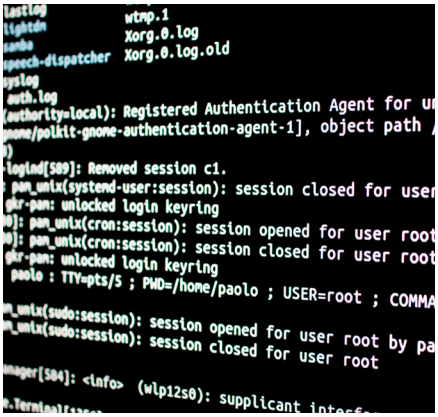
THE ARGUMENT FOR OPENSOURCE SIEMs

AVALON Cyber

AVALONCyber

THE ARGUMENT FOR OPENSOURCE SIEMs



The SIEM platform that simply pulled in log data with no actionable intelligence is dead.

But, over the years, SIEMs have evolved.

In the beginning, was the SIEM. And the SIEM was bad.

> "A SIEM costs over a million dollars a year!"
>
> "They're impossible to configure!"
>
> "SIEMs cause alert fatigue!"

These are a few complaints you may have heard about Security Information and Event Management (SIEM). And they are true…of the "original" SIEM. When SIEMs first came onto the scene in the mid-2000s, they helped organizations deal with a large number of intrusion alerts by streamlining tasks previously performed by two separate technologies: a Security Information Management (SIM) system, which collected, stored, and analyzed log data, and a Security Event Management (SEM) system, which provided real-time monitoring, event correlation, and alert notification.

However, the old SIEMs were expensive (like, only-Fortune-500-companies-could-afford-them expensive), difficult to configure and manage, and definitely caused alert fatigue for analysts and response teams. And, yes, the SIEM platform that simply pulled in log data with no actionable intelligence is dead.

But, over the years, SIEMs have evolved.

Now, SIEMs are based on big data infrastructure, allowing them to comb through enormous data sets, and can provide users with a broad scope view of everything happening on your network. They aggregate all your security-oriented log sources – from firewall and proxy logs to domain controller and threat detection logs – into one central location. Finally, they use correlation rules and behavioral detections to show patterns and derive meaningful information necessary for compliance reporting and threat alerting.

Cost, however, can still prove to be an issue. If, that is, you purchase a SIEM from a major software company.

But, just as brilliant minds have always come together to solve the challenge of affordability for cars, computers, medicine, and other necessities, a diverse group of technologically skilled men and

AVALONCyber

THE ARGUMENT FOR OPENSOURCE SIEMs

Talented cybersecurity engineers have taken a hard look at the opensource technology landscape and have implemented excellent, and much more affordable, technology solutions into their SIEMs.

women have developed tools that can be used to build world-class SIEMs at a fraction of the cost.

How? Opensource (OS) tools and technology. (If something is "opensource," it simply means that "thing" is publicly accessible – and FREE – and can be shared and modified by anyone who wants to use it.) So now, smaller, nimbler cybersecurity companies can take advantage of opensource offerings to develop SIEM platforms that are much more affordable.

There are companies, though (namely those that develop their own SIEM technology, rather than utilizing opensource technology), that minimize the abilities of opensource-based SIEMs.

THE TWO CAMPS

Anti-OS: The big-box, next-generation SIEM providers that offer all those flashy, new features, like SOAR (Security Orchestration, Automation, and Response, which allows SIEMs to automatically respond to threats) and UEBA (User and Entity Behavior Analytics, a tool which uses machine learning to identify suspicious behavioral patterns), often criticize opensource technology. They claim that opensource-based SIEMs don't offer proper data storage and lack standard SIEM capabilities. These big-box SIEMs are the ones that still come with the big price tag, which, of course, makes them difficult for small and medium-sized businesses to afford.

Pro-OS: On the other side, talented cybersecurity engineers have taken a hard look at the opensource technology landscape and – in the spirit of saving bottom-line hard costs and offering flexibility and customization capabilities – have implemented excellent, and much more affordable, technology solutions into their SIEMs to vastly improve visibility and incident response capability.

In case you haven't guessed, Avalon Cyber is proud to stand firmly in the Pro-OS Camp. Read on to find out why.

AVALONCyber

THE ARGUMENT FOR OPENSOURCE SIEMs

When it comes to opensource technology and software for SIEMs, the pros far outweigh the cons.

ADVANTAGES OF OPENSOURCE TECHNOLOGY

When it comes to opensource technology and software for SIEMs, the pros far outweigh the cons:

- **Becoming the norm** – Amazon, IBM, Google. These companies and many more utilize opensource software and technology for their online businesses. In fact, opensource code currently powers approximately 90% of the internet.
- **Community** – Think of peer reviews for scientific theories: Scientists love to poke holes in other scientists' ideas. It's the same with the opensource community. Together, these talented experts and afficionados scrutinize, edit, and improve the software and other resources developed by their fellow techies.
- **Cost effective** – IT managers in organizations face constant frustration when dealing with vendor software limitations. Vendors often lock down their products to make it less portable, so creating any kind of flexibility usually comes with a hefty price tag. With opensource software, you never need to worry about licenses and limitations. You can install it several times, use it from any location, and be 100% free from monitoring, tracking, or license-counting requirements.
- **Customizable** – Opensource software is typically of high quality and well designed. When you use opensource software, the source code is available for you to review and edit, which gives you more freedom and allows you to effectively address the "perceived disadvantages" of opensource technology. (See next section.)
- **Reliability** – Opensource support is freely available and can be easily accessed through online communities. These communities are filled with people who have been-there-done-that experience and are willing to assist you with whatever issue you may be encountering. Some may even say this level of support is better than the level 1 and level 2 support you might get through a licensed application!

AVALONCyber

THE ARGUMENT FOR OPENSOURCE SIEMs

If you decide to go with an opensource SIEM solution, consider using a trusted partner, such as Avalon Cyber.

PERCEIVED DISADVANTAGES OF OPENSOURCE TECH (AND WHY WE DISAGREE)

A few cons (we have to be sort of fair, right?) include:

- **Opensource SIEM software can be labor-intensive.** *True, but:* If you put time into developing opensource technology, your SIEM will be what you want it to be. And, if designed and implemented to fit your unique needs, you not only maximize your personnel investment, you save on capital expense as well.
- **Opensource SIEM solutions lack key SIEM capabilities (i.e. reporting, event correlation, and remote management of log collectors)** *True, but:* If you build and implement third-party, opensource plugins – for example, Wazuh and Security Onion – and integrate them directly with your ELK Stack (Elasticsearch, Logstash, Kibana [an opensource log analysis and management platform]), you gain SIEM visibility, which allows you to correlate events, provide reports, etc.
- **Opensource SIEMs require a high level of expertise and time to deploy.** *True, but:* Out-of-the-box solutions also require time and expertise to deploy, as even these types of SIEMs aren't fully plug-and-play.
- **Opensource SIEMs don't provide or manage storage.** *True, but:* This is true of all SIEMs. You could install an enterprise-level SIEM at your company – you'd still be responsible for managing your own storage. Even if data storage is "included" with a SIEM, you still pay for it. The cost may just be rolled into the overall price. And, if you combine an opensource SIEM with a cloud-based storage solution (such as Amazon's S3), you don't manage the storage, the cloud service provider does.

If you decide to go with an opensource SIEM solution, consider using a trusted partner, such as Avalon Cyber. That way, there's no need to worry about any of these "disadvantages", as your SIEM will be designed and architected to provide the full scope of SIEM capabilities required for your business.

AVALONCyber

THE ARGUMENT FOR OPENSOURCE SIEMs

There are literally thousands of tools available in the opensource world.

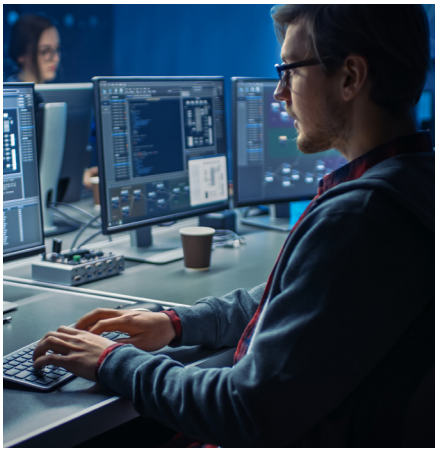
OPENSOURCE SIEM TOOLS

There are literally thousands of tools available in the opensource world. Here are a few typically used to develop opensource SIEMs:

- **Atomic Red Team** – Library of tests security teams can execute to assess a network's defenses against a wide range of attacks.
- **Kali Linux** – "White-hat hacker" framework; a forked version of the Linux OS – used for penetration testing (it contains more than 600 pen test tools!) and security auditing.
- **Metasploit Framework** – Penetration testing software that allows users to write, test, and execute exploit code.
- **Nikto** – Web server scanner that tests for 6,700+ potentially dangerous files/programs, more than 1,250 outdated servers, and version-specific problems on over 270 servers.
- **Nmap** – a.k.a., Network Mapper – used for vulnerability scanning, identifying which devices are running on a system, finding open ports, and detecting security risks.
- **OpenVAS** – Open Vulnerability Assessment – scanner that quickly and easily detects security issues in a range of servers and network devices.
- **OSSEC** – Open Source HIDS (Host-based Intrusion Detection System) Security – performs log analysis, time-based alerting, active response, and more.
- **Security Onion** – Linux distribution used for threat hunting, enterprise security monitoring, and log management; its many "layers" include tools like Snort/Suriticata, OSSEC, Squert, NetworkMiner, and others.
- **TheHive** – Scalable four-in-one opensource security incident response platform designed for SOCs, CSIRTs, CERTs, and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.
- **Wireshark** – Network protocol analyzer that allows users to see network activity at a microscopic level; used for network troubleshooting, analysis, software and communications protocol development, and education.

AVALONCyber

THE ARGUMENT FOR OPENSOURCE SIEMs



A SIEM is only as good as the people managing it.

IT'S ALL ABOUT THE PEOPLE

Here's what it really comes down to: a SIEM is only as good as the people managing it. Because, whether you're using an opensource SIEM or a top-of-the-line SIEM from a big-name software developer, your SIEM still needs human beings to implement and monitor it, and respond to alerts.

You're making an investment in your employees anyway, why not get the best people and make sure that they can not only manage the security tools you purchase, but leverage opensource software and technology to cut costs whenever and wherever possible? And, yes, there are talented people out there – despite the shortage of infosec pros – who can be trained to do this. We have them at Avalon Cyber, and you can too.

As SIEMs have evolved, the issue of affordability has continued, namely in enterprise-level platforms with all the bells and whistles – and prices to match. But today, thanks to opensource technology, SIEMs are accessible to many more businesses, not just those with a multimillion-dollar security budget. The lesson here is: No matter what SIEM you choose, be sure you have the people – whether in-house or outsourced to a trusted cybersecurity team – who will help you derive the most use of and value from this extraordinary cybersecurity tool.

AVALON Cyber

THE ARGUMENT FOR OPENSOURCE SIEMs

Partner with us to achieve a higher level of data security.

ABOUT AVALON CYBER

Avalon Cyber offers a full suite of cyber services, including vulnerability assessments, penetration tests, managed detection and response (MDR), and KnightVision CAM (compliance, alerting, monitoring). KnightVision CAM is our multi-tiered, opensource SIEM and MSOC solution, developed to assist small and medium-sized businesses with regulatory compliance, threat hunting, alert detection, and incident response.

Our team has decades of experience in digital forensics, IT risk management, cybersecurity incident response, and enterprise information security leadership, and our experts have, or previously have held, top secret government clearances and possess key industry certifications including: CISSP, GPEN, OSCP, CCNA, CCE, CFCE, EnCE, and ACE.

We work with clients, from commercial and government organizations in industries that include financial services, legal, healthcare, manufacturing, and telecommunications, who are looking to partner with us to achieve a greater level of data security.

If you have questions, would like a demo of KnightVision CAM, or want to speak to someone about implementing any of our cybersecurity services, contact our team today.

To learn more about Avalon Cyber, visit:
www.avaloncybersecurity.com

For questions, please contact:
Ian M. Gattie
Director of Marketing
716.995.7777
ian.gattie@teamavalon.com