Mi6Research is a market intelligence and advisory firm helping clients understand technology and market trends to develop insightful business strategies.

Mi6 Research
Actionable Business Insights

MI6RESEARCH PAPER

12/21/2015

SIEM

INTRODUCTION TO SECURITY INFORMATION AND EVENT MANAGEMENT - SIEM

By Feisal Mosleh

T

Mi6Research Paper

SECURITY INFORMATION AND EVENT MANAGEMENT - SIEM

Introduction

Today's IT infrastructures are creating tough new challenges for business and IT leaders. IT services are being delivered across an increasingly fragmented combination of physical, virtual and cloud environments. These services are being accessed in an always on world, from an ever increasing number of locations, both fixed and mobile, and on a growing variety of devices. As a result, organizations struggle to manage the growing complexity and risk and the mounting attacks from cyber criminals.

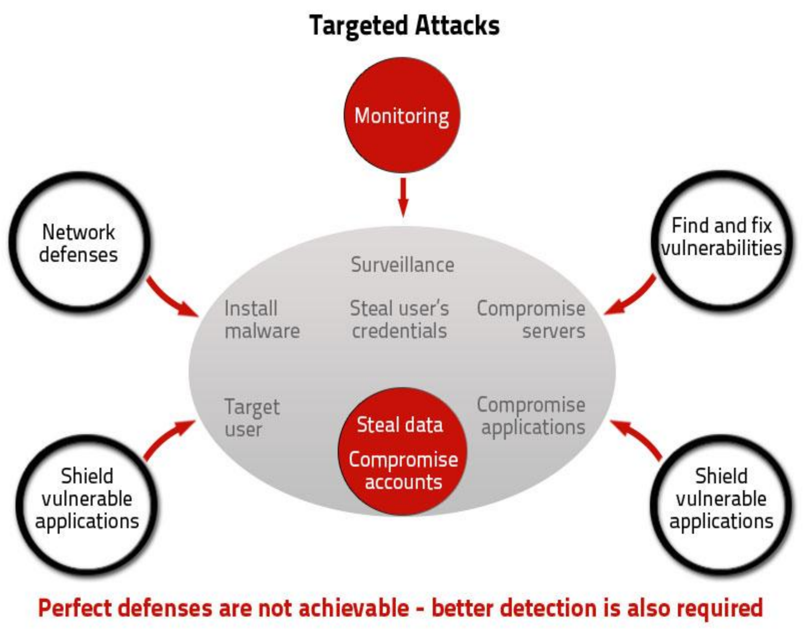
As cyber security incidents increase and hacking activities proliferate, enterprises are deploying more and more dedicated security tools, from biometric scanners to dedicated firewalls to authentication, authorization and encryption products across the whole enterprise landscape. This has resulted in a ton of incoming data, logs and alerts causing the security operations team to be overwhelmed.

By implementing Security Information and Event Management (SIEM), the process of collecting, sorting through, reporting and prioritizing security events is automated and managed such that the security team may respond to the most important, urgent issues in a more insightful and timely manner. Detailed reporting is provided to support the enterprise obligations to comply with regulations such as HIPAA, PCI-DSS[1], FISMA[2] and others. Data is correlated, alarms are appropriately signaled and lots of information is stored for later retrieval in a relatively easy manner.

In this paper we outline SIEM and a few of the more capable SIEM players to serve as a brief introduction to the SIEM market.

[1] The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards

[2] The Federal Information Security Management Act of 2002 - requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information, information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.



SIEM used to comprise two separate products: Security Event Management (SEM) and Security Information Management (SIM). It was originally developed as a compliance management tool which would centralize, review, and report on disparate log activity. The ability to correlate logs was developed further to provide threat detection and advanced intelligence to investigate security events and IT systems more closely. Initially large enterprises needed SIEM the most. Over time, SIEM products started integrating with other security products to give a more holistic view of the organizations security and send out commands and data to other systems.

The SIEM market has been around for about a decade and continues evolving as the market matures. The threats and regulatory landscape makes SIEM a very attractive solution especially as specialized correlation and analytics, dashboard features are productized. A good SIEM system will highlight threats and vulnerabilities as well as threats in real time providing a powerful insight into your strategic and tactical state of enterprise security.

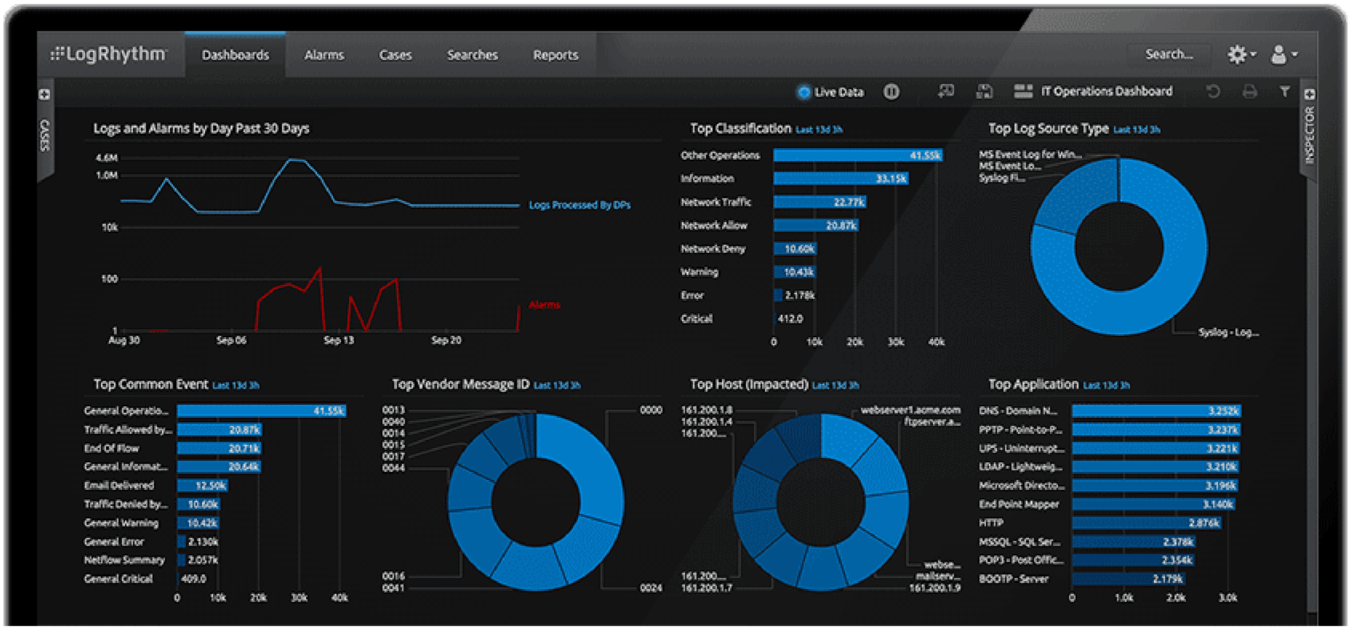
The SIEM Players

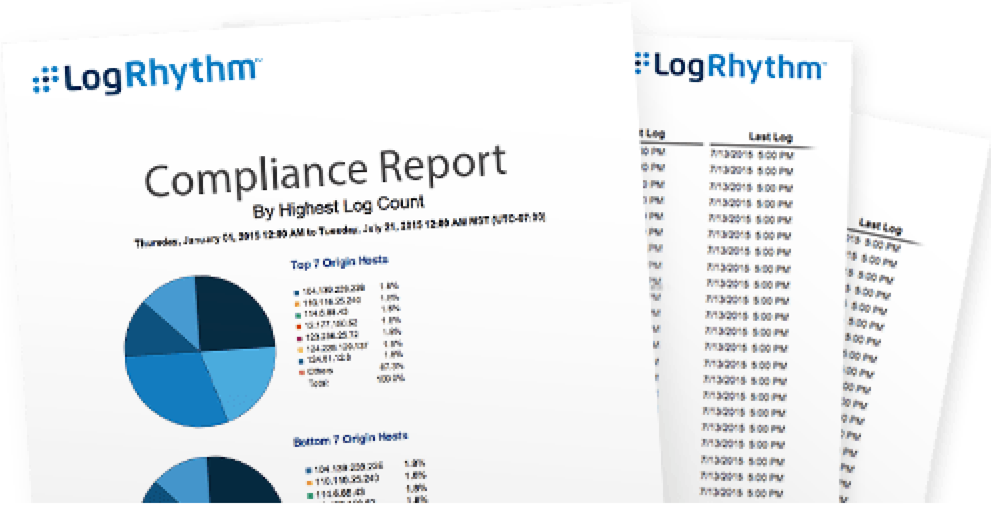
Below we discuss three of the more compelling SIEM players to provide an understanding of what matters in SIEM.

LogRhythm

LogRhythm, founded in 2003, and based in Boulder CO, with about 450 employees is a dedicated SIEM security vendor that provides simplified monitoring and management with improved usability and advanced analytics. The intent is to unify SIEM, log management, security analytics, forensics and network and endpoint monitoring.

As such it is a comprehensive solution at the higher end of the spectrum with many features and capabilities.





Cost

$$ Reasonable

The TCO calculated for a 3 year period is approximately in the $65k to $100k range.

Suited to

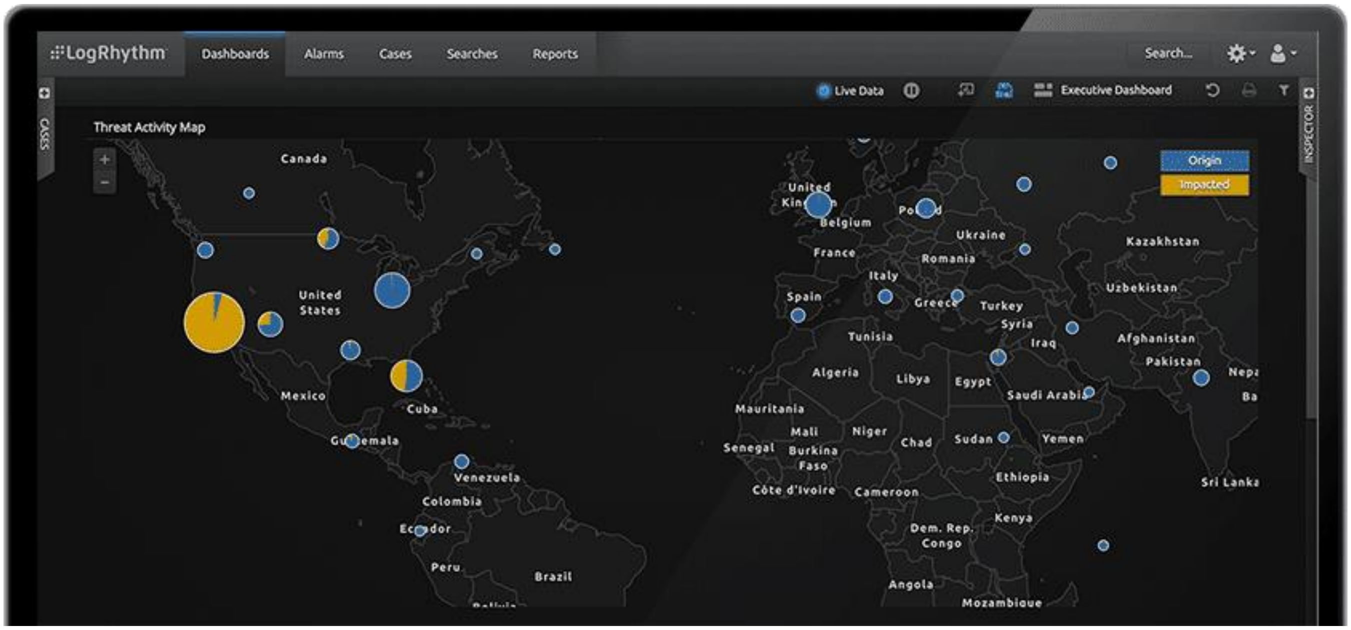
Smaller and medium sized enterprises with minimal security staff

Strengths:

- Fully featured yet easy to deploy and use
- Being a focused SIEM solution, LogRhythm is dedicated to enhancing their platform and making it work across a multi-vendor security landscape and become best in class.
- A recent feature called the Identity Inference Engine can infer missing identity information from an analyzed data event.
- Advanced Intelligence Engine provides advanced correlation and pattern recognition
- SIEM, log management, machine analytics provide enhanced manageability and visibility to threats.

Weaknesses

- The key strength of focus is also a weakness, as LogRhythm does not provide an array of security products that would make them a strategic vendor to a large enterprise



Bottom Line:

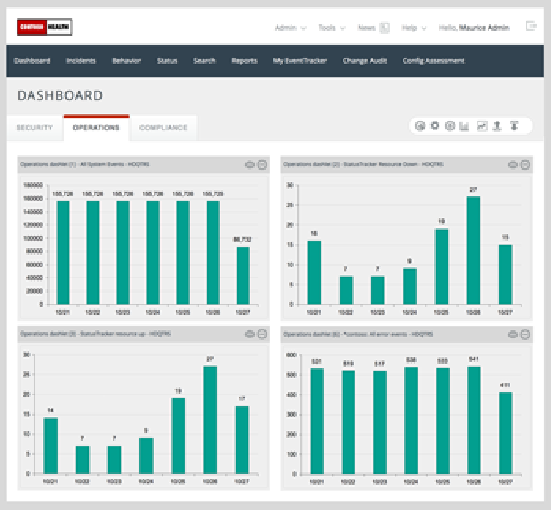
If you need a dedicated SIEM platform to manage multiple security nodes of information then LogRhythm performs very well with comprehensive analytics and monitoring at a very reasonable cost of ownership.

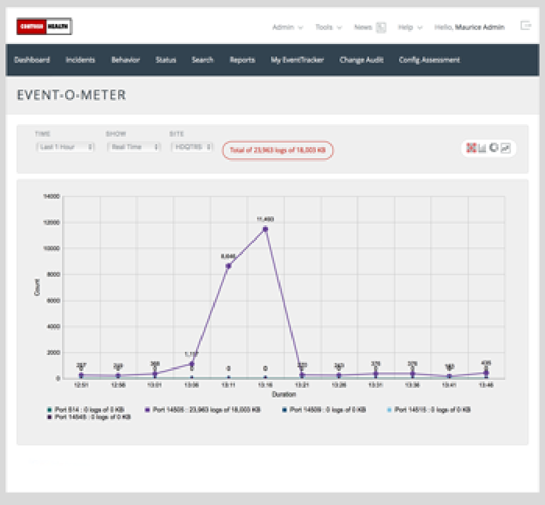
EventTracker

Founded in 2000, EventTracker is based out of Columbia MD with about 100 employees. EventTracker is focused on small to medium sized enterprises that have minimal IT and security staff. Their focus is on providing a complete solution for SIEM, IT Compliance audit, Log Management Tool, IT Security and System monitoring. One area of strength is the ability to provide a comprehensive security compliance solution. This is particularly of benefits to healthcare companies, finance, clinics, hospitals and the like.

Some of the recently added features in EventTracker Enterprise include

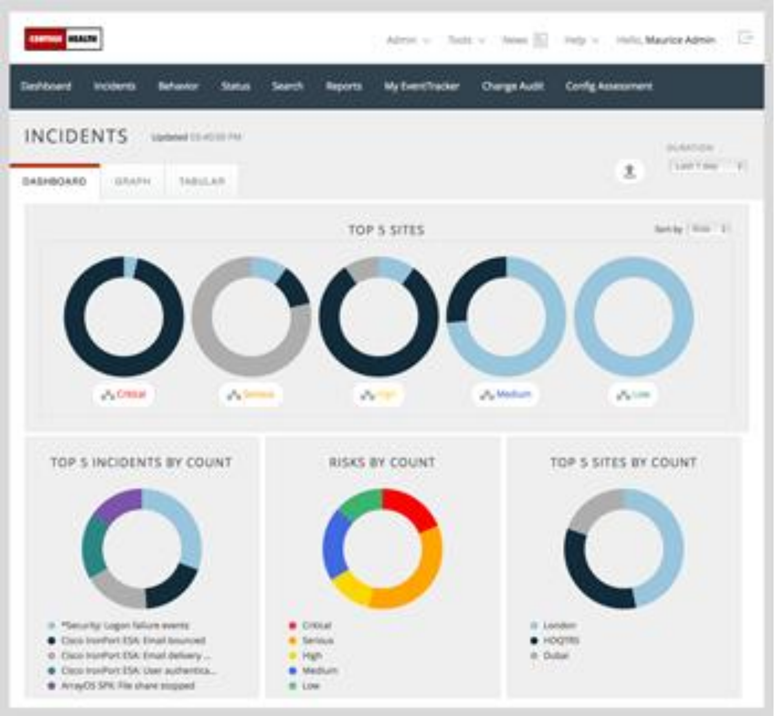
- A dashboard that highlights attackers and targets, to pinpoint the 4 Ws (who, what, when, where)
- Ability to detect unusual login places with User Logon Affinity feature
- Unknown process detection – report by signature, publisher, MD5 Hash
- Deeper integration with more threat intelligence sources
- Host level capabilities – to identify parent processes, host artifacts





EventTracker is now offering SIEM-as-a-service where your data and locations are monitored by EventTracker experts. This is a particularly strong offering for resource challenged smaller businesses which can use the SaaS model to expense their SIEM costs and allow precious IT resources to focus on other strategic issues.

In **SIEM Simplified**^{SM} EventTracker's staff assume responsibility for all SIEM related tasks including daily incident reviews, daily/weekly log reviews, configuration assessments, incident investigation support and audit support.



Cost

$$ Reasonable

The TCO calculated for a 3 year period is approximately in the $50k to $100k range.

Suited to

Smaller and medium sized enterprises with minimal security staff

Strengths:

- Targeted towards SMBs and delivers good feature range that's easy to manage and use.
- New SIEM-as-a-service offering goes a step further to enable resource challenged SMBs
- EventTracker Enterprise has built-in monitoring and reporting for FDCC, FFIEC, FISMA, GLBA, HIPAA, NERC, NISPOM, PCI-DSS and Sarbanes-Oxley (SOX 404)
- Updated and easier to use GUI
- EventTracker Enterprise helps to maintain regulatory compliance and simplifies the audit process, reducing audit times by a claimed 'up to 90%'. Detailed reporting helps rapidly identify gaps in compliance requirements, and address them.
- Good capability in prioritizing operational incidents, with real-time alerting, to help address the most critical incidents first.

Weaknesses

- EventTracker is a small private company and its reach is therefore constrained. This is more important for larger, global enterprises but less so for regional SMBs

- As a smaller player, EventTracker may not be able to scale their service offerings to larger enterprises

Bottom Line:

If you are an SMB who needs strong compliance with government regulations then EventTracker is a strong choice. EventTracker is also built for greater ease of use for SMBs at a reasonable price. If you lack IT and security resources then the SIEM-as-a-service offering is a valuable asset to protect your business.

NetIQ

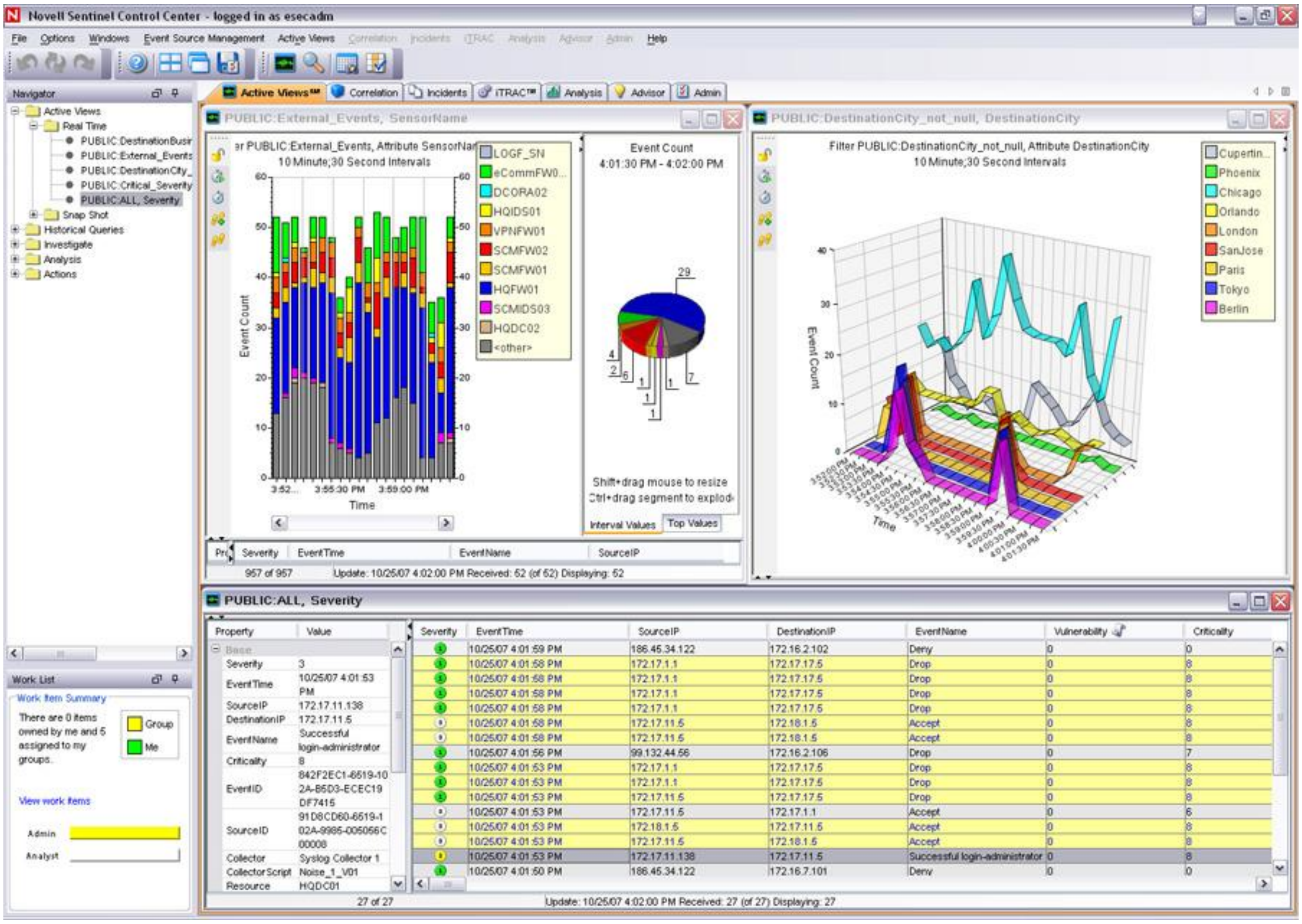
NetIQ, founded in 1995 is an enterprise software company based in Houston, Texas and recently acquired by Micro Focus International[3] (UK). NetIQ provides products for identity and access management, security and data center management. Micro Focus Group, offers a broad portfolio of IT solutions and services. Sentinel Enterprise 7 is a full-featured SIEM solution that simplifies the deployment, management and day-to-day use of SIEM. The focus is on adapting to dynamic enterprise environments and delivering "actionable intelligence" to help security professionals to quickly understand their threat posture and prioritize response.

Sentinel provides a flexible architecture that adapts to almost every environment, which is a boon for security architects looking for a great deal of customizability in a complex enterprise environment. For example, Sentinel's anomaly detection, can automatically identify inconsistencies in the organization's environment without the need to build correlation rules that expect you to know exactly what you are looking for. At installation time, you establish baselines for your organization's specific environment, enabling you to compare

[3] The product portfolios of Micro Focus, Borland, NetIQ, Attachmate and Novell have been brought together under the one portfolio of Micro Focus.

trends and to view historical activity patterns so you can develop models of typical IT activities—or states of normalcy—making it easier to spot potentially harmful trends. Sentinel Enterprise is available as a virtual appliance that can run on hypervisors such as VMware, XENServer, and Hyper-V.

NetIQ and its MicroFocus parent are very strong in the segments of federal, healthcare and cloud services providers. There is a strong compliance capability both in documentation and data management.



There are 0 items owned by me and 5 assigned to my groups.

Property	Value
Base	
Severity	3
EventTime	10/25/07 4:01:53 PM
SourceIP	172.17.11.138
DestinationIP	172.17.11.5
EventName	Successful login-administrator
Criticality	8
EventID	842F2EC1-6519-102A-B5D3-ECEC19DF7415
SourceID	91D8CD60-6519-102A-9985-005056C00008
Collector	Syslog Collector 1
CollectorScript	Noise_1_V01
Resource	HQDC01

27 of 27

Severity	EventTime	SourceIP	DestinationIP	EventName	Vulnerability	Criticality
●	10/25/07 4:01:59 PM	186.45.34.122	172.16.2.102	Deny	0	0
●	10/25/07 4:01:58 PM	172.17.1.1	172.17.17.5	Drop	0	8
●	10/25/07 4:01:58 PM	172.17.1.1	172.17.17.5	Drop	0	8
●	10/25/07 4:01:58 PM	172.17.1.1	172.17.17.5	Drop	0	8
●	10/25/07 4:01:58 PM	172.17.1.1	172.17.17.5	Drop	0	8
○	10/25/07 4:01:58 PM	172.17.11.5	172.18.1.5	Accept	0	8
○	10/25/07 4:01:58 PM	172.17.11.5	172.18.1.5	Accept	0	8
●	10/25/07 4:01:56 PM	99.132.44.56	172.16.2.106	Drop	0	7
●	10/25/07 4:01:53 PM	172.17.1.1	172.17.17.5	Drop	0	8
●	10/25/07 4:01:53 PM	172.17.1.1	172.17.17.5	Drop	0	8
●	10/25/07 4:01:53 PM	172.17.11.5	172.17.17.5	Drop	0	8
○	10/25/07 4:01:53 PM	172.17.11.5	172.17.1.1	Accept	0	6
○	10/25/07 4:01:53 PM	172.18.1.5	172.17.11.5	Accept	0	8
○	10/25/07 4:01:53 PM	172.17.11.5	172.18.1.5	Accept	0	8
●	10/25/07 4:01:53 PM	172.17.11.138	172.17.11.5	Successful login-administrator	0	8
●	10/25/07 4:01:50 PM	186.45.34.122	172.16.7.101	Deny	0	0

Update: 10/25/07 4:02:00 PM Received: 27 (of 27) Displaying: 27

Cost

$$$ Moderate

The TCO calculated for a 3 year period is approximately in the $80k to $150k range.

Suited to

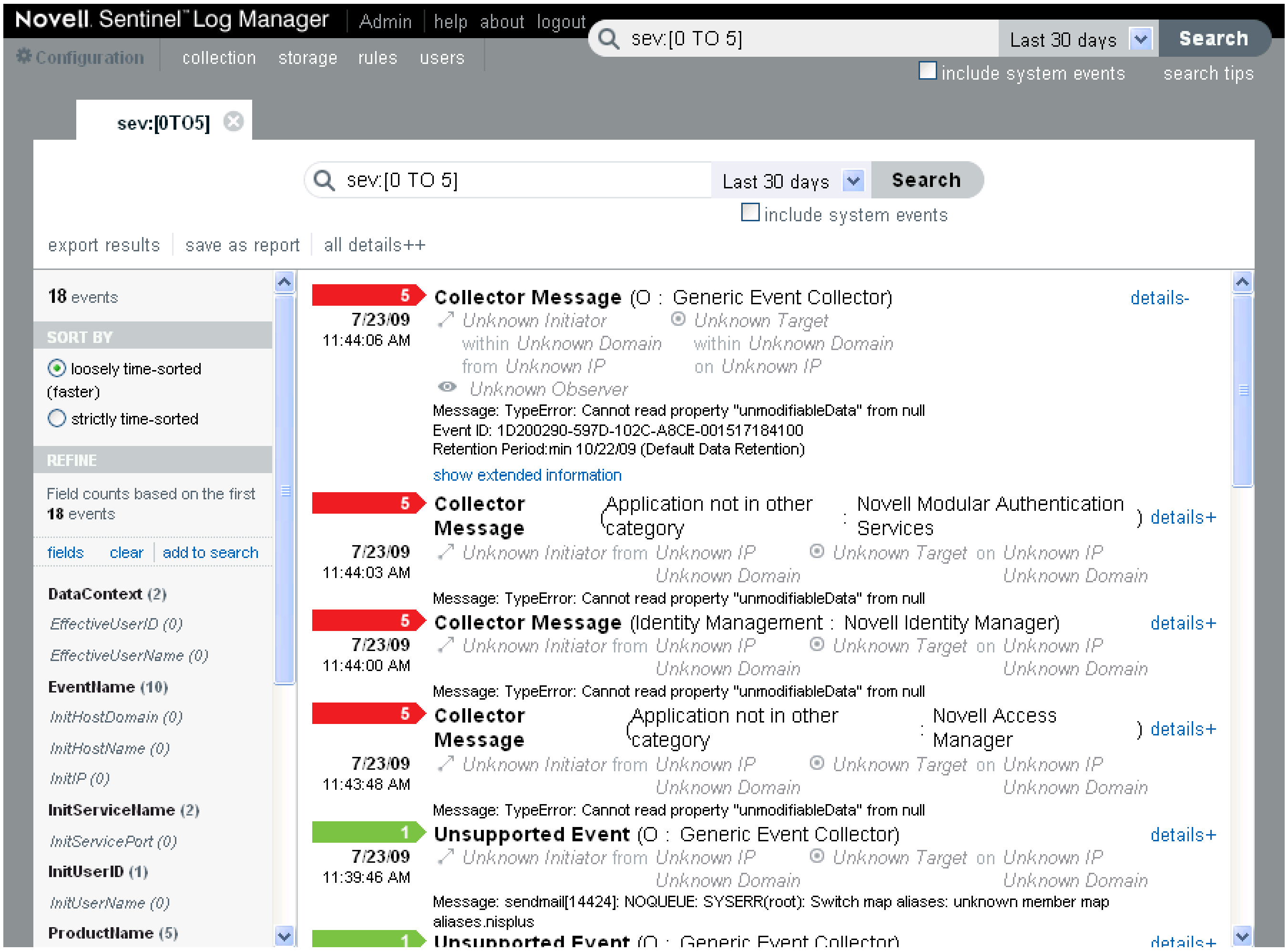
Medium and large sized enterprises with security staff

Strengths:

- Fast and easy to deploy, Sentinel begins to collect data, identify devices, and manage threats almost immediately its installed.
- Intuitive data searching allows security administrators to easily find the data they need and turn the search into a report for management review.
- Sentinel provides a highly customizable data management regime enabling flexible storage and retention. It also allows for customizable indexing and compression saving storage space and cost. E.g. Sentinel employs an efficient file-based event storage tier optimized for long-term event archiving.
- NetIQ Sentinel 7 offers integration with identity management to tie users to specific activities across a variety of environments to allow easier identification of critical risks, better reaction times and quicker remediation of threats and security breaches.
- NetIQ is the most international of all the smaller SIEM players with excellent global reach and investment behind it, which is important for large enterprises.

Weaknesses

- NetIQ provides a broad security solution set and its Sentinel offering is not as mission-critically dedicated to SIEM as some of the other specialized, totally dedicated (but smaller) SIEM vendors.
- With great customizability come more choices and complexity and the need for dedicated security staff to implement and manage Sentinel.
- NetIQ supports third-party threat intelligence, but is limited regarding the uses of that information in comparison to its peers.
- Out of the box, Sentinel provides fewer pre-packaged remediation solutions than is the norm. This may increase time to incident resolution.



```
5  Collector Message (O : Generic Event Collector)                                  details-
7/23/09      Unknown Initiator           Unknown Target
11:44:06 AM  within Unknown Domain       within Unknown Domain
             from Unknown IP             on Unknown IP
             Unknown Observer
Message: TypeError: Cannot read property "unmodifiableData" from null
Event ID: 1D200290-597D-102C-A8CE-001517184100
Retention Period:min 10/22/09 (Default Data Retention)
show extended information

5  Collector Message (Application not in other category : Novell Modular Authentication Services)   details+
7/23/09      Unknown Initiator from Unknown IP        Unknown Target on Unknown IP
11:44:03 AM                      Unknown Domain                      Unknown Domain
Message: TypeError: Cannot read property "unmodifiableData" from null

5  Collector Message (Identity Management : Novell Identity Manager)                details+
7/23/09      Unknown Initiator from Unknown IP        Unknown Target on Unknown IP
11:44:00 AM                      Unknown Domain                      Unknown Domain
Message: TypeError: Cannot read property "unmodifiableData" from null

5  Collector Message (Application not in other category : Novell Access Manager)    details+
7/23/09      Unknown Initiator from Unknown IP        Unknown Target on Unknown IP
11:43:48 AM                      Unknown Domain                      Unknown Domain
Message: TypeError: Cannot read property "unmodifiableData" from null

1  Unsupported Event (O : Generic Event Collector)                                  details+
7/23/09      Unknown Initiator from Unknown IP        Unknown Target on Unknown IP
11:39:46 AM                      Unknown Domain                      Unknown Domain
Message: sendmail[14424]: NOQUEUE: SYSERR(root): Switch map aliases: unknown member map
aliases.nisplus

1  Unsupported Event (O : Generic Event Collector)                                  details+
```

Bottom Line:

If you are a medium or larger enterprise with a complex security environment and especially if you are in federal, healthcare or the cloud service provider space, NetIQ's Sentinel is a powerful offering at a great value. NetIQ is ideal if you have (1) security operations staff and (2) security architects looking for a flexible, adaptable SIEM solution that is fully customizable.

Some of the other players in SIEM

These include

- Accelops
- AlienVault
- Eventsentry
- Exabeam
- HP
- IBM
- Intel Security (and McAfee)
- Intellisecure
- RSA
- Solarwinds
- Splunk

For example, at HP, ArcSight ESM is one of the log management solutions for HP's Enterprise Security Products (ESP). ArcSight offers a variety of SIEM solutions that vary for SME to enterprise businesses. Threat intelligence is provided by HP's own feed and by third party feeds, providing fast and robust up to date threat knowledge. ArcSight Threat Response Manager allows automated remediation of threats based on actionable events.

For more information about the overall SIEM landscape please read our upcoming report on the "SIEM Landscape – Analyzed 2016".

Mi6Research provides market research and business insights to help decision makers in information technology, business, marketing and investment functions. For more information visit www.Mi6Research.com or contact us at info@Mi6Research.com.

IMPORTANT NOTICE: Our information is based on sources believed to be reliable and information up to date and correct to the best of our knowledge at the time of preparation. The opinions reflect judgment at the time and are subject to change. Mi6Research disclaims all warranties as to the completeness, adequacy or accuracy of such information and shall have no liability for errors, omissions or inadequacy in such information. You assume responsibility for all interpretations of, use of all information in this report and Mi6Research is not liable for any interpretations or decisions made by you.