NetGain systems

Maximize uptime. Develop insights. Provide answers.

NetGain SIEM (Security Information and Event Management)

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.

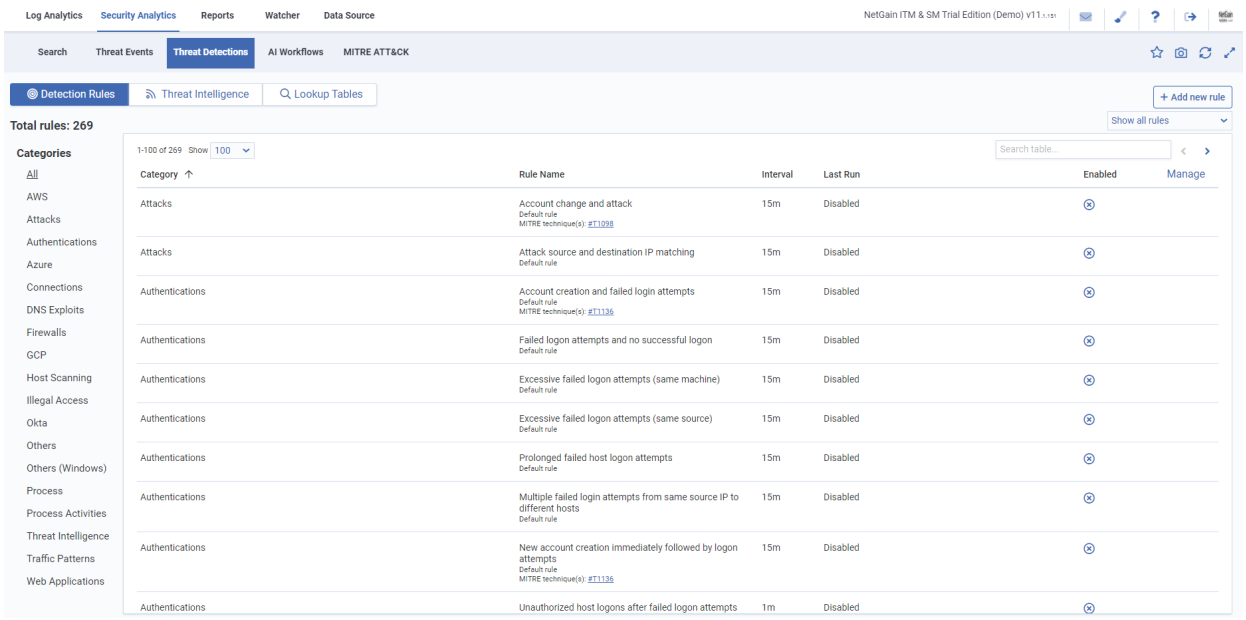
NetGain systems

Maximize uptime. Develop insights. Provide answers.

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.

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's 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. NetGain SIEM also has an Advanced Intelligence Workflow tool which simplifies the creation of a new threat rule by letting you create a visual workflow to easily implement the required detection logic without writing a single line of code.

2

Powerful Performance

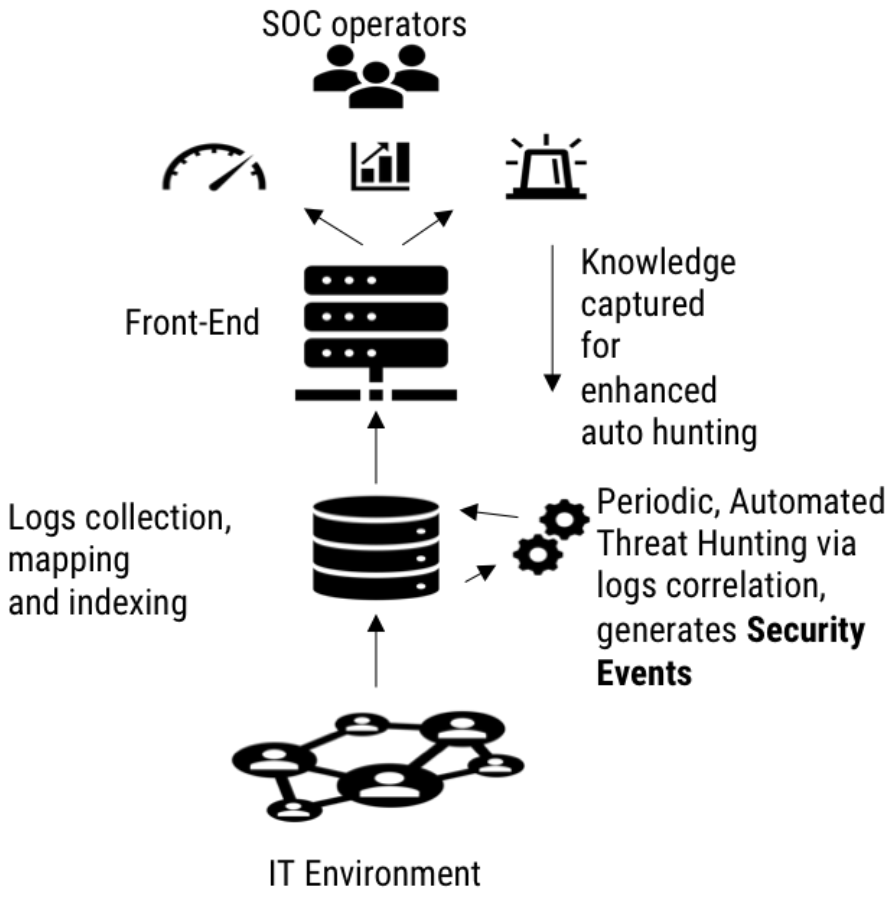
NetGain SIEM can ingest and aggregate all kinds of log data from many different devices. It has excellent query performance and can return a query within millions of logs in less than a second. It also has a powerful auto-threat hunting tool to let you co-relate seemingly innocent stand-alone events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

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.