NetGain
systems

Maximize uptime. Develop insights. Provide answers.

NetGain SIEM

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.

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.

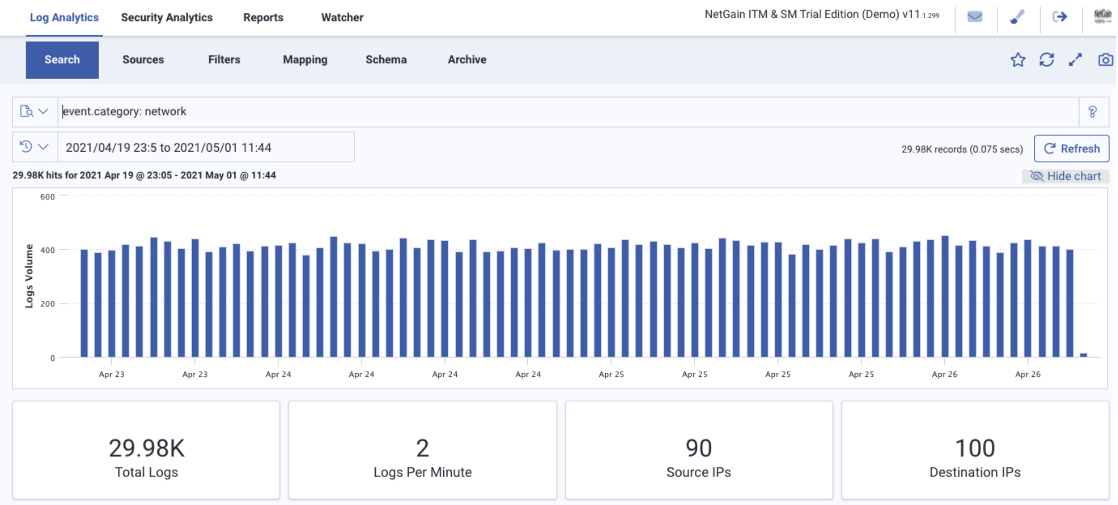
Unlike most other SIEM solutions, NetGain SIEM simplifies how SIEM is deployed and used to put it within reach of organizations with smaller IT departments, yet has the flexibility and scalability to be used by larger and more demanding organizations looking to reduce the complexity in managing their IT security operations.

The NetGain SIEM solution comprises two modules:

- Log Analytics
- Security Analytics

NetGain
systems

Maximize uptime. Develop insights. Provide answers.



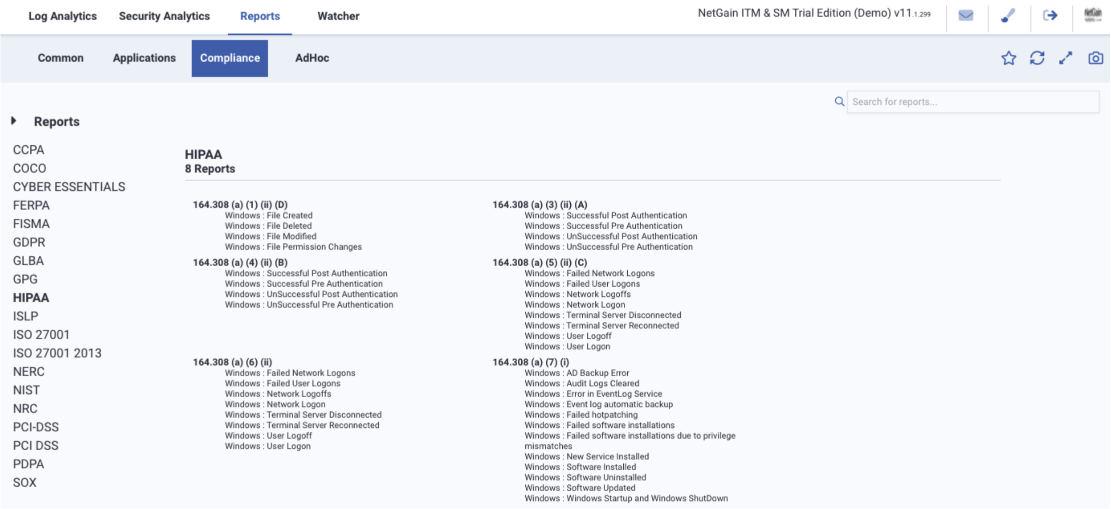
event.category: network

2021/04/19 23:5 to 2021/05/01 11:44

29.98K records (0.075 secs)

29.98K hits for 2021 Apr 19 @ 23:05 - 2021 May 01 @ 11:44

29.98K Total Logs	2 Logs Per Minute	90 Source IPs	100 Destination IPs



Reports

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

HIPAA
8 Reports

164.308 (a) (1) (ii) (D)
Windows : File Created
Windows : File Deleted
Windows : File Modified
Windows : File Permission Changes

164.308 (a) (4) (ii) (B)
Windows : Successful Post Authentication
Windows : Successful Pre Authentication
Windows : UnSuccessful Post Authentication
Windows : UnSuccessful Pre Authentication

164.308 (a) (6) (ii)
Windows : Failed Network Logons
Windows : Failed User Logons
Windows : Network Logoffs
Windows : Network Logon
Windows : Terminal Server Disconnected
Windows : Terminal Server Reconnected
Windows : User Logoff
Windows : User Logon

164.308 (a) (3) (ii) (A)
Windows : Successful Post Authentication
Windows : Successful Pre Authentication
Windows : UnSuccessful Post Authentication
Windows : UnSuccessful Pre Authentication

164.308 (a) (5) (ii) (C)
Windows : Failed Network Logons
Windows : Failed User Logons
Windows : Network Logoffs
Windows : Network Logon
Windows : Terminal Server Disconnected
Windows : Terminal Server Reconnected
Windows : User Logoff
Windows : User Logon

164.308 (a) (7) (i)
Windows : AD Backup Error
Windows : Audit Logs Cleared
Windows : Error in EventLog Service
Windows : Event log automatic backup
Windows : Failed hotpatching
Windows : Failed software installations
Windows : Failed software installations due to privilege mismatches
Windows : New Service Installed
Windows : Software Installed
Windows : Software Uninstalled
Windows : Software Updated
Windows : Windows Startup and Windows ShutDown

BENEFITS

1

Simplified Operations

NetGain SIEM has an easy-to-use and understand Graphical User Interface (GUI). While it can be used as a stand-alone solution, NetGain SIEM interface is integrated with that of NetGain Enterprise Manager (EM), providing you with a single pane of glass from which to manage both IT infrastructure and security events.

2

Powerful Performance

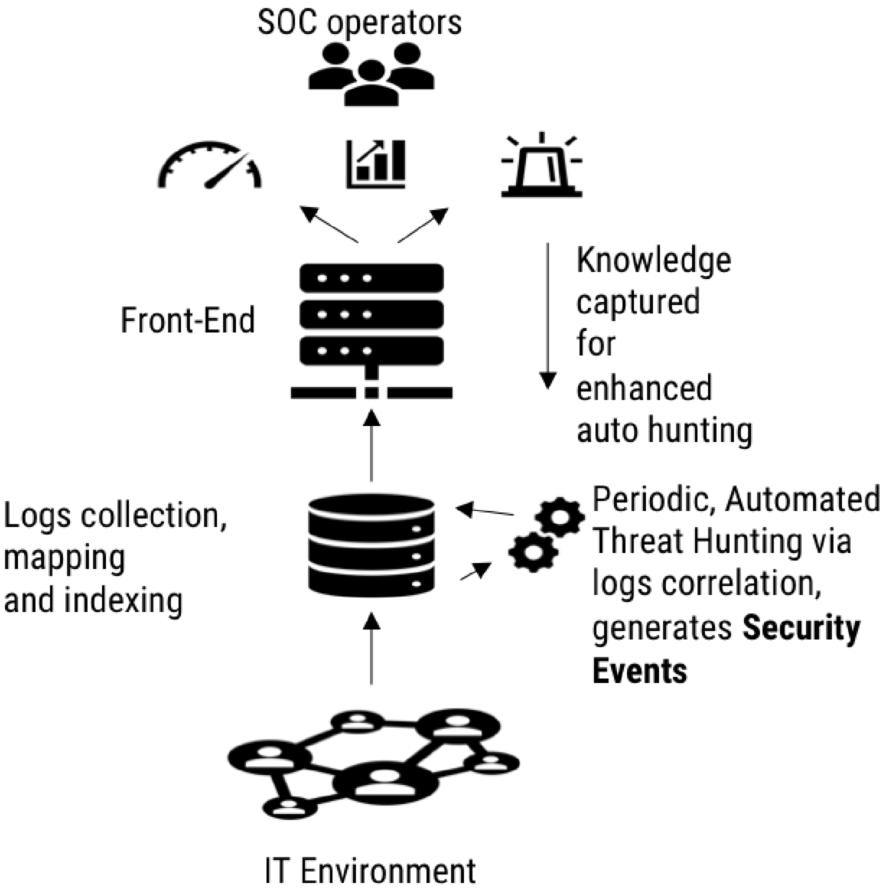
NetGain SIEM can ingest and aggregate all kinds of log data from many different devices. It has excellent query performance and can return a query within millions of logs in less than a second. It also has a powerful auto-threat hunting tool to let you co-relate seemingly innocent stand-alone events across different sources to identify any potential threat.

3

Fully customizable

While it is aligned with ECS and the MITRE ATT&CK framework, you can easily add and redefine the events that constitute a security threat, allowing you to customize NetGain SIEM to handle threats specific to your industry or organization, and to suit the security posture of your organization. This also allows it to remain relevant in the ever-changing threat landscape.

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

KEY FEATURES

1

Comprehensive and efficient log ingestion and mapping

NetGain SIEM supports a variety of log sources, including syslogs from network, security devices, servers, on-prem and cloud. Logs are mapped into standard fields to facilitate analysis and correlation. More than 50 vendors are supported comes out-of-the-box and new devices can be mapped through Filebeats GROK function.

2

Threat rules, threat intelligence, threat investigations

The solution comes out-of-the-box with more than 500 threat rules that follow the MITRE ATT&CK framework. New rules can be created using query, python script, or an innovative Advance Intelligence Workflow with minimal coding. Integration to third-party threat intelligence sites is supported. Threat investigations are facilitated with a powerful and fast search query and correlation capabilities.

3

Reports and compliance

NetGain SIEM come with 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, GDPR, SOX etc. are also available out-of-the-box. Adhoc reports can also be created by the user. Reports can be scheduled to run automatically in batch mode and sent to the user.

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.