Siemonster Documentation

Release 0.0.1

Iku Turso

Nov 17, 2017

Contents

CHAPTER 1

Guide

1.1 Overview

Kustodian's SIEMonster: SIEM for everyone with no limits

As a security professional, protecting your company's assets from internal or external attacks is a never ending complex job. It is crucial that you have visibility across your entire environment. It's like having a house alarm, there is no point having some rooms with motion sensors and others without it.

All systems have the ability to let out an event that something is going on but is there anyone listening to these events or cries for help. When you picture your environment, with servers, workstations, network appliances, printers, SCADA and other equipment they all log events. On top of this all your applications are sending out events or alerts including Web Servers, Databases, Applications, Anti-Virus and Endpoint protection.

By using a Security Incident Events Management system (SIEM) we can capture all of these events and separate the "Cry wolfs" from the real attacks and alert the security professional that an attack maybe underway. SIEM's can be configured to alert operators via a console, SMS or email for any suspect activity. This could be when an administrator creates another privileged account or alerted when an executive is using email from a destination that is different from their current location or a compromised endpoint. The rules and alerts to suit your business are limitless. One of our customers retrenched 50 staff, they wanted to monitor closely the activity around intellectual property going out the door. By creating a rule and putting the members into that group alerts could be raised on file/folder copies from central servers to USB sticks.

What are the SIEM options? Of course there is a myriad of commercial products out there including HP ArcSight and SPLUNK which are great products but these solutions com with node/GB limitations and can be expensive and of course the ongoing annual license and support costs stack up an compete with your other necessities in your security budget.

Of course you can go the open source/open framework route, and use Elastic Logstash and Kibana (ELK) system or Cisco OpenStack, but speaking from direct experience the time you have built the plugins, dashboards, configs, parses and fine tuning to have a functioning SIEM you're looking at a years' worth of development which is a huge problem if highly sort after security staff leave the organisation.

Kustodian have done all this development and built a SIEM using open source only product built on Elastic without the price tag of Elastics Shield or Marvel add-ons. The free open source version is called SIEMonster. SIEMonster

is a free open source unlimited use version and comes complete with dashboards, plugins, rules, incident response tools and alerting to make a functioning SIEM and contribute to your Security Operation Center (SOC). Included is an open source ticketing system for Incident Response recording, reporting and raising tickets to other analysts for shift changes as well as handy documentation and know issues whiteboard. Item such as open tickets is fed into the dashboards for easy viewing.

We have also included an open source vulnerability scanner OpenVAS which can be used to scan your end points and visualize risks in your dashboard and linked to a word maps so you can visualize where the issues are across the world. If you already have a commercial scanner such as Nessus or McAfee these can be fed into the dashboard as well.

The solution can be either onsite in a data centre or in the cloud such as AWS. This solution makes it simple for businesses to use open source SIEM technologies without the development headaches, documentation integration, and unlimited use and is affordable which all other products don't provide. SIEMonster is completely scalable, you can download a single instance VMware image or a 3 node cluster and syslog engine or multi node clusters in each geographic region.

After the successful development and roll out of SIEMonster into an International stock listed company with over 20,000 seats, it made sense to allow companies to use our built system for their own environments. SIEMonster can take alerts from anything that gives an event/alert and fully integrates with any vulnerability scanning products you are running for a central dashboard of risks and alerts.

http://www.cso.com.au/article/587763/how-bluescope-cso-saved-big-an-open-source-global-security-operations-centre/

Kustodian who provide Penetration Testing and Security Operation Architecture and SOC monitoring using commercial and open source products, have made the executive decision to only provide open source solutions that are completely free with no licensing or node limitations and make it available to everybody.

http://www.cso.com.au/article/588265/kustodian-goes-open-source-only-after-success-bluescope-soc/?utm_campaign=online-data-security-briefing-2015-11-10&utm_medium=newsletter&eid=-302&utm_source=online-data-security-briefing

Commercial products and open source solutions lack security design, build, and operation documentation integrating into your companies Information Security Management Systems (ISMS), whether it be aligned to ISO27001, HIPPA or PCIDSS, which causes SIEM integration costs to balloon out. Kustodian have documented these for you. SIEMonster comes with a suite of documentation (Standard Operating Procedures, Detailed Designs, DR fail over, Backups, installation guides etc.) which can slot into your existing ISMS program.

Kustodian want the communities help in developing this solution going forward and in return we will continue to advance the development of the product in regular version updates with your input and our experience in our own rollouts in commercial organisations. This product will remain completely free and with unlimited use. So rest assured you won't be hit with a support license fee in the future. Of course if your company needs additional enterprise support, custom plugins for complex equipment Kustodian can provide that as we do with our commercial clients.

CEO of Kustodian – Chris Rock

"As a Security Professional, SIEM provides an essential tool in any environment, however commercial and opens source products licensing cost models, licensing node limitations really annoyed me. Documentation integration costs also needed to be factored in to any roll out project and a lot of documentation for SIEMS was non-existent or not sufficient.

Open Source frameworks or products like Cisco Open stack or ELK are fantastic, but developing a functioning SIEM/SOC takes a lot of skill and development which not all companies want risk or invest into. These products are like building a car, they provide you 1000's of parts and then expect you to put it all together and learn from trial and error not documentation.

After Kustodian successfully built and rolled out a SIEM for one for one of our clients, and then another client, we wanted to share and develop this solution for everybody to use. As the product matures and the community develops dashboards and plugins we can all take this product into the future. This is not a Tenable Nessus Model where we turn free into a chargeable model. The product will remain open and free.

1.2 Help

For any additional help or questions please contact chris@siemonster.com

1.3 License

1.4 Contact

Anything to ask, just contact chris@siemonster.com

CHAPTER 2

Indices and tables

- genindex
- modindex
- search