NetGain Security Analytics Datasheet

The IT security landscape is ever evolving. 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.

While enterprises may invest in security solutions such as firewalls and malware detection software, there is never a 100% guarantee that a hacker cannot penetrate the enterprise network. As such, more and more IT departments are turning to SIEM (Security Information and Event Management) to catch abnormal behaviour and potential threats inside the enterprise.

By analyzing log data from multiple sources in their IT infrastructure created by events and activities, SIEM identifies such threats in real-time and alerts the security ops team of such threats.

SIEM is also a useful tool for forensics, to interrogate historical data to determine any past attacks or if there is a pattern to attacks.

NetGain Security Analytics

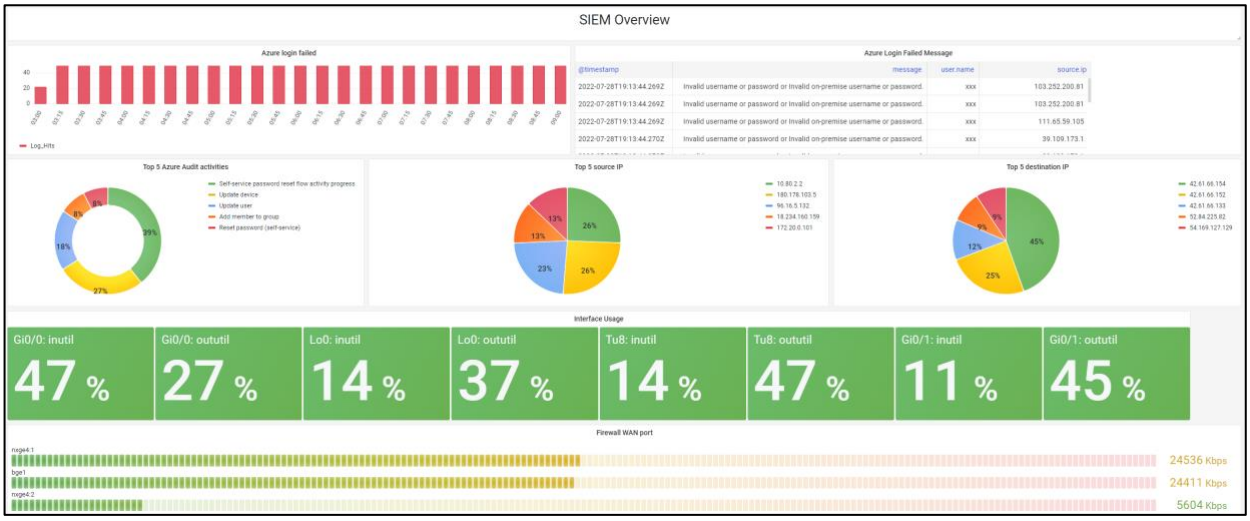
Implementing a SIEM solution does not have to be a complex and expensive affair. Like any other SIEM solution, NetGain Security Analytics will improve the visibility of your organization's overall security and identify threats to your IT infrastructure by correlating the different events from the log data that constitute a threat.

Unlike most other SIEM solutions, NetGain Security Analytics 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 Security Analytics solution comprises two functions:

- Log Analytics, which provides log ingestion, powerful query capabilities, Watcher and Reports
- Security Analytics, which also provides security threat hunting capabilities

NetGain Security Analytics is available as both an on-premise software or as a SaaS offering.



Key Features

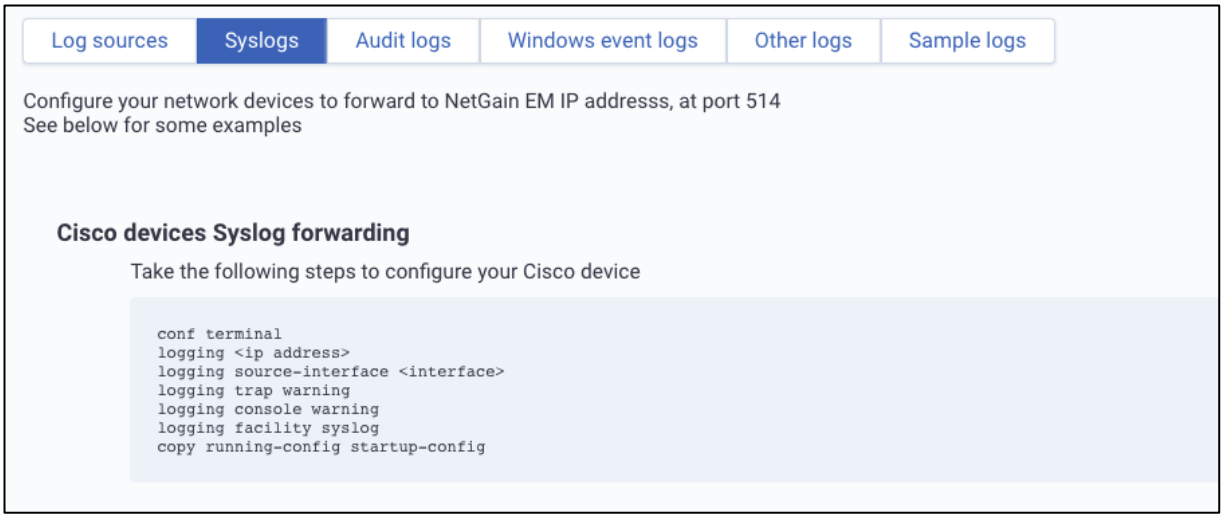
Log Analytics

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 Filebeat 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 vendors and device types. For any other brands which are not currently supported, the user can use GROK function to map the logs.

The following are the out-of-the-box supported vendors:

activemq	apache	auditd	aws	awsfargate	azure	barracuda	bluecoat
cef	checkpoint	cisco	citrix	coredns	crowdstrike	cyberark	cyberarkpas
cylance	elasticsearch	envoyproxy	f5	fortinet	gcp	google_workspace	googlecloud
gsuite	haproxy	ibmmq	icinga	iis	imperva	infoblox	iptables
juniper	kafka	logstash	microsoft	misp	mongodb	mssql	mysql
mysqlenterprise	nats	netscout	nginx	o365	okta	oracle	osquery
panw	pensando	postgresql	proofpoint	rabbitmq	radware	redis	santa
snort	snyk	sonicwall	sophos	squid	suricata	symantec	system
threatintel	tomcat	traefik	zeek	zookeeper	zoom	zscaler	

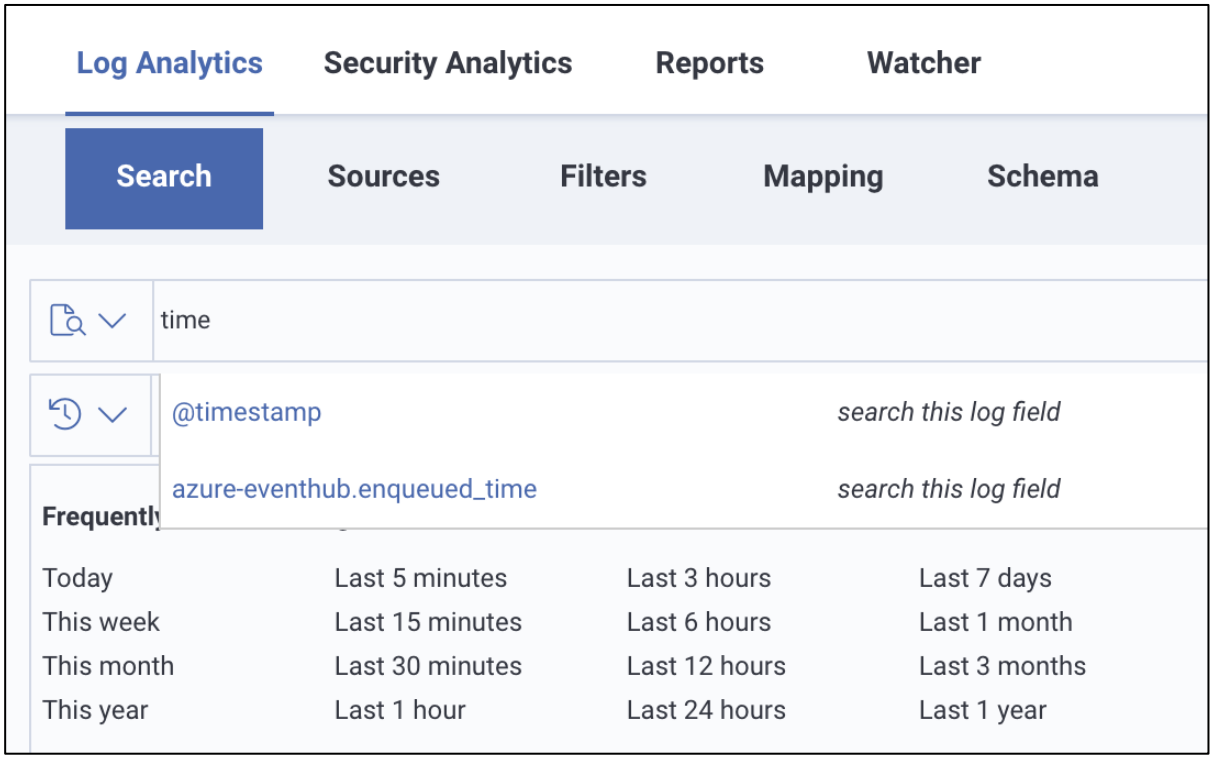
- Mapping to the Elastic Common Schema (ECS)

NetGain uses Elasticsearch as the underlying database, and Filebeat as the primary tool to collect and map the logs. Filebeat 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 close to 700 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.

The following are the threat rule categories:

APM	AWS	Active Directory	Application	Asset Visibility	Azure
Cloud	Collection	Command and Control	Configuration Audit	Credential Access	Data Protection
Defense Evasion	Endpoint Security	Execution	GCP	Google Workspace	Host
Identity	Identity and Access	Impact	Initial Access	Lateral Movement	Linux
Log Auditing	MacOS	Microsoft 365	Network	Okta	Persistence
Post-Execution	Privilege Escalation	Windows	Zoom	cyberarkpas	

- Integration to third-party threat intelligence

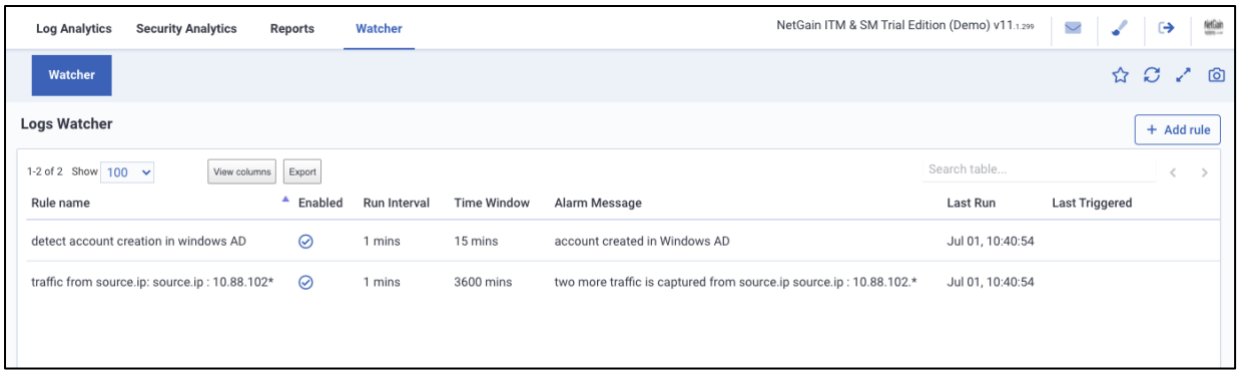
The solution can be integrated to external threat intelligence information from trusted sources. The user can add more sources as needed. Examples of such threat intelligence include blacklists for compromised IP addresses, domain names, or other similar information.

- 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.



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.

Standard compliance reports include:

CCPA	COCO	CYBER ESSENTIALS	FERPA	FISMA
GDPR	GLBA	GPG	HIPAA	ISLP
ISO 27001 2013	NERC	NIST	NRC	PCI DSS
PDPA	SOX			

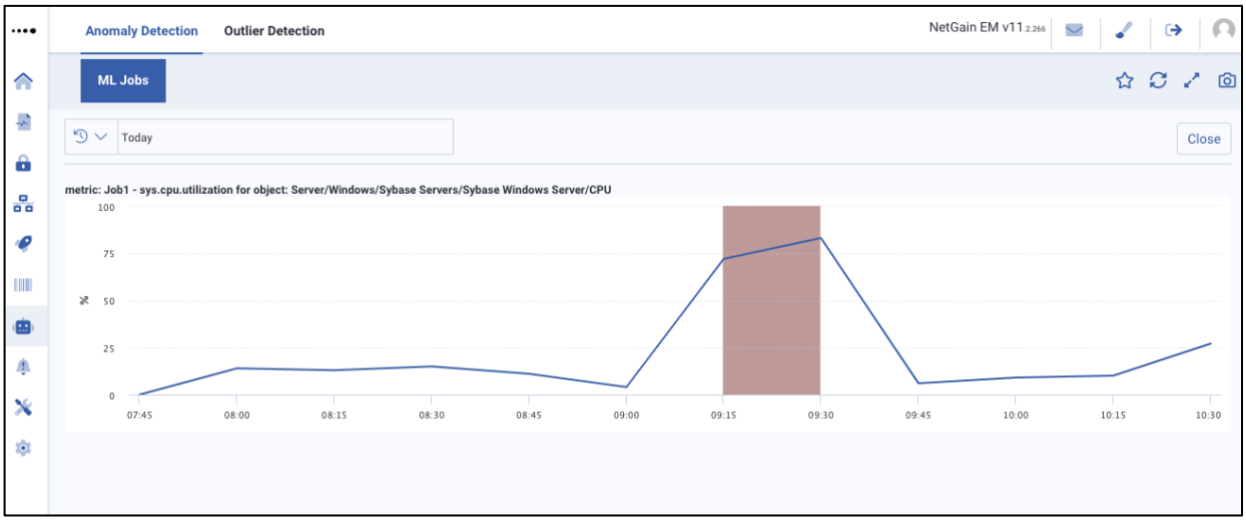
AI Ops

Artificial Intelligence-assisted Operations (AI Ops) is a separate module that uses the logs ingested to perform the following functions:

- **Anomaly detection**

Anomaly detection is the identification of the behavior of IT components that deviate from its normal behavior. An example would be a source IP which sends traffic to a specific server only during office hours. However, if it starts to send traffic to the same server at midnight, this is an anomaly. By using historical data, the AI determines the baseline behavior, and identifies deviation from baseline behavior as it happens. IT ops may also set the sensitivity of the AI detection.

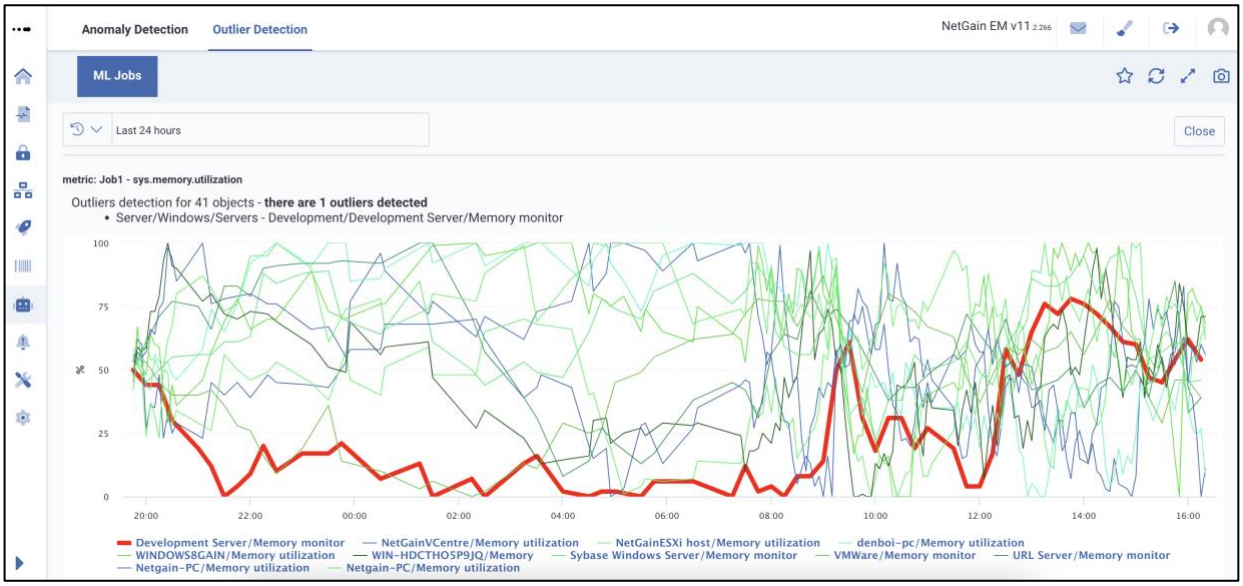
With anomaly detection, IT ops do not need to set static thresholds, and instead rely on the AI to find the thresholds automatically, and then alert the ops team when the anomaly occurs.



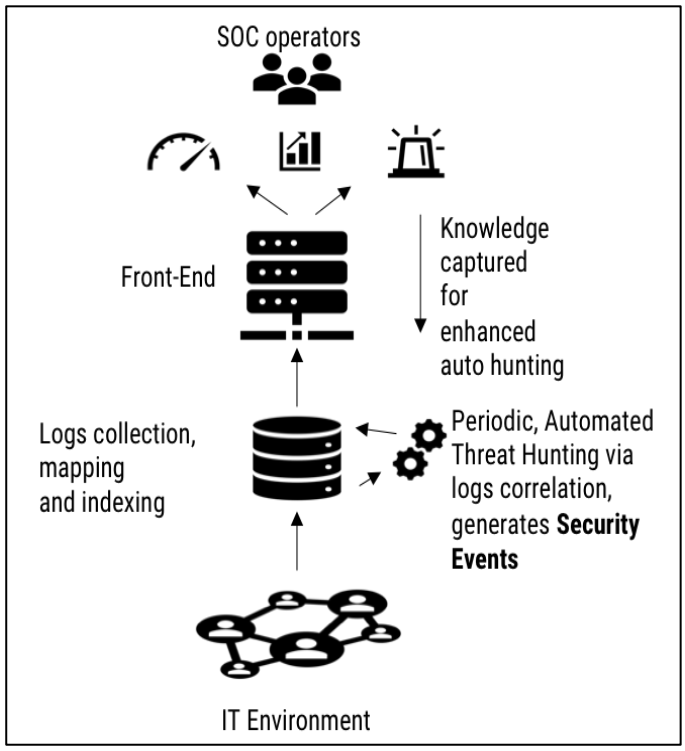
- **Outlier detection**

An outlier is an IT component that deviates drastically from the given norm or average of the data set. An example would be if a set of 20 servers are all sending logs to the system, and one server is sending more logs than the others, then this server would be deemed an outlier. AI is used to identify the outlier in the given data set. IT ops may also set the sensitivity of the AI detection

With outlier detection, the AI is able to find potential issues even if the fault does not exceed the threshold, and is able to alert the IT ops team automatically.



How It Works



Logs are collected and ingested into the NetGain platform. Logs typically come from a variety of IT devices, including security devices, servers and networking devices.

Logs data are normalized using the Elastic Common Schema. This allows the data from different devices to be correlated for analysis.

The user can start to do intelligent search and correlation through user-friendly query interface.

For security analytics, the logs are automatically run against the threat rules. Any threats identified are alerted to the IT ops team.

Deploying NetGain Security Analytics

NetGain Security Analytics 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 Security Analytics 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.

System Requirements

The requirements for running and operating NetGain **Security Analytics** 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 **Security Analytics** 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 7, RHEL 8 or equivalent
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 continues to develop its business as it evolves from IT monitoring to IT observability. It has established local teams throughout the Asia Pacific Region, including Australia, China and Singapore.

Regardless of location, type, size, or complexity, our solutions give our customers the power to observe their IT infrastructure, services, applications and devices with ease, all from a single management dashboard, to achieve operational excellence with reduced complexity and gain useful insights to improve business outcomes.

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