NetGain systems

Maximize uptime. Develop insights. Provide answers.

NetGain SIEM Datasheet

The IT security landscape is ever changing. We have moved from perimeter security to enterprise cybersecurity, from protecting only enterprise-owned assets to ensuring the safety and integrity of user-owned and IoT devices connecting to corporate networks.

In wanting to keep their organization secure, more and more IT departments are turning to SIEM (Security Information and Event Management) to catch abnormal behavior and potential threats by analyzing log data from multiple sources in their IT infrastructure created by actual events and activities. SIEM would enable IT departments to identify such threats in real-time, as well as interrogate historical data to determine any past attacks or if there is a pattern to attacks.

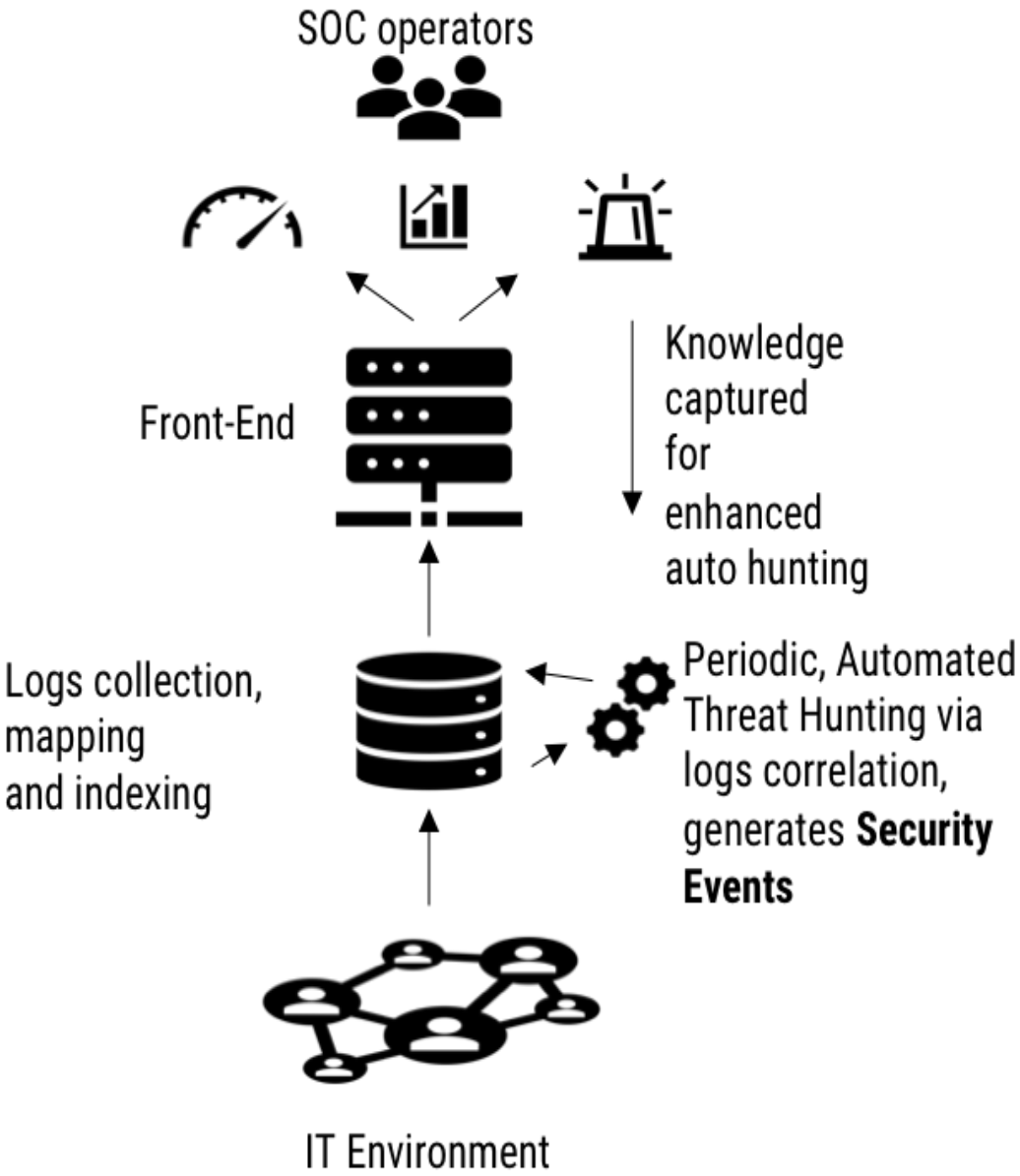
Introducing NetGain SIEM

Implementing a SIEM solution does not have to be a complex and expensive affair. Like any other SIEM solution, NetGain SIEM will improve the visibility of your organization's overall security and identify threats to your IT infrastructure by correlating the different events from the log data that constitute a threat. But unlike most other SIEM solutions, NetGain SIEM simplifies how SIEM is deployed and used to put it within reach of organizations with smaller IT departments, yet has the flexibility and scalability to be used by larger and more demanding organizations looking to reduce the complexity in managing their IT security operations.

NetGain systems

Maximize uptime. Develop insights. Provide answers.

How it works



NetGain systems

Maximize uptime. Develop insights. Provide answers.

Key Highlights

• Comprehensive visibility of security related data and events

NetGain SIEM comprises Log Analytics and Security Analytics.

Log Analytics uses Elasticsearch for quick searching and investigation into multiple log datasets to provide you with comprehensive visibility of the activities occurring in your IT infrastructure.

NetGain SIEM supports the collection and normalization of the logs of a wide variety of devices, applications, and cloud services, including Network devices, firewalls, IPS, identity and authentication systems, servers, Syslog/Windows Event logs, AWS, Google Cloud, office365, MS SQL etc.

Supported Vendor List
• Apache_Tomcat.log • ArcSight_ArcSight.log • Blue Coat_Proxy SG.log • CISCO_ASA.txt • CISCO_CiscoRouter.log • CISCO_IronPort.txt • Clavister_W50 Entry.log • ContentKeeper Technology_ContentKeeper.log • FireEye_MPS.log • Fortinet_FortiGate-500D.log • Fortinet_Fortigate.log • HPE_HPE-UX.log • IBM_Domino.log • Imperva Inc_SecureSphere.txt

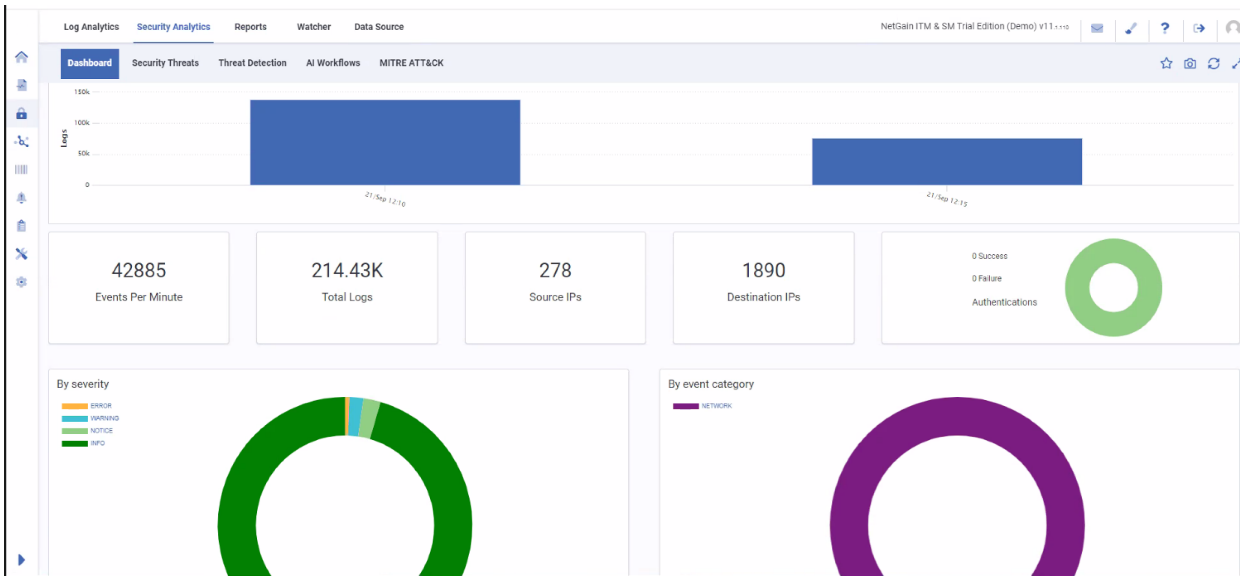
- IntersectAlliance_Snare.log
- Jboss_Jboss Wildfly.log
- Juniper_Firewall-VPN.log
- Juniper_JUNOS.log
- McAfee_Secure Internet Gateway.txt
- Microsoft_DHCP Server.log
- Microsoft_DNS Trace Log.log
- Microsoft_Exchange Server.log
- Microsoft_Internet Information Server.log
- Microsoft_WindowsMicrosoft-Windows-Security-Auditing.log
- NetScreen_Firewall-VPN.log
- Palo Alto Networks_PAN-OS_5.log
- Palo Alto Networks_PAN-OS_6.log
- Palo Alto Networks_PAN-OS_7.log
- Palo Alto Networks_PAN-OS_8.log
- PostgreSQL.log
- Secure Computing_Gauntlet.log
- Snort_Snort.log
- Sourcefire_Sourcefire.log
- Squid_Squid Web Proxy Server.log
- Trend Micro Inc_OSSEC HIDS.log
- Trend Micro_Control Manager.log
- Trend Micro_Deep Security Manager.log
- Unix_Unix.log
- VMware_ESX.log

NetGain systems

Maximize uptime. Develop insights. Provide answers.

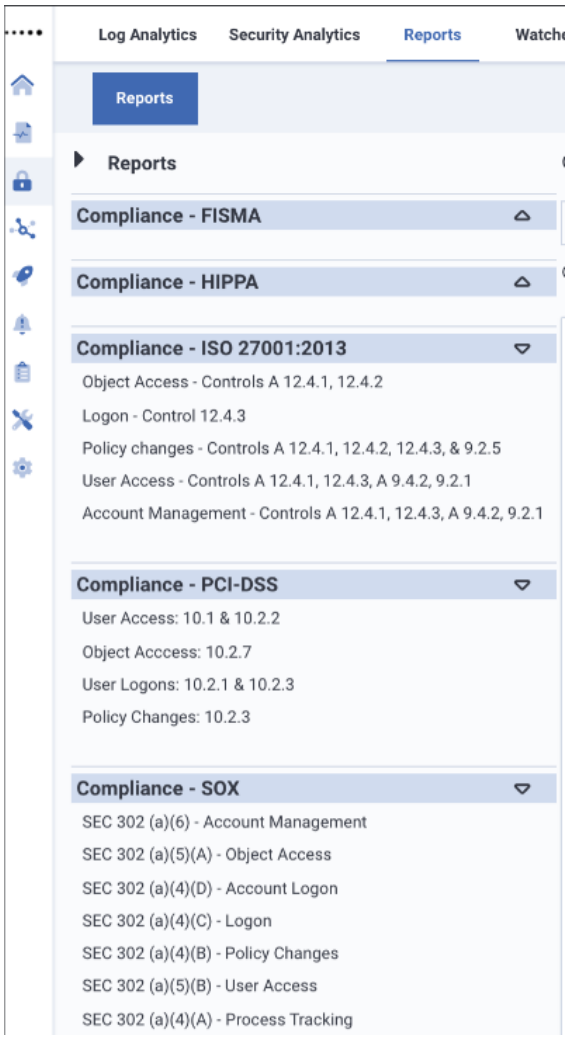
Security Analytics is designed to automatically analyze and correlate data across multiple data sources including events, network traffic/flow and user authentication/logon activities to detect potential known or unknown threats.

Logs from different devices are collected, normalized, and mapped into a centralized file following the Elastic Common Schema. Hundreds of pre-built automatic threat detection rules including security use cases, anomaly detection algorithms and real-time correlation policies are run against the centralized data to rapidly identify known and potential threats, including complex incident



• Comprehensive reports

NetGain SIEM has built-in reports and customized reporting templates to enable you to get the report you need and to easily meet industry compliance or auditors' audit requirements. You can also easily convert a frequently used query into a report format with just a few clicks of the mouse. Reports can be generated and delivered according to user-defined schedule.



• Integration with threat intelligence from open-source platforms or organizations

By integrating information from other threat intelligence sources, NetGain SIEM can flag out a threat when it comes across a domain or IP in your logs identified as malicious by such sources. Some of the threat intelligent sources NetGain SIEM can integrate with include talosintelligence.com, rules.emergingthreats.net and tech.gov.sg.

Deploying NetGain SIEM

NetGain SIEM can be deployed in a single server or distributed over multiple VMs, appliances or Cloud instances. Its highly flexible and scalable architecture lets it fit easily into any existing environment while having the capacity to meet any future growth and expansion.

NetGain SIEM can manage devices in your IT infrastructure spanning multiple geographies, in the cloud and in hybrid physical / cloud networks by leveraging on NetGain Cloud Vista Suite, allowing you to remotely monitor and manage threats to your IT infrastructure from virtually anywhere.

Appliance/Server/VM requirements

The requirements for running and operating NetGain SIEM will depend on the number of devices and the size of the network it is deployed in. The following gives an indication of the NetGain SIEM requirements for a given small IT environment. Please contact NetGain on the NetGain SIEM requirements for your environment.

Managed SIEM environment: Up to 100 devices, consisting of 1-10 firewalls, 10-40 switches/routers, and 20-40 Windows or Linux servers/containers **Data Retention period:** 6 months	
Hard disk	**2TB**
CPU	**Qual Core**
RAM	**16GB**
Operating System	**CentOS**
Browsers Supported	**Firefox, Google Chrome, Safari, Microsoft Edge.**

NetGain systems

Maximize uptime. Develop insights. Provide answers.

About NetGain Systems

Founded in 2002, NetGain Systems is a pioneer in the IT monitoring business and has established local teams throughout the Asia Pacific Region, including Australia, China and Singapore.

Regardless of location, type, size, or complexity, our solutions give customers the power to monitor their IT services, infrastructure, applications and devices with ease, all from a single management dashboard, so you can maximize uptime and achieve IT excellence.

By understanding that every organization's IT environment is different, NetGain's dynamic solutions are designed to be uniquely adaptable, fitting the unique demands of your operating environment and evolving with your growing organization.

E info@netgain-systems.com