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 behaviour and potential threats by analyzing log data from multiple sources in their IT infrastructure created by actual events and activities. SIEM enables 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.

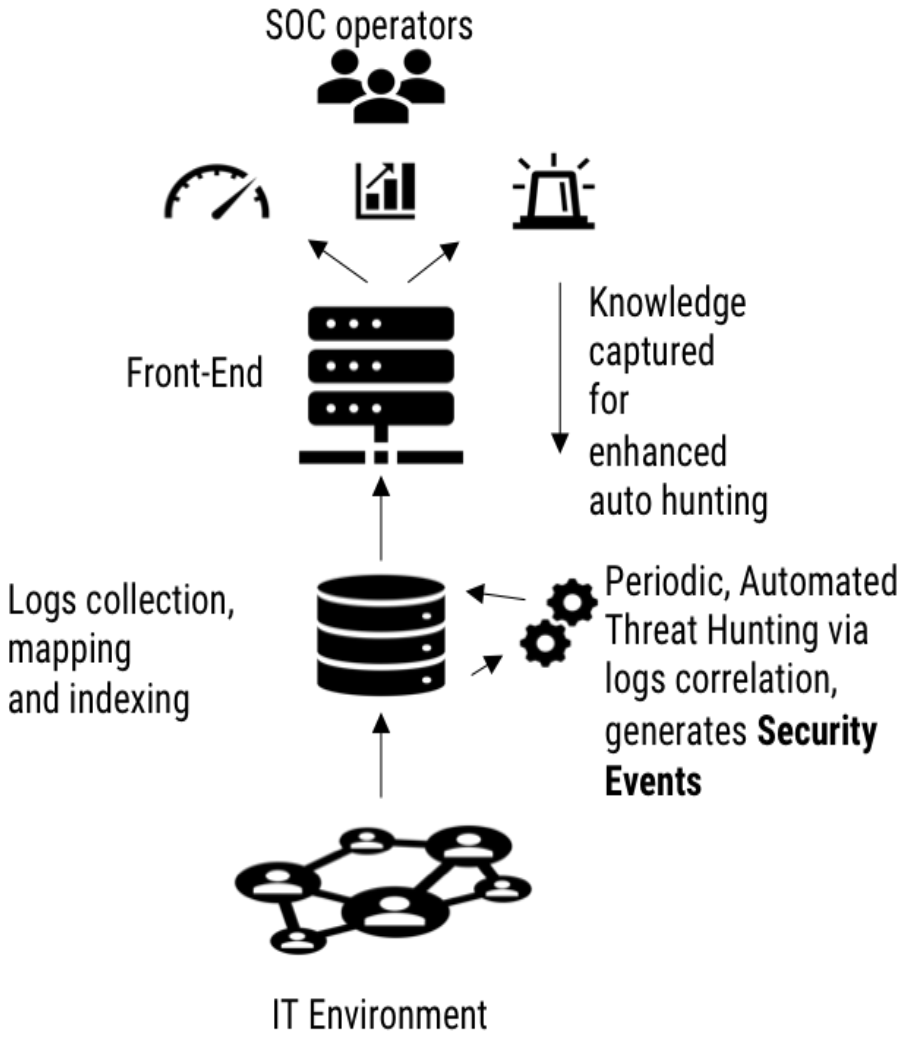
Introducing NetGain SIEM

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.

The NetGain SIEM solution comprises two functions:

- Log Analytics
- Security Analytics

How it works


SOC operators
Front-End
Knowledge captured for enhanced auto hunting
Logs collection, mapping and indexing
Periodic, Automated Threat Hunting via logs correlation, generates **Security Events**
IT Environment

NetGain systems

Maximize uptime. Develop insights. Provide answers.

Key Features

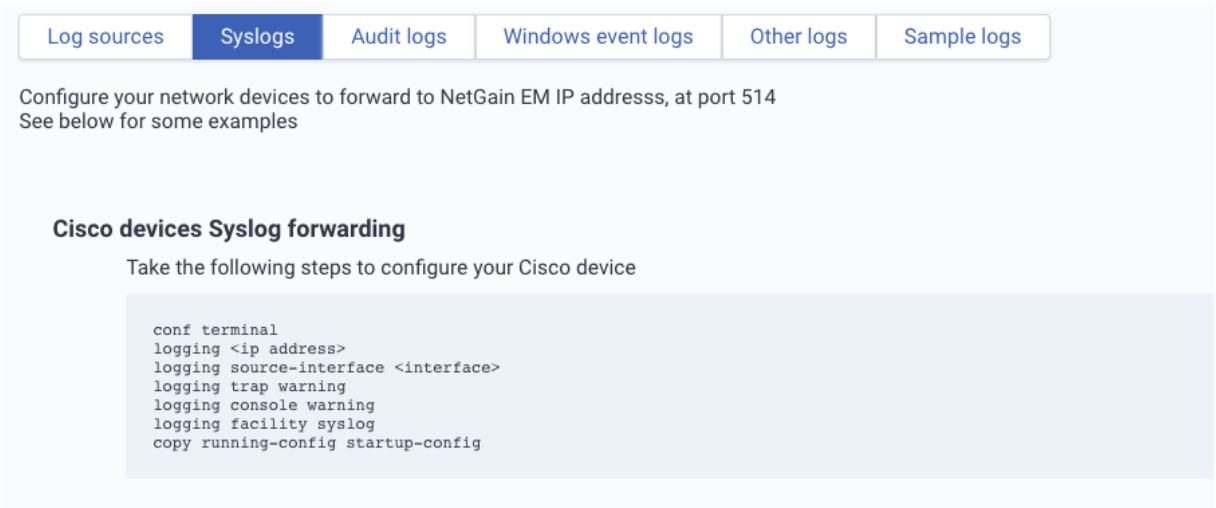
Log Analytics

Log Analytics is designed to collect systems logs from a variety of IT devices, including security devices, servers, network devices and more, whether they are on-prem or in the cloud. The logs are mapped using a common schema, that will allow intelligent search and correlation. The user can then generate custom dashboards and compliance reports from the logs.

- Comprehensive log sources supported

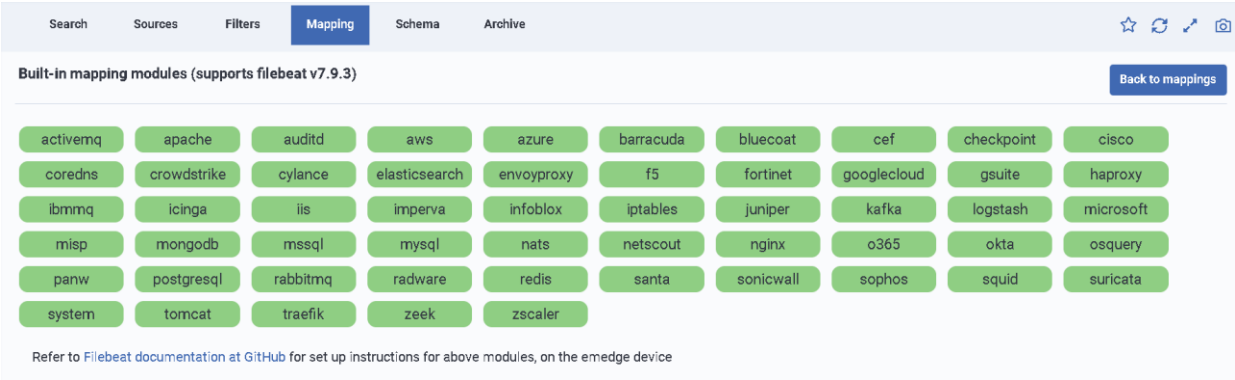
A variety of log sources are supported, including syslogs from network, security devices, servers, on-prem and cloud.

Instructions are provided in the software on how to configure the devices to send logs to NetGain.



- Efficient log mapping using Filebeats and GROK

Log mapping is the process of putting different log data into standard fields so that logs can be treated intelligently, can be manipulated, and logs from different systems can be correlated. The solution comes out-of-the-box with support for more than 50 vendors and device types. For any other brands which are not currently supported, the user can use GROK function to map the logs.



- Mapping to the Elastic Common Schema (ECS)

NetGain uses Elasticsearch as the underlying database, and Filebeats as the primary tool to collect and map the logs. Filebeats is community-created to support the latest devices. The logs are mapped to Elastic Common Schema.

- Intelligent search, query and correlation

The module comes with an intelligent search capability that provides search suggestions as you type. The query is lightning fast even with a large data set. The search allows correlation of the data and the results are shown on screen or can be downloaded as a report.

The GUI also allows the user to select and zoom into the time period as needed.

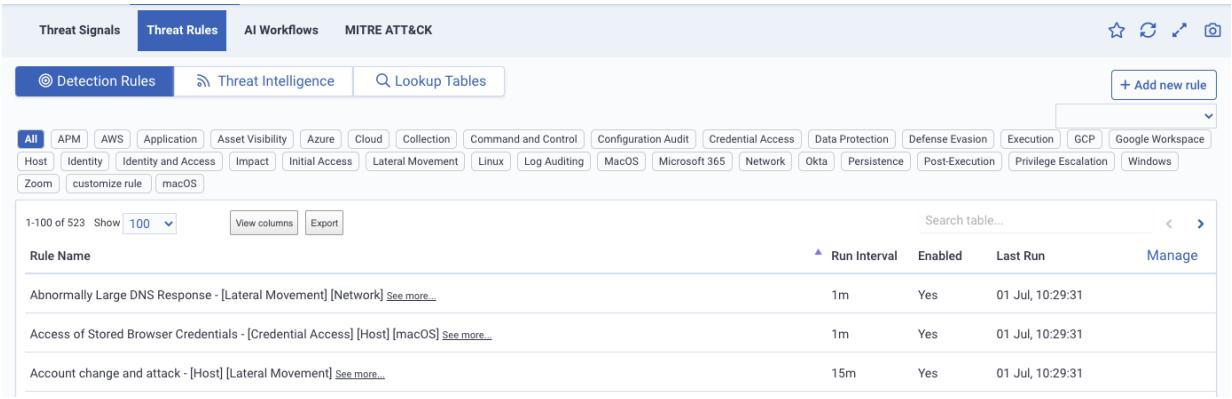
Security Analytics

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. Security Analytics is built on top of Log Analytics.

After the logs are collected, and mapped into a centralized file, they are run against hundreds of pre-built automatic threat detection rules, including security use cases, anomaly detection algorithms and real-time correlation policies. The module rapidly identify known and potential threats, provides alerts and notifications, and reports for compliance.

- Threat rules

The solution comes out-of-the-box with more than 500 threat rules. These rules follow the MITRE ATT&CK framework which is an industry body that documents known attacks globally. New rules are constantly updated by NetGain, and the user may also create threat rules using query, python script, or an innovative Advance Intelligence Workflow with minimal coding.



- Integration to third-party threat intelligence

The solution can be integrated to external threat intelligence information from trusted sources. The user can add more sources as needed. Examples of such threat intelligence include blacklists for compromised IP addresses, domain names, or other similar information.

- Intelligent search, query and correlation

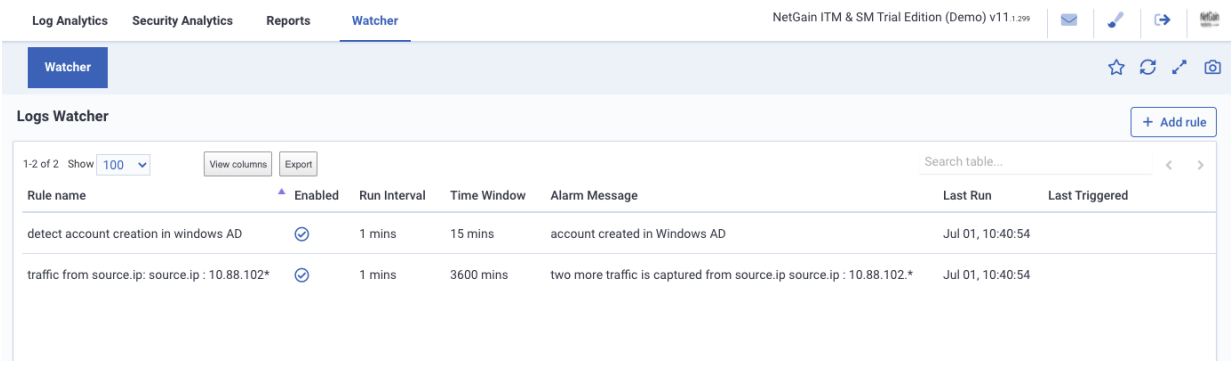
For the security analyst, once a threat is detected by the system, he or she must be able to investigate the threat quickly and accurately. The powerful search and query function allows for lightning fast performance even with a large data set. The search allows correlation of the data and the results are shown on screen or can be downloaded as a report.

- Watcher

The Watcher feature allows the user to set a query based on key words or phrases, and the system will alert the operation staff once the query is triggered.

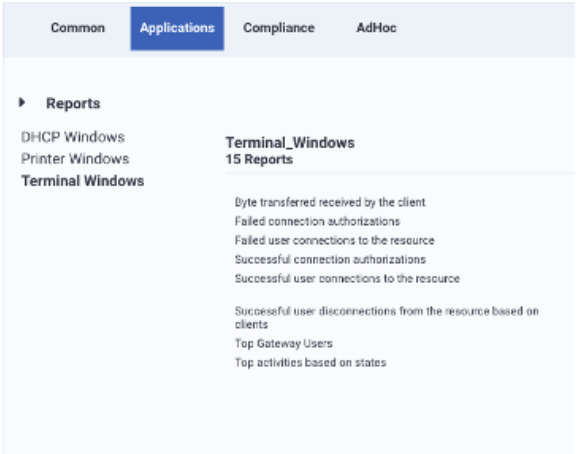
NetGain systems

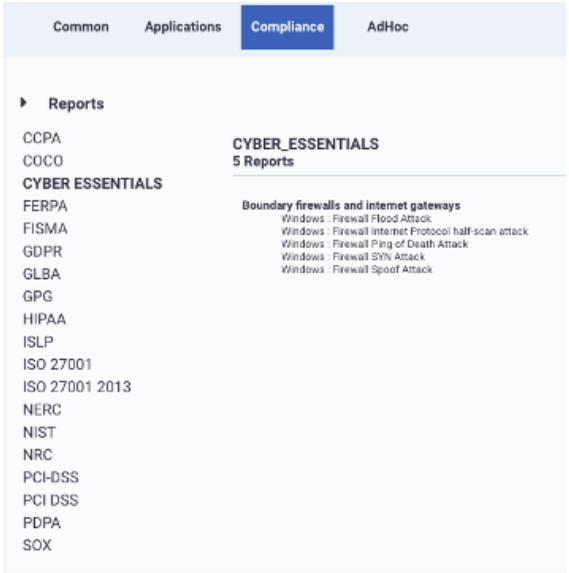
Maximize uptime. Develop insights. Provide answers.



- Reports

There are hundreds of standard reports that are configurable so the user can always get the report that he or she needs. Compliance reports for standard compliance such as HIPAA, are also available out-of-the-box. Adhoc reports can also be created by the user.





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 hardware requirements for a given IT environment. Please contact NetGain on the 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	Quad Core
RAM	16GB
Operating System	CentOS
Browsers Supported	Firefox, Google Chrome, Safari, Microsoft Edge.

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.