SolarWinds Security Event Manager

Author, Dr.Barakkath Nisha.U

A Data Science Foundation Blog

October 2021

---

www.datascience.foundation

Data Science Foundation
Data Science Foundation, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ
Tel: 0161 926 3670 Email:admin@datascience.foundation Web: www.datascience.foundation
Registered in England and Wales 4th June 2015, Registered Number 9624670

Overview

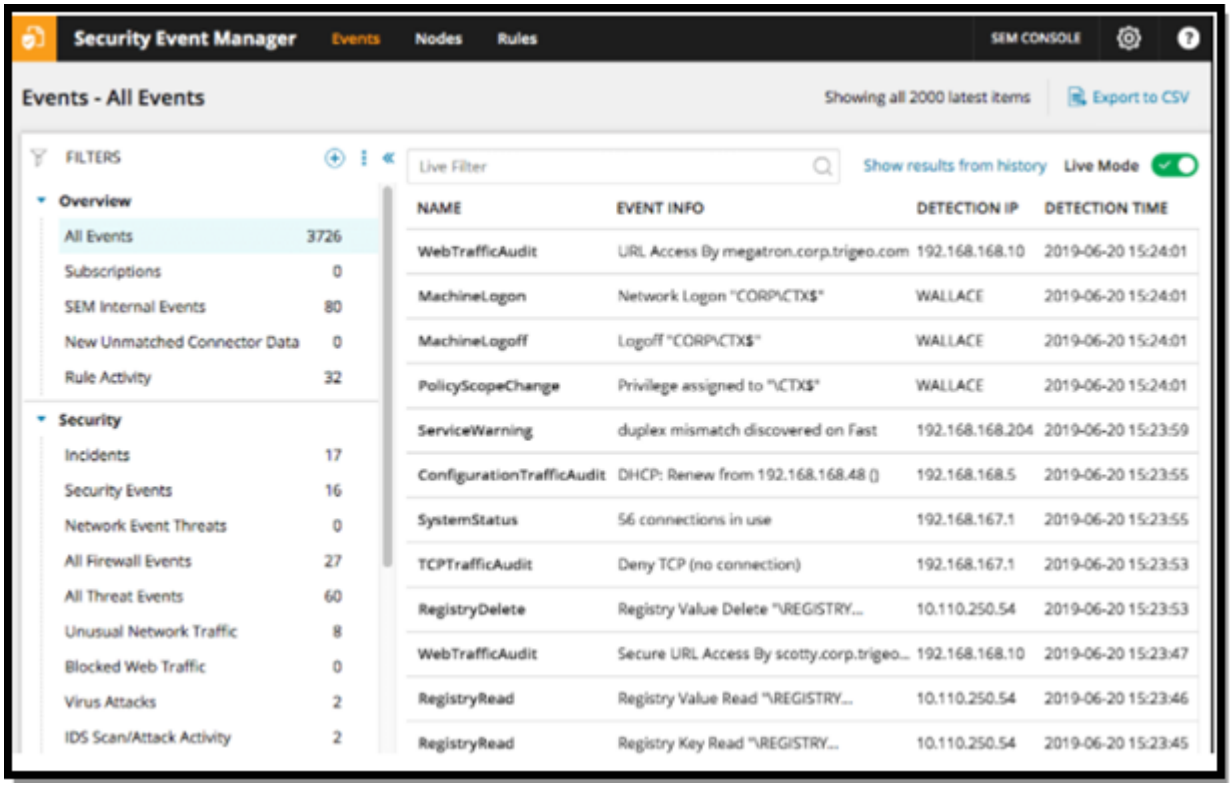
SolarWinds Security Event Manager (SEM) takes a highly intelligent approach to threat detection.

By collecting network intrusion detection system logs, SEM collates information on attack types and amounts. This information is then integrated with other infrastructure logs, creating a vast network of data to contribute to threat detection. This data is constantly optimizing the security systems and processes of our Intrusion Detection System(IDS).

With SEM, we can identify problematic devices on the network, use the data to create risk assessment reports for stakeholders, and identify highly advanced threats before they create a massive damaged situation to our system.

Working Process

As is clear from overview, manual network intrusion detection can be exhausting. And no matter how hard we work; the system will never be entirely fool proof. We were in a race against constantly evolving threats and managing them manually is an uphill battle



SEM uses native technology to save us time that would otherwise be spent performing routine tasks. It does this by monitoring and alerting us to any suspicious events or activities, and by acting automatically when specific events are detected.

It deploys network sensors to assist with detecting intrusions, conducts data analysis, identifies services being consumed, and automates. By automating the process wherever possible, these capabilities reduce the need for us to manually detect and respond to threats and suspicious activity.

SolarWinds security event management features:

1. Advanced pfsense Firewall log analyser
2. APT security for advanced persistent threat defence.
3. Centralized log management.
4. Compliance Reporting feature.
5. File integrity monitoring system. Etc.

SEM not only centralizes and collects logs, but it also helps correlate important events, provides advanced searching features, and even takes automatic action against threats, all in

real-time.

This full range of functions is referred to as SIEM—Security Information and Event Management—and it provides a powerful way to manage events on any network.

Events are processed in real-time and in memory, meaning they don't need to be written to a database and then queried before the system can identify problems.

Response is incredibly fast, though obviously higher log volumes could lead to slower processing depending on how powerful your server is.

SolarWinds calls this "Active Response," and SEM includes a large library of possible responses to common situations. You can automate actions like:

- Quarantine infected machines, or force shutdowns and restarts
- Block IP addresses.
- Disable user accounts.
- Kill processes.
- Restart or stop services
- Force user log-off
- Reset passwords

Encounter security breaches in real-time

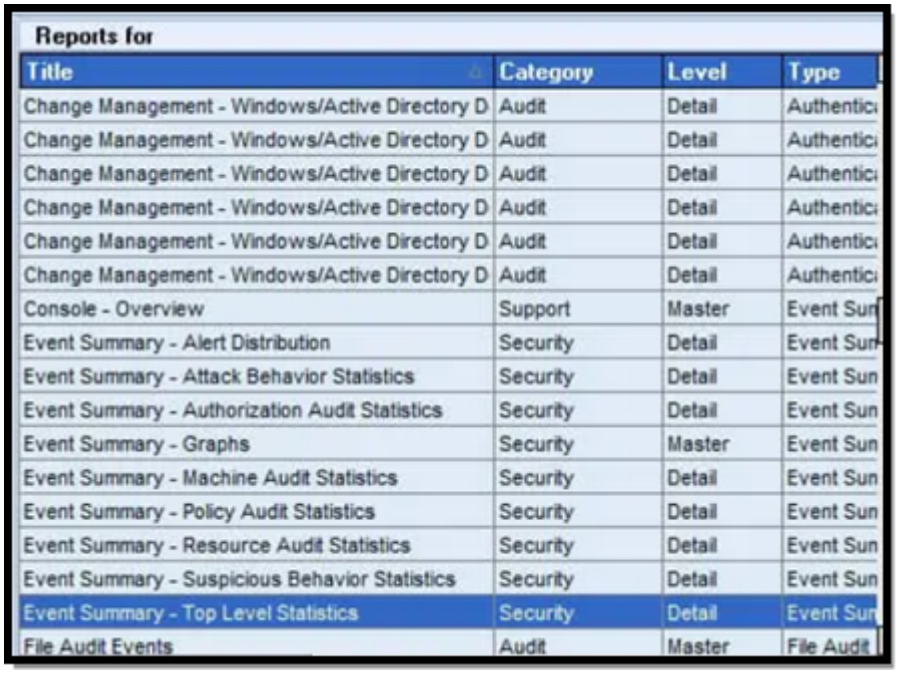
SolarWinds LEM's Vulnerability management skills (now known as SEM) can still empower your IT team to respond to potential threats rapidly by automating result of discussions. Log & Event Manager (LEM) was an all-in-one SIEM tool IT and security pros used to simplify detecting and investigating security issues using event log data. To fill your cybersecurity needs, we have released a brand-new SIEM, SolarWinds Security Event Manager (SEM).

A unified view of security event logs and effective event correlation across your network are designed to simplify and accelerate threat mitigation.

SolarWinds SEM monitors file integrity (FIM) and USB devices from start to finish to detect any suspicious user activity.

To combat such threats, you can set up automated responses such as blocking IP addresses, changing privileges, disabling accounts, and configuring alarms to alert you of potential security breaches in real time.

Reporting:



Reports for

Title	Category	Level	Type
Change Management - Windows/Active Directory D	Audit	Detail	Authentic
Change Management - Windows/Active Directory D	Audit	Detail	Authentic
Change Management - Windows/Active Directory D	Audit	Detail	Authentic
Change Management - Windows/Active Directory D	Audit	Detail	Authentic
Change Management - Windows/Active Directory D	Audit	Detail	Authentic
Change Management - Windows/Active Directory D	Audit	Detail	Authentic
Console - Overview	Support	Master	Event Sun
Event Summary - Alert Distribution	Security	Detail	Event Sun
Event Summary - Attack Behavior Statistics	Security	Detail	Event Sun
Event Summary - Authorization Audit Statistics	Security	Detail	Event Sun
Event Summary - Graphs	Security	Master	Event Sun
Event Summary - Machine Audit Statistics	Security	Detail	Event Sun
Event Summary - Policy Audit Statistics	Security	Detail	Event Sun
Event Summary - Resource Audit Statistics	Security	Detail	Event Sun
Event Summary - Suspicious Behavior Statistics	Security	Detail	Event Sun
Event Summary - Top Level Statistics	Security	Detail	Event Sun
File Audit Events	Audit	Master	File Audit

SolarWinds has included a powerful reporting engine with Security Event Manager. Over 300 built-in reports can help with everything from graphical summaries of activity, to detailed threat reporting and compliance.

Summary

Network intrusion detection software is only as good as its console. SEM, despite offering some seriously advanced utilities, is one of the most user-friendly programs on this list. Its interface is simple, with events, nodes, and rules accessible.

About the Data Science Foundation

The Data Science Foundation is a professional body representing the interests of the Data Science Industry. Its membership consists of suppliers who offer a range of big data analytical and technical services and companies and individuals with an interest in the commercial advantages that can be gained from big data. The organisation aims to raise the profile of this developing industry, to educate people about the benefits of knowledge based decision making and to encourage firms to start using big data techniques.

Contact Data Science Foundation

Email: admin@datascience.foundation
Telephone: 0161 926 3641
Atlantic Business Centre
Atlantic Street
Altrincham
WA14 5NQ
web: www.datascience.foundation