ted and may earn a commission when you buy through links on our site

ree Open Source SIEM Tools

of open source SIEM solution out there, choosing the right business and budget can be challenging. In this article, we present a review of our seven best open source SIEM solutions.

AMAKIRI WELEKWE - TECHNOLOGY ADVISOR | CYBERSECURITY EVANGELIST
February 26, 2021

Security Information and Event Management (**SIEM**) software is a tool that provides a single centralized platform for the collection, monitoring, and management of security-related events and log data from across the enterprise. Because a SIEM correlates data from a wide variety of event and contextual data sources, it can enable security teams to identify and respond to

Latest Posts

What is Maze Ransomware & How to Protect Against It?
July 4, 2021 / by Stephen Cooper

What is NotPetya Ransomware & How to Protect Against It?
July 4, 2021 / by Stephen Cooper

What is Petya Ransomware & How to Protect Against It?
July 4, 2021 / by Stephen Cooper

What is Ryuk Ransomware &

suspicious behavior patterns more effectively than would be possible by merely looking at data from individual systems.

Security is achieved via a combination of prevention, detection, and response efforts. However, it appears most security failures these days are more of detection and response than prevention, and this is where SIEM comes into play. A SIEM solution provides a great opportunity for organizations to manage their security issues, especially in the area of incident detection and response, insider threat mitigation, and regulatory compliance.

Open Source SIEM Tools

Cost no doubt plays a major factor in most IT decisions. For SMBs, investing in enterprise-grade SIEM tools can be capital intensive. The option of open-source SIEM software has become increasingly popular and adopted by businesses both in the public and private sector. Open source SIEMs have matured considerably over the years and provide basic capabilities that can suit the needs of SMBs that are starting to log and analyze their security event information. It helps to reduce licensing costs and provides an opportunity to evaluate certain capabilities before extending investments to premium products. While it can’t provide the comprehensiveness of enterprise-level solutions, open-source SIEM does offer solid functionality at an affordable rate. This makes it appealing to SMBs and other organizations looking to minimize cost.

Of course, open-source SIEM solutions also have their drawbacks, so it is important to look at some of the

How to Protect Against It?
July 4, 2021 / by Stephen Cooper

Popular Posts

11 Best Free TFTP Servers for Windows, Linux and Mac
February 28, 2019 / by Jon Watson

10 Best SFTP and FTPS Servers Reviewed 2021
February 27, 2019 / by Jon Watson

13 Best NetFlow Analyzers & Collector Tools for 2021
January 23, 2019 / by John Kimball

Best Bandwidth Monitoring Tools – Free Tools to Analyze Network Traffic Usage
December 21, 2018 / by John Kimball

downsides associated with them. Listed below are some of the downsides associated with open-source SIEM tools:

1. There's a possibility that the open-source software may not always be available: When the community behind maintaining and updating the source code goes out of business, you may be left to bear the burden of maintaining it yourself. You may save money on licensing costs but may end up spending more on continual maintenance.

2. Support isn't always available or reliable: With open-source software, support isn't always guaranteed, and if there is, it would be bereft of the benefits associated with SLA kind of support.
3. Because of the massive amount of aggregated data, most open-source SIEMs don't provide or manage storage. They may have to combine open-source SIEM with other tools to realize expected benefits.
4. Many open-source SIEM solutions lack key SIEM capabilities, such as next-generation capabilities, reporting, event correlation, and remote management of log collectors.

Premium Enterprise SIEM Tools

While the main driver for the adoption of open-source SIEM is reduced license costs, it is important to highlight the fact that license costs are only a fraction of the total cost of ownership of a SIEM solution, especially when other factors like hardware, storage, and human capital are considered. If you are planning on adopting an open-source SIEM software, it's advised that you carefully consider the pros and cons, and be prepared to accept the risks associated with them.

However, premium enterprise SIEM solutions offer better configuration and installation processes, correlation and reporting capabilities, machine learning and SaaS options, reliable vendor support, and many other useful functionalities. They enable organizations to monitor large-scale data center activities and centrally manage the security of key applications and network infrastructure. Perhaps most importantly, only enterprise SIEM platforms provide options for on-premise or cloud deployments and the capabilities of next-generation SIEM. Next-generation enterprise SIEMs come with powerful technologies such as User and Event Behavior Analytics (UEBA) and Security Orchestration, and Automation and Response (SOAR)—which significantly improve the effectiveness of incident detection and response efforts.

We have reviewed and documented some of the best enterprise-grade premium SIEM tools in the market. Some of them such as the **SolarWinds Security & Event Manager** (SEM) and the ManageEngine EventLog Analyzer offer a **30-day free trial**, which provides an opportunity to evaluate certain capabilities before deciding to invest in the product.

Notwithstanding, premium enterprise SIEM tools are not cheap and most businesses may not be able to afford them. This is where open-source SIEM tools stand out. With a variety of open-source SIEM out there, choosing the right one for your business can be challenging. What fits perfectly from a feature and functionality standpoint for one organization may not fit for another. To help you decide between the countless free and open-source SIEM tools on the market, we’ve put together a list of the seven best open-source SIEM software. Hopefully, this will guide you in the process of selecting the right one for your business.

The Best Open-Source SIEM Tools

1. AlienVault OSSIM

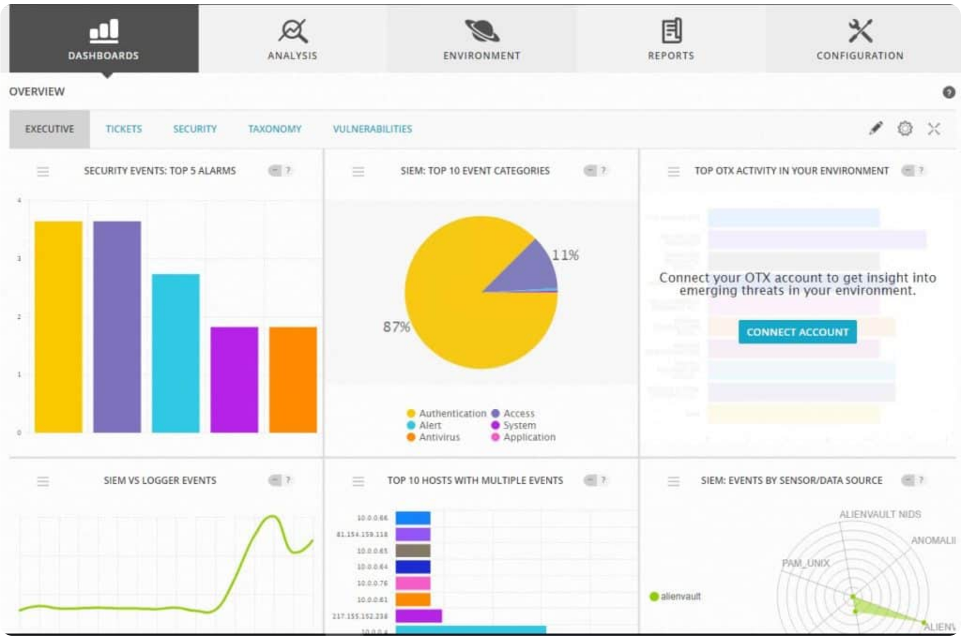
The Open Source SIEM (OSSIM) software by AT&T Cybersecurity, prides itself as the world’s most widely used open-source SIEM. OSSIM leverages the power of the AT&T Open Threat Exchange (OTX)—which provides open access to a global community of threat researchers and security professionals; thereby allowing users to both contribute and receive real-time information about malicious activities. AT&T provides ongoing development and maintenance for OSSIM.

OSSIM includes key SIEM components such as event collection, normalization, and correlation. Other features and capabilities include:

- Asset discovery and inventory
- Vulnerability assessment
- Intrusion detection
- Behavioral monitoring
- SIEM event correlation

For organizations looking for a credible open-source alternative to enterprise-grade SIEM tools, OSSIM offers the chance to experience core SIEM functionalities without spending so much on license costs. OSSIM can be deployed on-premises either on physical or virtual environments, but installation is limited to a single server only. Community support is provided via product forums. OSSIM is available for download here.

However, the downside of this open-source tool is that it can be a bit difficult and laborious to set up and customize especially in Windows environments. It also has limited log management, application, and database monitoring. For organizations that are looking for a more complete SIEM solution, AlienVault Unified Security Management (USM) is a cloud-hosted service that delivers additional functionality that provides everything needed for effective threat detection, incident response, and compliance management.



Connect your OTX account to get insight into emerging threats in your environment.

Figure 1.0 Diagram showing OSSIM application dashboard

2. ELK Stack

The ELK Stack (Elastic Stack) is the world's most popular log management platform and open-source building block for SIEM. The ELK Stack is popular because it fulfills a key need in the SIEM space. It provides organizations with a powerful platform that collects and processes data from multiple sources, stores that data in one centralized data store that can scale as data grows, and a set of tools to analyze the data. The ELK Stack is developed, managed, and maintained by Elastic.

The ELK Stack utility is comprised of the open-source tools—Logstash, Elasticsearch, Kibana and Beats:

- Logstash is a log aggregator and parsing tool that collects and processes data from a variety of sources. Logstash plays a critical role in the stack—it allows you to filter, massage, and shape your data in a way that makes it easier to work with.
- Elasticsearch is the storage, full-text search, and analytics engine for storing and indexing time-series data. Its role is so central that it has become synonymous with the name of the stack itself.
- Kibana is the visualization layer that works on top of Elasticsearch, providing users with the ability to analyze and visualize data.
- Beats are lightweight agents that are installed on edge hosts and are responsible for collecting and shipping the data into the stack via Logstash.

ELK can be installed locally on-premises, or on the cloud, using Docker and configuration management systems like Ansible, Puppet, and Chef. For organizations that want to completely avoid investments in onsite infrastructure and human capital, there’s a ready SaaS-based cloud platform called Elastic Cloud (with a 14-day free trial) which includes features such as machine learning, security, and reporting managed by the creators of the stack.

Figure 2.0 Screenshot showing Elastic Stack dashboard

3. OSSEC

Open Source Security (OSSEC) is an open-source security project for cybersecurity founded in 2004. This open-source tool is technically known as a host-based intrusion detection system (HIDS). However, OSSEC has a log analysis engine that is able to correlate and analyze logs from multiple devices and formats, thereby enabling it to function as a SIEM. You can tailor OSSEC to meet your SIEM needs through its extensive configuration options.

OSSEC is supported by various operating systems, such as Linux, Windows, macOS, Solaris, as well as OpenBSD and FreeBSD. It is broken into two main components:

- The server—responsible for collecting log data from different data sources.
- The agents—applications that are responsible for collecting and processing the logs and making them easier to analyze.

In addition to its log analysis capabilities, OSSEC provides intrusion detection for most operating systems and performs integrity checking, Windows registry monitoring, rootkit detection, and alerting. The OSSEC project is currently maintained by Atomicorp who stewards the free and open-source version and also offers an enhanced commercial version. However, the main pain point of this tool is that it lacks some of the core log management and analysis components of a typical SIEM. This limitation motivated other HIDS solutions like Wazuh to fork OSSEC in order to extend and enhance its functionality and make it a more complete SIEM tool. However, in recent times, Atomicorp has made a lot of changes, upgrades, and enhancements to OSSEC, which has repositioned it to be more competitive.

Figure 3.0 Screenshot showing OSSEC dashboard

4. Wazuh

Wazuh is a free, open-source project for cybersecurity founded in 2015 as a fork of OSSEC. Just like OSSEC, this open-source tool is technically known as a Host-based Intrusion Detection System (HIDS). Today, Wazuh stands as a unique solution with over 10,000 open-source community users, including top Fortune 100 companies. Wazuh describes itself as “a free, enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response, and compliance”.

The main components of Wazuh are the agent, the server, and the Elastic Stack:

- The Wazuh agent is a lightweight app designed to perform a number of tasks to detect and respond to threats.
- The Wazuh server is in charge of processing and analyzing the data received from the agents, and using threat intelligence to search for known indicators of compromise.
- The Elasticsearch component of the Elastic Stack receives, indexes and stores alerts generated by Wazuh. The Kibana component of the Elastic Stack provides a user interface for data visualization and analysis.

Wazuh is used to collect, aggregate, analyze, and correlate data; helping organizations detect and respond to threats and security incidents, as well as meet compliance requirements without spending so much on license cost. It can be deployed on-premises, hybrid, or cloud environments. It has a centralized, cross-platform architecture that allows multiple systems to be easily monitored and managed.

A cloud-based premium version known as Wazuh Cloud is also available. Wazuh Cloud centralizes threat detection, incident response, and compliance management across your cloud and on-premises environments. Wazuh Cloud uses lightweight agents that run on monitored systems to collect and forward events to the Wazuh cloud infrastructure, where data is stored, indexed, and analyzed.

Figure 4.0 Screenshot showing Wazuh dashboard

5. Apache Metron

Apache Metron is a security application framework that provides organizations the ability to ingest, process, and store a variety of data feeds at scale in order to detect and respond to cyber threats. First released in 2016, Apache Metron is a relatively new player in the industry and another example of a security framework that ties a collection of open-source tools into one platform.

Figure 5.0 Diagram showing Melton core capabilities | Image credit: Apache Software Foundation

Metron provides capabilities for log aggregation, indexing, storage, behavioral analytics, and data enrichment while applying the latest threat-intelligence information. From an architectural perspective, Metron's strongest feature is its pluggable and extensible architecture. As the diagram above indicates, the Metron framework provides four key capabilities:

- Security Data Lake: Just as the name implies, a data lake provides a large collection of data used to power discovery analytics and a mechanism to search and query for operational analytics.
- Pluggable Framework: Provides parsers for common security data sources (pcap, NetFlow, bro,

snort, fireye, Sourcefire); and pluggable framework to add new custom parsers for new data sources. It can add new enrichment services to provide more contextual info to the raw streaming data, pluggable extensions for threat intel feeds, and the ability to customize the security dashboards.

- Security Application: Provides standard SIEM-like capabilities (alerting, threat intel framework, agents to ingest data sources). It also has packet replay utilities, evidence store, and hunting services commonly used by SOC analysts.
- Threat Intelligence Platform: Provides next-generation defense techniques that consist of a class of anomaly detection and machine learning algorithms that can be applied in real-time as events are streaming in.

Metron leverages the Apache big data technologies such as Apache Hadoop in order to offer a centralized tool for security monitoring and analysis. However, the main pain point of this tool is that it can only be installed on a limited number of operating systems and environments. Metron is available for download here.

6. MozDef

The Mozilla Defense Platform (MozDef) is a set of micro-services that can be used as an open-source SIEM. It was created by the Mozilla Foundation in 2014 with the goal of automating the security incident handling process and facilitating the real-time activities of incident handlers, according to the MozDef docs.

MozDef describes itself as a SIEM add-on that uses Elasticsearch for logging and storing data, and Kibana for dashboarding capabilities. This means that if you use MozDef for your log management, you can easily leverage the features of Elasticsearch to store, archive, index, and search event data using Kibana.

The MozDef architecture is designed in a way that does not allow log shippers (rsyslog, syslog-ng, beaver, nxlog, heka, logstash) direct access to Elasticsearch. Rather, MozDef places itself between Elasticsearch and the log shippers, thereby making it possible for log shippers to interact directly with MozDef as shown in the diagram below. This makes MozDef different from other log management tools that use Elasticsearch and enables it to provide basic and advance SIEM functionalities such as event correlation, aggregation, and machine learning.

Figure 6.0 Diagram showing MozDef system architecture

If you’re looking for a tool that provides basic SIEM functionalities, MozDef is surely a good fit. However, don’t expect it to meet your every need as it doesn’t have a lot of functionality. It is best suited for SMBs but not for corporate environments. The main pain points of this tool are that getting it up and running can be time-consuming and technically demanding. It also lacks high availability options, and key reporting and compliance capabilities.

7. SIEMonster

SIEMonster is a customizable and scalable SIEM software drawn from a collection of the best open-source and internally developed security tools, to provide a SIEM solution for everyone. SIEMonster is a relatively young but surprisingly popular player in the industry. SIEMonster was inspired by the need to build a SIEM solution that will minimize frustrations caused by the exorbitant licensing costs of commercial SIEM products.

SIEMonster has something for everyone—SMBs, large corporations, managed service providers, and the community. The community edition is the free open-source single server edition for businesses with up to 100 endpoints. The community edition (free version) supports real-time threat intelligence and reporting capabilities. It can be deployed on the cloud using Docker containers, and on physical and virtual machines (macOS, Ubuntu, CentOS, and Debian).

However, the major downside to the free version is that it is not easily upgradable, and does not offer user behavioral analytics, machine learning, and most importantly—support. Furthermore, its reporting capability is limited to only two reports. For organizations that want to completely avoid the limitations of the community edition and investments in onsite infrastructure and human capital, SIEMonster SIEM as-a-Service option is your best bet.

Comments

Leave a Reply

Comment

Name *

Leave Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.