ATOMICORP®

WHITE PAPER

How OSSEC Logging Can Dramatically Reduce Your SIEM Costs

What is logging and why is it important in the enterprise?

There are at least two reasons why logging is essential today.

The first is a practical need. Security engineers need real-time awareness to identify and fix problems. They are always identifying activity that could be negatively impacting operational performance as well as nefarious activity that could indicate a cyberattack is underway. The best scenario is that logs help you identify and proactively stop an attack. At the very least, you need data that enables you to audit what happened.

It is this scenario that led to the second reason why logging is essential. It has become an important regulatory requirement.

For regulated organizations, log capture is a requirement to meet compliancy requirements such as PCI-DSS, HIPAA, NERC CIP, or Sarbanes-Oxley.
For government contractors or agencies there is FISMA and JSIG and for European companies and those who do business with European companies, there is now GDPR. And for many organizations, the majority or even all of these regulations may apply to them. That's a lot of regulatory requirements that require logging.

What is involved in logging?

Logging is not simple.

Cyberattacks may be happening in an abstraction layer and may be interacting with multiple databases through a web application. This means it can be very challenging to figure out what's going on because you need to view logs from multiple systems to identify the attack. If the applications are generating telemetry, what many people call logs, you can create rules or apply machine learning to review system data and alert you to anomalies.

But, there are a lot of systems. We need tools to automate that process because there's entirely too much data. Even in a small organization, it is overwhelming. It is not only more information than is reasonable for a human being to look through, but by the time that human being has discovered that something bad has occurred, it is already too late. The situation really reinforces the fact that human beings will always lose the race against computer-based attacks.

Security Information and Event Management (SIEM)

So, this is where a SIEM comes in to try and help. Decades ago, we had log-based intrusion detection systems.

SIEM is just a derivative of that approach.

Gartner defines the SIEM market by *"the customer's need to analyze event data in real time for the early detection of targeted attacks and data breaches, and to collect, store, analyze, investigate and report on event data for incident response, forensics and regulatory compliance."*[1]

SIEM solutions aggregate data produced by security devices, systems and applications. Data from logs is the primary source but SIEM's also collect data from other sources such as networks. All of this data is then normalized so that it can be correlated and analyzed for security management, user activity monitoring and compliance reporting.

Alarm Avalanche

In short, there are more systems, more data and more attacks than most SIEM architects ever contemplated.

Rules are applied to SIEM solutions to analyze the logs to detect potential problems that may reveal a cyberattack. However, the SIEM will also identify a lot of other events that are not attacks. Most of the alerts generated reference an event that is benign. It may take a cyber analyst a great deal of data sifting to find something that really does require attention.

7 minutes

Security professionals have, on average, 7 minutes per SIEM alert to decide whether an APT attack is occurring.[2]

This leads to the human factor that analysts refer to as "alert avalanche." It's not very useful to tell a human being that a lot of potentially bad things are happening if that person then has to analyze all of that data to determine what is really occurring. There is too much data to analyze and too many alerts. Security analysts become overwhelmed and you have alerts that are never analyzed and hacks that go undetected.

According to Information Age, *"on average, a security professional has just 7 minutes per SIEM alert to decide whether an APT attack is occurring, or if a user has opened a phishing email."*[2]

#1 driver

According to Gartner, threat management is the primary driver of SIEM growth.[1]

Nevertheless, the SIEM market is growing.

According to Gartner, the SIEM market grew from $2.001 billion in 2015 to $2.167 billion in 2016. Gartner reports that threat management is the primary driver, and general monitoring and compliance remains secondary.[1]

So the need for SIEMs hasn't changed and the market is growing. We still have the issue of growing data and alert avalanche, but that's not all. SIEM costs are also dramatically on the increase.

More data results in greater costs.

Back to the problem of increasing data volume.

Logging data never lessens; it only gets bigger and as data grows so will your SIEM vendor bill. Most SIEM vendors charge by data volume.

2x

Gartner estimates that SIEM costs are doubling annually.[1]

This could be measured in several different ways: events per second, data indexed or average data volume processed, but regardless, it means increasing costs. Gartner estimates that these costs are doubling annually.[1] And there is another issue with growing data that impacts SIEM costs. The amount of storage needed.

Those are problems that impact SIEM costs directly but there are other cost-related issues with the exponential increases in the volume of log data. The amount of "noise" that security engineers have to respond to impacts their productivity, causes delays in attack detection and remediation and also results in more false positives; all of which indirectly impact costs.

Can open source help?

> According to Gartner, "the complexity and cost of SIEM, have driven interest in alternative approaches to collecting and analyzing event data to identify advanced attacks."

One such alternative is the open source, Elastic Stack (the combination of Elasticsearch, Logstash and Kibana) that can leverage or natively use a big data platform like Hadoop to offer data collection, management and analytics capabilities.

Gartner reports that "*organizations with sufficient resources to deploy and manage these and develop and maintain analytics to address security use cases, may be able to get a solution that addresses a sufficient number of their requirements for a lower cost compared with commercial technologies.*"[1]

So, there are alternatives but they have their challenges. Gartner continues to track the development of these alternative approaches but have encountered some less-than-positive feedback from customers.

> *"The workload involved in engineering these solutions to scale and the development effort to support the required event sources and analysis is significant, despite the software itself being free. This may negate the objective of being less expensive than a commercial SIEM deployment."*[1]

What is OSSEC?

OSSEC is an open source host-based intrusion detection system (HIDS) used by leading global companies ranging from **Netflix** and **Facebook** to **Workday** and **Airbus**.

The solution is incredibly robust and flexible, but it is also complicated.

OSSEC was started approximately 13 years ago. One of the first things the OSSEC community did was address log aggregation and analysis for scale. It was designed to handle tens of thousands of nodes and the data they generate.

80%

A recent OSSEC implementation decreased the amount of data going into the SIEM by 80%!

Some organizations today are using OSSEC in place of a SIEM and others use it to complement an existing SIEM. If you want to replace a SIEM there are open source visualization tools such as Elasticstack that can be used as a replacement for a SIEM dashboard. However, the more important factor is creating rules that help identify the problems, so analysts are only using the dashboard to investigate real attacks. This is simple with OSSEC.

OSSEC and the detection and compliance modules can also be used to complement an existing SIEM. In those instances, you use the rules modules to filter data before it goes to the SIEM by discarding alerts that are clearly not security related. During one recent OSSEC implementation, the amount of data going into the SIEM was reduced by 80%!

Here you need to consider the difference between alerts and events. Using OSSEC, you are not reducing the fidelity of the data going into the SIEM, you are making it better while reducing both costs and alert avalanche. This makes the cyber analysts more productive since they are sifting through less chaff and able to focus more on significant alerts. They can identify real attacks sooner and initiate remediation and active response, which is another OSSEC feature beyond logging. Plus, OSSEC will keep a copy of all those log events, so you can still mine the data anytime you want. You get the best of both worlds. It also means organizations can dramatically reduce their SIEM costs as many SIEM providers charge based on data volume.

OSSEC Logging Trifecta Advantage

Increased security analyst productivity

Faster attack detection and remediation

Dramatically reduced SIEM costs

What does Atomicorp bring to OSSEC?

While OSSEC is free to use, as previously mentioned, it can be complicated to use.

Organizations implementing OSSEC may encounter challenges in configuration and the absence of purpose-built tools like a management GUI, real roadblocks. It's also worthy to note that OSSEC, while a powerful engine for the collection of system data for analysis, does nothing to provide security or prevent attacks. Atomicorp is addressing these issues for global companies today.

Atomicorp provides a set of OSSEC specific add-ons including both a free security WAF and an advanced security WAF that protect endpoints from both common and targeted attacks. Atomicorp has taken this even further by developing pre-packaged rule modules that are designed to identify specific classes of attacks and others that are used to comply with common regulatory regimes. It's a fast and efficient way to protect your OSSEC installation from cyberattacks.

Atomicorp OSSEC Rules

Unrivaled WAF Protection

Atomic ModSecurity Rules protect against SQL injection, cross-site scripting, cross-site request forgery, encoding abuse, protocol abuse, Unicode and UTF-8 attacks, HTTP smuggling, path recursion, web spam, shells, spam tools, mailers, malicious iFrames and more.

Real-time Patches for Vulnerabilities

Atomicorp has been building ModSecurity Rules for more than a decade so most high- profile attacks are covered by existing rule sets. When new vulnerabilities arise, Atomicorp implements real-time patches to ensure security.

Real-time Blacklists

Dynamic blacklist updates as new nefarious IP addresses are identified provide protection from spammers.

Real-time Malicious Domain Blocking

Real-time monitoring of activity enables Atomicorp to identify malicious activities from domains hitting one set of servers and use that data to automatically protect all other Atomicorp protected servers before they are hit.

Real-time Modsecurity and AV Rules Updates

Even without new vulnerabilities, Atomicorp frequently updates rules that are made available to all customers.

global
500

Enterprises such as Salesforce, GE and Sony are bringing OSSEC into their security stack.

Atomicorp OSSEC GUI

OSSEC is a great tool set, but it is lacking when it comes to a management GUI. The command line interface is effective if you are an expert in OSSEC, but can be difficult for both novice and experienced users.

Atomicorp offers an OSSEC specific GUI that enables you to quickly analyze attacks, manage OSSEC and your agents and take action where needed. Unlike other dashboards that have been cobbled together to work with OSSEC, Atomicorp's OSSEC dashboard was built from the ground up for OSSEC.

OSSEC offers a great set of foundational tools that the Atomicorp OSSEC GUI makes more powerful and easier to use. It includes not just the ability to see your events, but also to manage the systems OSSEC is monitoring. This gives you true control over your security.

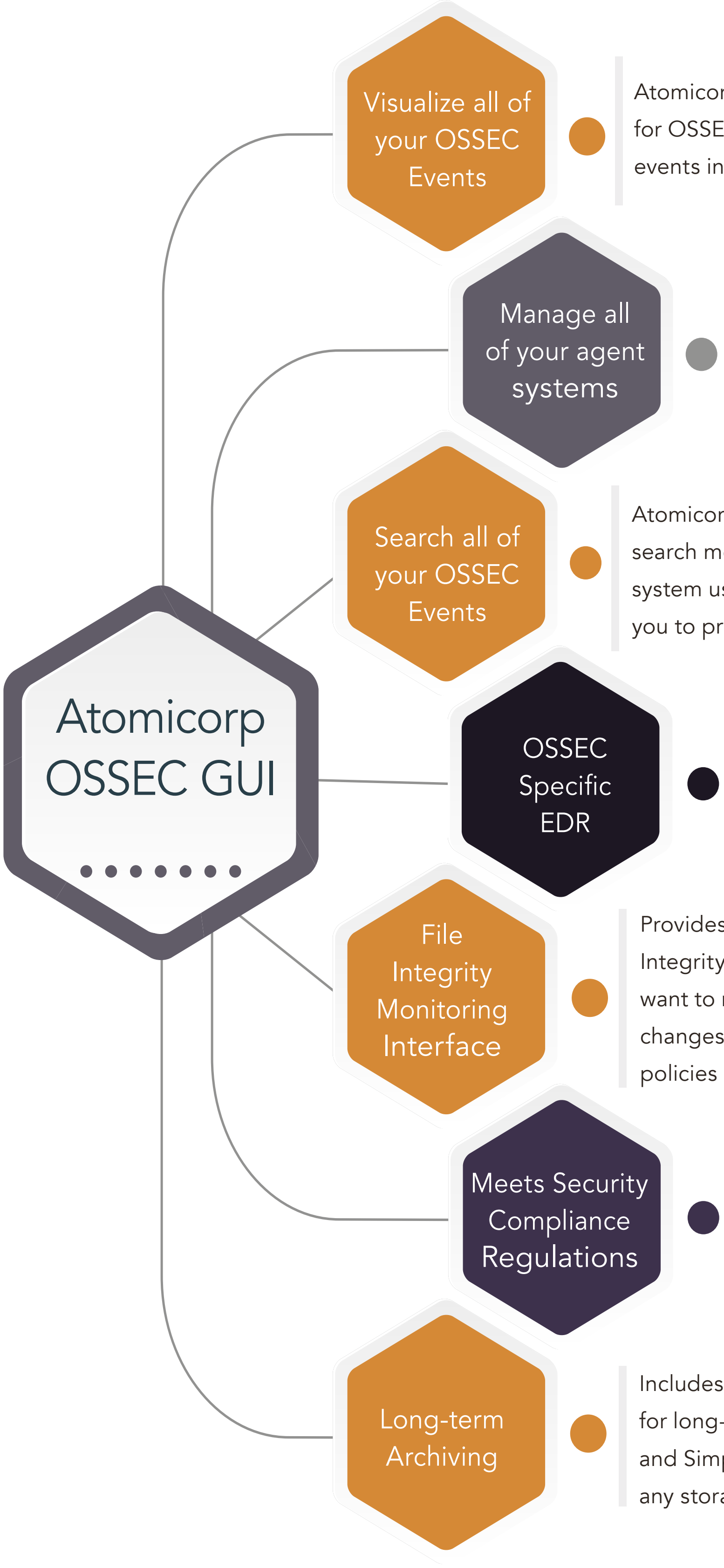
Why Atomicorp?

Why does Atomicorp know so much about OSSEC?

Because Atomicorp built a significant portion of the OSSEC code base and has used that expertise to add much needed functionality for enterprise users.

Atomicorp's CTO, Scott Shinn, is the official OSSEC open source project manager and he is passionate about expanding the use of OSSEC. Building upon more than 10 years of research and 20 years of experience, the Atomicorp team developed Atomic Enterprise OSSEC (AEO) which assists OSSEC users with configuration and management of their OSSEC implementation.

A Management GUI Built for OSSEC



Atomicorp OSSEC GUI

Visualize all of your OSSEC Events

Atomicorp's GUI was specifically designed and built for OSSEC allowing you to see, react and manage events in real-time on your systems.

Manage all of your agent systems

Centrally manage all of your agents and rules with the Atomicorp OSSEC GUI. You can even drill down and manage rules on individual agent systems.

Search all of your OSSEC Events

Atomicorp provides a lightweight but powerful search mechanism that allows you to quickly scour the system using a long list of parameters. This enables you to precisely address any event on your system.

OSSEC Specific EDR

Atomicorp allows you to turn OSSEC into an Endpoint Detection and Response (EDR) system giving you a fully-automated playbook.

File Integrity Monitoring Interface

Provides a management interface for the File Integrity Monitoring system. Configure what you want to monitor, add, delete, update or even ignore changes. This interface also allows users to set base policies and create custom notifications.

Meets Security Compliance Regulations

Atomicorp's GUI for OSSEC is turn-key for meeting security compliance regulations including HIPAA, PCI DSS, SOX, DoD and more.

Long-term Archiving

Includes a built-in log archive management system for long-term storage solutions like Amazon Glacier and Simple Storage (S3) service, Microsoft Azure or any storage array you choose.

Conclusion

Logging is critical in today’s cybersecurity landscape.

Security engineers need it for real-time awareness to operational efficiency and potential attacks.

If you’re unable to stop an attack before it happens, log data is necessary to audit what occurred. Equally important, is the need for logging in order to meet compliancy regulations. But organizations have multiple systems and the amount of data being logged never decreases. This results in security analysts becoming overwhelmed by the vast number of alerts being generated. It is inevitable that human beings are unable to keep up and dangerous events are overlooked. SIEMs were developed to help circumvent this problem. They serve to aggregate and analyze event data for early detection, investigation and reporting for response, forensics and compliance. But the data continues to grow as do SIEM costs. Most SIEM vendors charge by data volume, plus there is the added cost of increased storage and costs associated with security analyst’s compromised productivity and delayed attack detection and remediation due to the “noise.”

That is why many **large, Global 500 organizations** are turning to the open source community for help.

OSSEC is a robust and flexible open source host-based intrusion detection system.   It’s detection and compliance modules can replace or complement a SIEM. In the case of the latter, rules modules filter data before it goes to the SIEM by discarding “noise” which greatly reduces costs.

But OSSEC is complicated.

This is where Atomicorp can help. Atomicorp has been heavily involved in developing the OSSEC code base and is leveraging that experience to make OSSEC functional for enterprise users.

Learn more about how Atomicorp can help your organization take advantage of the benefits of OSSEC while significantly reducing costs.

ATOMICORP®

About Atomicorp

Atomicorp eliminates the complexity and burden of cybersecurity and compliancy across cloud infrastructures through its comprehensive, multi-layered cloud and server protection platform. Harnessing the power of Open Source Security (OSSEC) and proprietary machine learning, Atomicorp aggregates and correlates data across the enterprise to automatically provide high fidelity active response and recovery. And, Atomicorp enables organizations to maximize their cybersecurity resources to better address today's rapidly evolving threat environment. From end-of-support to cutting edge systems, Atomicorp has the flexibility to provide security and compliancy to any organization. Atomicorp protects thousands of customers within retail, media, healthcare, insurance, and government institutions worldwide.

www.atomicorp.com

info@atomicorp.com
(703) 299-6667

15049 Conference Center Drive
Suite 180
Chantilly VA 20151

Footnotes:

[1] Gartner. "Forecast: Information Security, Worldwide, 2015-2021, 3Q17 Update."

[2] Information Age. "Best Practices for Optimizing SIEM Environments," Nick Ismail, 1/26/17.

ac_wp_300001.0718_siem_cost_reduction