BUILDING A POWERFUL CYBERSECURITY ARSENAL

Free & Open Source Tools

HOMAND

Introduction

Strapped for resources, but still want to build an effective security program? The right people and processes set a strong foundation, but at some point, you also need tools to help your team scale and ensure your organization stays protected.

There are many security vendors out there, many with great technology that unfortunately comes with a hefty price tag. At smaller or medium-sized organization, often the security team does not have ability to make large million-dollar+ purchases on security products - yet is still mandated to protect their business against many of the same types of threats. We've put together a guide on how to build a powerful security tools arsenal for those of us who don't have a lot to budget to spend on products.

Approach

The right approach is to always invest in people and strategy first. Too many security organizations purchase expensive products without a clear understanding of how to deploy or use them (leading to the phenomenon of seeing expensive servers sitting in boxes in data centers, untouched). To avoid wasteful spend, the smart security leader will look first at hiring great staff and focus on understanding what the team is trying to accomplish before

selecting a product or tool to try to address an issue. Without measurable goals, it is difficult to understand if a particular product is going to help and is worth the ROI.

Free and Open Source tools can provide a great and affordable way to accomplish common security-team tasks like server hardening, security monitoring, and incident response without purchasing expensive products.

Even if the free or open source solution ultimately will not fit your needs, it can also provide a good proof-of-concept to demonstrate a use case for a product and justify why your organization needs to make a purchase. If your organization is not convinced you need to purchase an endpoint security product, for example, implementing a limited deployment of a free endpoint and/or AV solution to demonstrate that there are threats you are missing on the endpoint can provide a powerful business case.

Starting with an open source deployment first, then moving to a commercial solution as your organization scales is also another viable path. Alternatively: consider that it is not uncommon that some commercial solutions work well at small scale, and later down the line you may need to use open source technologies on commodity hardware to accomplish the same tasks effectively and cost-efficiently when the organization is large.

Evaluating the Costs of an Open Source Deployment

Before you deploy an open source solution, you should thoroughly understand what you are trying to accomplish and ensure your staff has the skills and bandwidth to make a successful evaluation (or that you can bring in outside resources like consultants to support your efforts). These tools are often harder to deploy than commercial solutions, and they do not come intrinsically with support, so they may require a more sophisticated team that is comfortable with tasks like building from source code and writing their own deployment scripts.

Many open source tools are not well-documented, so your team must be comfortable diving in and figuring out tools via internet research, forums articles, blogs, and chat rooms, and just exploring the software themselves. Projects like Security Onion are dedicated to lowering the bar for using a lot of these tools, and our very own **Komand Komunity** provides helpful guides for the defender that is considering open source solutions.

Before you attempt a widespread deployment of an open source solution, it's a good idea to implement a limited scope proof-of-concept evaluation that can help you understand factors like performance, management/operations overhead, and scalability.

Our Recommended Tools

We've outlined some open source or free resources for the security team that doesn't have a lot of budget, and why we think you'll love them. We've grouped them by category:

Network Security Monitoring

Host Security

Log Collection/Aggregation

App Security

SIEMs and Event Consoles

Malware Analysis

Threat Intel

Network Security Monitoring

Security Onion is a great asset in the defender's toolkit. It is a Linux distro for intrusion detection, network security monitoring, and log management, and comes bundled with a variety of the free and open source tools mentioned in this article - pre-installed and continuously updated so you don't have to mess around with difficult configurations.

Bro is a powerful network security monitoring tool that features an event based scripting language. Bro is also scalable across hosts with its clustered design. Out of the box, Bro records detailed protocol logs of all the traffic it sees, and performs malware hash lookups on all the files it sees traversing the network, among other things. It's scripting language that allows one to write both simple and complex detections of network traffic and files, as well as making external calls to integrate with your environment's hosts such as firewalls.

Suricata is a multi-threaded intrusion detection system that supports the snort-like rule language and has the ability to integrate with many frontends and tools. It's fast, powerful, and keeps getting better. It has support for complex detections and integrations using Lua. With a ruleset, it will begin identifying and alerting on suspicious and malicious traffic on your network.

Snort is a popular intrusion detection system that uses a common rule and alert format. It's been around for a long time and has the most integrations available. It identify and alerts on suspicious and malicious traffic.

Wireshark is the world's most powerful and advanced packet analyzer/sniffer. It provides an easy way to examine network traffic at the protocol level and deeper to diagnosis and understand network issues as well as investigate malicious traffic. It features nice graphing and stats tools as well as providing the ability to export data such as files from network traffic.

TCPDUMP

Tcpdump is network traffic analyzer that is not as feature rich as Wireshark, but has a major advantage of being available by default on many unix-like operating systems. Tcpdump helps you analyze packets at a deeper level, but requires a greater knowledge of protocols to use efficiently.

argus

ARGUS is a program that records bi-directional network flows and provides a suite of tools for analyzing the flows. At a high level, you can quickly begin to ask questions like which IP addresses did machine X talk to. Looking at flow data allows you to get answers to higher level questions more quickly than digging into packets.

SiLK

SiLK is another suite of flow tools. At a high level, you can quickly begin to ask questions like which IP addresses did machine X talk to. Looking at flow data allows you to get answers to higher level questions more quickly than digging into packets.

Netsniff-NG Toolkit is a suite of high performance networking tools. The Netsniff-ng tool is a good choice for Full Content Packet (FPC) capture which allows the storage of all network transactions. It supports multiple I/O mechanisms and the latest related kernel packet processing features. Recording all events allows one to ask questions accurately about a previous point in time. Netsniff-ng is used to perform FCP in the Security Onion distribution.

Stenographer

Stenographer is another Full Content Packet (FPC) tool for buffering packets to disk for intrusion detection and incident response purposes. It's newer and has the ability to write packets to disk very quickly as well as manages storage space for the packet content.Netsniff-ng is used to perform FCP in the SecurityOnion distribution.

Host Monitoring

osquery provides real time visibility into endpoint systems. It accomplishes this by creating a queryable frontend for a SQL-like language which can be used to retrieve information across hosts. Questions like “what ports and processes are currently open on host x“ can easily be answered.

OSSEC is a free and open source host based intrusion detection system. It’s major features are a log analysis engine, a rootkit detection daemon, and a file integrity daemon. It will alert on things such as SSH bruteforce attacks and important file changes right out of the box. It also provides active response scripts to automatically block hosts acting with malicious behavior.

Sagan is a multi-threaded log analysis engine based on the Snort rule language but applied to logs. It supports things like flowbits so you can track activity across multiple log messages and works with existing Snort integrations and frontends.

GRR Rapid Response is an endpoint visibility tool that is used to perform incident response and forensics. You can ask hosts questions as well perform lookups of indicators of compromise such as whether any of your hosts contain a malicious file hash. You are able to query hosts across your network by using management user interface.

Sysdig Falco is a behavioral system monitoring tool for containers. It has a simple rule language which can be used to alert when certain events happen in a container such as the execution of a shell. It's rule language is similar to that of Sysdig.

Fail2Ban is a tool designed to automate the blocking of hosts by analyzing logs. It supports logs from many network based daemons.

AVG or Avast or MalwareBytes

There are a variety of AntiVirus (AV) vendors out there, but if you need a solution that is affordable you can't argue with free. Both AVG, Avast, and Malwarebytes provide free but not open

ClamAV is a Free and Open Source antivirus engine for detecting many types of malware and threats. It's supported on many operating systems and is easy to write and submit virus rules for.

Log Collection/Aggregation

Rsyslog is a powerful syslog daemon with many features and modules. It has a newer and improved syntax style called Rainerscript which resembles simple code. Rsyslog supports RELP to ensure the integrity and arrival of logs as well as has many output plugins for programs such Kafka, MySQL, and Redis. Rsyslog is replacing Syslog-NG and older syslog daemons.

Syslog-NG is a syslog daemon that has nice features such as content filtering and logging over TCP but the best ones are in the commercial version.

ELK or Splunk or ELSA

To do any level of effective investigation on a security alert, you'll need the ability to search and review your logs. All of these solutions provide a nice way to store and search your logs, and even create alerts on top of them to look for custom security events. Splunk's free version caps out at 500MB/day, but is a popular tool.

App Security

Kali Linux is an open source debian distribution that comes with pre-installed pen testing tools. Although not strictly open source for security reasons, Kali provides a great arsenal of tools for testing your application (some of which are listed below). It includes everything from information gathering to exploiting applications to forensics. A complete listing can be found **here**.

Nikto is a web server scanner that searches for default and insecure files, configurations, and programs that could compromise your app or the server on which it resides.

Burp Suite or OWASP Zap

While the Burp Suite commercial edition costs money, the free version is still very useful for inspecting HTTP traffic and doing some ad-hoc web application testing. Zap adds additional functionality by including automated scanners and other manual tools to find security vulnerabilities. It is made for a wide range of security expertise, so it can be used by developers, testers, and security team members.

Naxsi or modsecurity

Concerned about protecting your web apps? We all try to write secure code, but web application firewalls add another layer of protection against app attacks like SQL injection by blocking them before they reach the app.

SIEMs and Event Consoles

OSSIM is an open source SIEM. Maintained by AlienVault, which also sells a commercial version with more features. It includes a few of the aforementioned intrusion detection tools such as OSSEC and Snort to generate events which are then analyzed in the SIEM.

elsa

Enterprise Log Search and Archive (ELSA) is a search and retrieval tool that will help you correlate and ask questions of hosts using log and event data. It's used in Security Onion and can ingest many types of data formats such as Syslog, Bro logs, and intrusion alerts from Suricata and Snort.

sguil

SGUIL is an event console for your network security events that allows you to pivot from a Network IDS event to full packet capture, session information, and other relevant data.

Malware Analysis

VxStream Sandbox or ThreatExpert or Cuckoo Sandbox
Need to examine a binary to see what happens when it runs? A sandbox can be very useful because it will record what a program does when it runs in a virtual machine.

Payload Security, Threat Expert, and other vendors provides free hosted services where you can upload your suspicious binary and allow them to run it on their virtual servers. You will get a nice report showing the what the program did in the sandbox, including screenshots.

Cuckoo allows you to host your own sandbox locally, so you aren't sharing sensitive binaries outside your organization.

VirusTotal acts as a 'meta scanner' for binaries. It aggregates a number of virus scanning engines and will run a binary against all of these engines, providing you a helpful report that can help you evaluate whether a binary is malicious (or not). VirusTotal also provides a URL scanning capability. It is free to use via the website or via API (for a limited number of API calls).

Threat Intel

Critical Stack is a free threat intelligence service, intel.criticalstack.com, aggregates a number of free/open source threat intelligence feeds and provides an easy way for you to use this information within your Bro intrusion detection installation (although the intel downloaded is in a convenient CSV format that can also be used elsewhere).

Collective Intelligence Framework (CIF) is a framework that allows you to retrieve, store, query, and create intelligence feeds and output them to various formats such as iptables and snort rules. It supports multiple intelligence types such as IP addresses, domains, URLs, and file hashes. It has support for federation which allows intel to be shared within or across trusted organizations. You can perform lookups such as is this IP or domain name known to be associated with malicious activity.

Conclusion

Open Source tools are a great alternative to resource-strapped organizations. However, they are not a replacement for people or strategy. The smart security leader will invest in people first, no matter if they use commercial solutions or open source tools.

Additionally, open sources tools may not be for everyone. But they can provide great benefits to teams that are relatively scrappy and willing to put up with some of the warts. The price-point isn't too bad, either... Free!

Komand is a security orchestration and automation platform that gives your team the power to quickly automate and optimize security operations, with no need for code. Connect your tools, build workflows, and utilize human decisions to accelerate incident response and move security forward, faster.

KOMAND