEM Holistic View*

A perimeter is the fortified boundary of the network that might include: routers, firewalls, IDSs, IPSs, VPN devices, software architecture, DMZs, and screened subnets.

SIEM software centrally collects, stores, and analyzes logs from *perimeter* to end user. It monitors for security threats in real time for quick attack detection, containment, and response with holistic security reporting and compliance management.

It's time for SIEM software in any network that is open to attacks.

Juniper Networks Secure Analytics

Once you realize the value of a SIEM and its functionality, you need to understand how JSA can support SIEM security and compliance requirements.

A JSA Series appliance is a SIEM appliance that solves many requirements of IT staffs around the world. To better understand how JSA works, let's briefly review its key components and how they operate as a SIEM solution.

Event Collection and Processing

JSA combines many key SIEM features (see Table 1) but the core components of the JSA Series are an event processor, a flow processor, an event collector, and a magistrate (console).

A log source is a data source that creates an event log.

An event is a record from a *log source*, such as a firewall, a router, a server, an IDS, or an IPS, that describes an action on a network or a host.

As shown in Figure 5, JSA event processing involves the following steps:

1. Log sources typically send syslog messages (but they can use other protocols, too).

2. The event collector receives the raw events as log messages from a wide variety of external log sources.

3. Device Support Modules (DSMs) in the event collectors parse and normalize raw events as the raw log messages remain intact.

A rule is a collection of tests that triggers an action when specific conditions are met. Each rule can be configured to capture and respond to a specific event, sequence of events, flow sequence, or offense. The actions that can be triggered include sending an email or generating a syslog message.

4. The classification engine and the *rules* are responsible for processing events received by JSA and comparing them against defined rules, keeping track of systems involved in incidents over time, generating notifications to users, and generating offenses.

5. Event processors receive the normalized events and raw events to analyze and store them.

6. The magistrate correlates data from event processors and creates offenses.

7. Event storage (Ariel) is a time series database for events and flows where data is stored on a minute-by-minute basis. Data is stored where the event is processed.

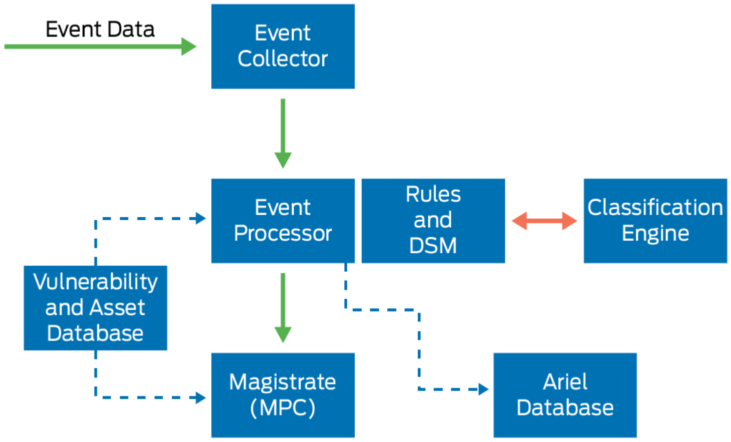


Figure 5 *Event Collection and Processing Flow Diagram*

Flow Collection and Processing

A flow is a communication session between two hosts that provides information about network traffic and can be sent to JSA in various formats, including network taps, span or mirror ports, flowlog files, NetFlow, J-Flow, sFlow, and Packeteer.

The flow processing (see Figure 6) involves the following steps:

1. The flow collector reads different types of flow data and creates flow records to be processed.

2. The event collector completes a number of flow processing functions, such as:

- Removing duplicate flows when multiple flow collectors are providing data to flow processor appliances.
- Recognizing flows from each side and combining them into one record. When data is not received from both sides, the event collector then analyzes and combines the external flow sources, such as NetFlow, that might only report ingress or egress traffic, as well as instances where span traffic enters a network from a single point, and exists through another, creating asymmetric reporting of data to flow collectors.
- Monitoring the number of incoming events and flows to the system to manage input queues and licensing.

- Applying routing rules for the system, such as sending data to offsite targets, external syslog systems, JSON systems, other SIEMs, and so on.

3. Classification engine and the rules are responsible for processing events received by JSA and comparing them against defined rules, keeping track of systems involved in incidents over time, generating notifications to users, and generating offenses.

4. Event processors parse the message's fields (IP address, ports, and so on) and store data in the Ariel database.

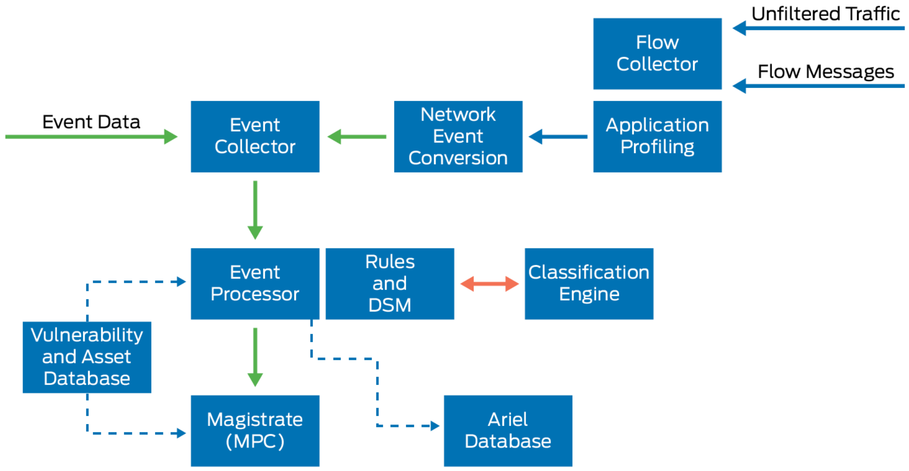


Figure 6 *Flow Collection and Processing Flow Diagram*

As you can see, JSA goes beyond traditional SIEM products and network behavior analysis (NBA) products to create a command-and-control center that delivers threat analytics, log analytics, and complete compliance measurability.

When it comes to secure analytics, JSA Series appliances can protect your network. Let's look very briefly at all the features and benefits of the JSA Series.

JSA Appliance Features and Benefits

JSA Series appliances come in several form factors to enable you to scale their features and benefits:

- JSA Virtual Appliance – A virtualized platform that can be deployed as an all-in-one appliance or in a distributed setup as a console, or as an event or a flow processor. A JSA virtual appliance can also be deployed as a store and forward event collector.
- JSA3800 – An enterprise-class appliance that provides a scalable network security management solution for medium-to-large size companies, including globally deployed organizations. It is also the base platform for an enterprise-class scalable secure analytics solution. JSA3800 can be deployed as an all-in-one appliance or in a distributed setup as a dedicated event, flow, or combination processor. It can also be deployed as a store and forward event collector.
- JSA5800 – An enterprise and carrier-class appliance that provides a scalable network security management solution for medium-size companies and scales to support large, globally deployed organizations. JSA5800 can be deployed as an all-in-one appliance or in a distributed setup as a console or dedicated event or flow processor. It can also be deployed as a store and forward event collector.

- JSA7500 – An enterprise and carrier-class appliance that provides a scalable network security management solution for large, globally deployed organizations. JSA7500 can be deployed as a console or distributed event or flow processor. It can also be deployed as a store and forward event collector.

Table 1 details some of the major features and benefits of owning and using JSA appliances, many of which go beyond the SIEM discussions in this *Learn About*.

Table 1 *JSA Features and Benefits*

Features	Description	Benefits
All-in-one appliance	Event collection, flow collection, event processing, flow processing, correlation, analysis, and reporting are all embedded within JSA.	All core functions are available within the system and it is easy for users to deploy and manage in minutes. The architecture provides a streamlined solution for secure and efficient log analytics.
Distributed support	Ability to scale to large distributed deployments that can support up to 5 million events per second.	Gives users flexibility to scale to large deployments as their business grows and can be easily deployed in large distributed environments.
HDD implementation	Utilizes SAS HDD in RAID 1 and RAID 10 setups.	SAS HDD is designed for 24x7 operations. RAID 1/10 implementation provides best possible performance and redundancy.
Quick install	Comes with an easy, out-of-the-box setup wizard.	Users can install and manage JSA Series appliances in a couple of steps.
Automatic updates	Automatically downloads and deploys reputation feeds, parser updates, and patches.	Users do not need to worry about maintaining appliance and OS updates and patches.
High availability	Users can deploy all JSA Series appliances in HA mode.	Users can deploy JSA with full active or passive redundancy. This supports both deployment scenarios: all-in-one and distributed.
Built-in compliance reports	Out-of-the-box compliance reports are included with the JSA.	Provides more than 500 out-of-the-box compliance reports.
Reporting and alerting capabilities for control framework	Control Objectives for Information and related Technology (CobiT) International Organization for Standardization (ISO) ISO/IEC 27002 (17799) Common Criteria (CC) (ISO/IEC 15408) NIST special publication 800-53 revision 1 and Federal Information Processing Standard (FIPS) 200	Enables repeatable compliance monitoring, reporting, and auditing processes.
Compliance-focused regulation workflow	Payment Card Industry Data Security Standard (PCI DSS) Health Insurance Portability and Accountability Act (HIPAA) Sarbanes-Oxley Act (SOX) Graham-Leach-Bliley Act (GLBA) Federal Information Security Management Act (FISMA)	Supports multiple regulations and security best practices. Includes compliance-driven report templates to meet specific regulatory reporting and auditing requirements.

Features	Description	Benefits
Management-level reports on overall security state	The JSA reports interface allows you to create, distribute, and manage reports that are generated in PDF, HTML, RTF, XML, or XLS formats.	Users can use the report wizard to create executive and operational level reports that combine any network traffic and security event data in a single report.
One-stop support	Juniper Networks Technical Assistance Center (JTAC) supports all aspects of JSA.	Users do not need to go to several places to get support, even for multivendor issues.

JSA Use Case

As a final step, let's review a use case for JSA, and follow the requirements and the solution. This use case concerns the Payment Card Industry Data Security Standard that was created by major credit card companies to ensure privacy and security of credit card holders. All organizations that deal with credit card processing and transactions need to comply with these standards to avoid fees and penalties, and this use case will show you how JSA addresses the six main PCI DSS objectives.

PCI DSS Requirements

The PCI DSS standard outlines six relatively broad control objectives for network security:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability assessment (VA) program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

It is not an easy task for IT administrators to implement these standards across their network as there is no single product that complies with all six standards. Many SIEM and log management products claim to answer all these concerns, but the PCI DSS standard calls for more than the collection and correlation of logs. Insight into the network from the passive monitoring of network communications must be put in place in conjunction with aggregation and correlation of logs from the security and network infrastructure.

The Solution

NBAD is the continuous monitoring of a proprietary network for unusual events or trends. NBAD is an integral part of NBA.

JSA is a network security management platform that facilitates the comparison of data from the broadest set of devices and network traffic. It combines log management, SIEM, and network behavior anomaly detection (NBAD), into a single integrated end-to-end network security management solution. This allows administrators to get a complete picture of their network security posture. This surveillance capability brings together all pertinent PCI DSS data for the purpose of executing and maintaining an organization's PCI DSS program. Table 2 details the JSA approach to meeting PCI requirements. Whether it's for the PCI industry, the Federal Information Security Management Act (FISMA), or any other compliance-driven organization, JSA has a complete solution.

Table 2 *JSA Approach to Meeting PCI Requirements*

PCI Requirement	JSA Approach
Build and maintain a secure network	▪ Detection and classification of protocols and applications within the network. ▪ Automatic policy creation through learning normal traffic behavior and acceptable protocols, alerting when traffic deviates from normal patterns, and alerting when new servers, databases, protocols, or applications are discovered in the DMZ. ▪ Layer 7 visibility detects and alerts risky or secure protocols running over non-standard ports, which indicates suspicious behavior. ▪ Real time intuitive views of network traffic by protocol or application allow for in-depth analysis and troubleshooting. ▪ Stores flows like NetFlow, SFlow, and JFlow and allows for detailed forensic searching of network communications associated with risky or mistrusted protocols. ▪ Default PCI report templates and a flexible reporting wizard provide in-depth reports on PCI-related networks and services.
Protect card holder data	▪ Send alert and notification of any suspicious attempts to access sensitive data. ▪ Detect unencrypted data even in the absence of intrusion detection systems. ▪ Store the content from flows, which allows detection of unencrypted user name and passwords, or information on potential data theft. ▪ Logging from encryption technologies such as SNMPv3 devices.
Maintain VA program	▪ Automatic correlation of antivirus data with other logs and network information for accurate detection and prioritization of threats. ▪ Reporting and real time viewing of antivirus logs. ▪ Integration with vulnerability management and assessment tools used for creation of asset/host profiles. ▪ Asset profiles are centrally stored within the JSA and used for detection of new hosts on the network, new services running on a host or network, and accurate prioritization of threats based on vulnerability information. ▪ Use real time passive profiling to augment vulnerability data, which is typically not kept up to date, by using network communications to profile which services are running on hosts and keep asset profiles current.
Implement strong access control measures	▪ Complete auditing and alerting for access, configuration changes, and data changes to systems and databases with cardholder data. ▪ Detection of multiple logins that are followed by a failed login from suspicious or unknown hosts. ▪ Default, out-of-the-box authentication log correlation rules allow for easy identification of regulatory compliance servers and quick configuration of internal policies.
Regularly monitor and test networks	▪ Out-of-the-box customizable access and authentication rules allow for easy detection of threatening or invalid access attempts. ▪ Deep inspection analyzes all log data and network communications to monitor and audit all activity around an access offense. ▪ File integrity monitoring and notification through log analysis. ▪ Backup and archive of access audit trails. ▪ Provides continuous monitoring of security, systems, and processes. ▪ Real time alerting and notification of changes to the network, threats or violations that impact meeting compliance, and views and historical reports of all collected network and log data. ▪ Up to date vulnerability information through the use of passive profiling of network communications.

PCI Requirement	JSA Approach
Maintain an information security policy	▪ Continuously analyzes all network and security data for identification of threats and vulnerabilities. ▪ Automatically learns all assets and hosts on the network and provides user identity profiles and running services profiles based on passive vulnerability assessment and active vulnerability assessment. ▪ Default built-in policy rules map directly to PCI requirements. ▪ Easy-to-use customizable rules engine that allows organizations to build their own compliance intelligence for monitoring and notification of specific violations. ▪ Offenses provide documented and historical perspective of all analysis and data associated with a PCI-related incident.

Useful Links and References

- This technical documentation includes everything you need to understand and configure all aspects of JSA: http://www.juniper.net/techpubs/en_US/release-independent/jsa/information-products/pathway-pages/jsa-series/product/

- JSA7500 introduction video. In this video, learn about JSA7500 and its components: https://www.youtube.com/watch?v=mcVUm2MsN2g

- Contains PCI DSS objectives for network security and the solution using JSA: http://www.juniper.net/us/en/local/pdf/whitepapers/2000260-en.pdf

- This technical documentation includes all the information you need to understand and configure all aspects of QRadar software: http://www-01.ibm.com/support/docview.wss?uid=swg21614644

- This IBM page can help you to learn more about QRadar software and its features: http://www-03.ibm.com/software/products/en/qradar-siem

- This is the official IBM Security Support channel. It provides presentations and videos—such as IBM Security QRadar Open Mic webcasts—created by the IBM Support team: https://www.youtube.com/playlist?list=PLFip581NcL2XlvaEyrZMm3Nf1-Mc5-wRk

- This site provides WordPress posts on SIEM from the professionals: http://siemthoughtsonsecurity.wordpress.com/tag/what-is-a-siem/

- This site provides articles on SIEM from the professionals: http://www.networkworld.com/article/2180119/tech-primers/5-reasons-why-siem-is-more-important-than-ever.html

- This site provides articles on understanding and implementing a SIEM in your network: http://www.tomsitpro.com/articles/siem-solutions-guide,2-864.html

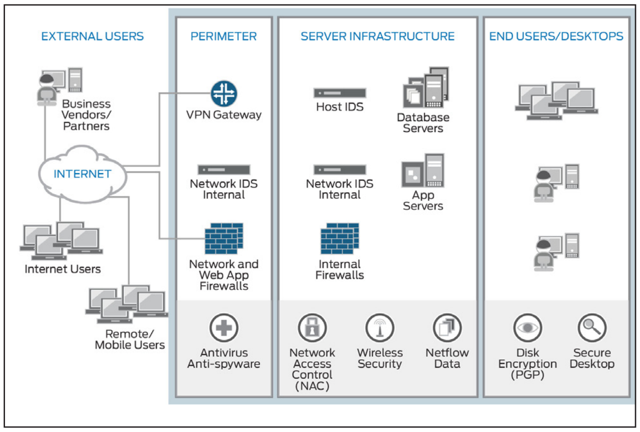
- This site provides articles on SIEM dos and don'ts: http://www.csoonline.com/article/2124604/network-security/siem--security-info-and-event-management-dos-and-don-ts.html

- At this site SANS Reading Room maintains, and makes available at no cost, a wide collection of research documents about various aspects of information security. It features over 2,460 original computer security white papers in 96 different categories: http://www.sans.org/reading-room

Learn About Secure Analytics

by Keerthi Latha M R

Learn about security information and event management (SIEM) and how Juniper Secure Analytics (JSA) implements this powerful solution while maintaining your compliance requirements. JSA can centrally collect, store, and analyze logs from perimeter to end user, monitoring for security threats in real time for quick attack detection, containment, and response. This Learn About is required reading for all IT professionals who maintain today's modern networks and who need to know how to keep those networks secure.



About the Author:
Keerthi Latha M R is an Information Development Engineer at Juniper Networks with over 10 years of experience in writing and developing documentation for networking and telecommunications.

Author's Acknowledgments:
Thanks to Patrick Ames, Nancy Koerbel, Julie Wider, Lisa Eldridge, and Karen Joice for their engagement in this project, and to project promoters Mindy Isham and Indira Upadhayaya.

Version History: First Edition, March 2016 2 3 4 5 6 7 8 9

For more information see:
juniper.net/documentation