AT&T Cybersecurity

AT&T Business

Beginner's guide: Open source intrusion detection tools

Is open source security a good route?

Threat and intrusion detection have become a top priority in cybersecurity, making it more important than ever before. If you aren't already running an intrusion detection system (IDS) in your network, you should start now.

AT&T Business

Introduction

There are a wealth of great tools out there that can dramatically improve the security of your network. Open source security goes back decades, and there is a large, active community behind many of the tools. In fact, some of these tools are used by commercial security vendors in their products, and these vendors contribute to the tools to keep them current.

Before getting started, we'd be remiss not to address the pros and cons of going the open source route.

Open source might be a good solution for you if:

- Your company has the expertise in both security and system administration needed to deploy several tools with only community support.
- You want "complete control" over your security architecture and are willing to do extra work to make that happen.
- You develop a plan for keeping these tools up-to-date. Unlike most software, failure to keep security tools current with the latest versions and security updates (which may come weekly, daily, or even hourly) renders the tools themselves almost useless after a short time.
- You have a very low budget to buy products, but have the staff needed to maintain open source tools.
- Your use case and security concerns don't align well with commercial products.

Open source is easier than ever to install and maintain. However, on the "con" side, there are a few important concerns. If you are going to design a security solution for your company, please keep in mind:

- You will have to do your own support. There are great communities behind some of these tools, but you are the only one who is responsible for your network. You'll have to use your "phone a friend" if you need a lifeline.
- Many of these tools need "content"—signatures, rule updates, and the like. You will be responsible for finding these in the community, or purchasing a threat feed from a commercial source. As stated above, security tools are only as good as their content. Otherwise, your network will have an amazing defense—against last year's threats.
- Combining different tools can be challenging even for a seasoned architect. You'll need to understand what threats you are protected from and what gaps remain.

IDS basics

An IDS is a visibility tool. It gives your administrators and security analysts clarity on your network's security posture. It allows tangible insight into modern network security threats, as a part of your organization's network security monitoring strategy (NSM). An IDS can improve your team's understanding of your network activity, explore cyber threat intelligence, discover policy violations, and most importantly, help to protect your assets.

In more technical terms, an IDS is a network security tool built to detect intrusion attempts against a targeted computer system or application. These threats can be detected using signature-based or anomaly-based intrusion detection techniques, further discussed later in this white paper. An IDS analyzes network traffic for potentially malicious activity. Whenever a suspicious activity is detected, a network "event" will be logged, and a notification sent to the administrator.

Looking for attacks isn't the only use case for an IDS. You can also use it to identify unauthorized systems, malicious programs and files, and find violations of network policy. An IDS will tell you if an employee is using Gchat™, uploading to Box®, or spending all their time watching Netflix® instead of working.

In the realm of intrusion detection, there are primarily two methods of security management for computer networks: network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). More on these later.

It's essential to deploy IDS everywhere you're storing or processing critical applications and data, which could stretch from your internal network and on-premises data centers to public cloud environments. When evaluating IDS solutions, it's important to evaluate whether you need an IDS that can monitor both your cloud and on-premises assets.

IDS detection techniques

There are two primary threat detection techniques: signature-based detection and anomaly-based detection. These detection techniques are important when you're deciding whether to go with a signature or anomaly detection engine, but vendors have become aware of the benefits of each, and some are building both into their products. Learning their strengths and weaknesses enables you to understand how they can complement one another.

Signature-based IDS tools

With a signature-based IDS, aka knowledge-based IDS, there are rules or patterns of known malicious traffic being searched for. Once a match to a signature is found, an alert is sent to your administrator. These alerts can discover issues such as known malware, network scanning activity, and attacks against servers.

Anomaly-based IDS tools

With an anomaly-based IDS, aka behavior-based IDS, the activity that generated the traffic is far more important than the payload being delivered.

An anomaly-based IDS tool relies on baselines rather than signatures. It will search for unusual activity that deviates from statistical averages of previous activities or previously seen activity. For example, if a user always logs into the network from California and accesses engineering files, if the same user logs in from Beijing and looks at HR files this is a red flag.

Both signature-based and anomaly-based detection techniques are typically deployed in the same manner, though one could make the case you could (and people have) create an anomaly-based IDS on externally-collected netflow data or similar traffic information.

Advantages and disadvantages

Fewer false positives occur with signature-based detection but only known signatures are flagged, leaving a security hole for the new and yet-to-be-identified threats. More false positives occur with anomaly-based detection but if configured properly it catches previously unknown threats.

Snort

Ah, the venerable piggy that loves packets. Many people will remember 1998 as the year Windows 98 came out, but it was also the year that Martin Roesch first released Snort®. Although Snort wasn't a true IDS at the time, that was its destiny. Since then it has become the de-facto standard for IDS, thanks to community contributions.

It's important to note that Snort has no real GUI or easy-to-use administrative console, although lots of other open source tools have been created to help out, notably Snorby, and others like BASE and Sguil. These tools provide a web front end to query and analyze alerts coming from Snort IDS.

Snort summary:

- Great community support
- According to Snort's website, features include:
  - » Modular design
  - » Multi-threading for packet processing
  - » Shared configuration and attribute table
  - » Use a simple, scriptable configuration
  - » Plugin framework, make key components pluggable (and 200+ plugins)
  - » Auto-detect services for portless configuration
  - » Auto-generate reference documentation
  - » Scalable memory profile
  - » Rule parser and syntax (support sticky buffers in rules)
- A plugin for Snort is available for AlienVault® Unified Security Management™ (USM) from AT&T Cybersecurity

Suricata

What's the only reason for not running Snort? If you're using Suricata® instead.

Although Suricata's architecture is different than Snort, it behaves the same way as Snort and can use the same signatures.

What's great about Suricata is what else it's capable of over Snort. There are third-party open source tools available for a web front end to query and analyze alerts coming from Suricata IDS.

Suricata summary:

- Great community support
- According to Suricata's website, features include:
  - » High performance: Multi-threaded, scalable code base
  - » Multipurpose Engine: NIDS, NIPS, NSM, offline analysis, etc.
  - » Cross-platform support: Linux,® Windows, macOS, OpenBSD, etc.
  - » Modern TCP/IP support including a scalable flow engine, full IPv4/IPv6, TCP streams, and IP packet defragmentation
  - » Protocol parsers: Packet decoding, application layer decoding
  - » HTTP engine: HTTP parser, request logger, keyword match, etc.
  - » Autodetect services for portless configuration
  - » Lua scripting (LuaJIT)
  - » Application-layer logging and analysis, including TLS/SSL certs, HTTP requests, DNS requests, and more
  - » Built-in hardware acceleration (GPU for network sniffing)
  - » File extraction

Bro*

Bro®, sometimes referred to as Bro-IDS, is a bit different than Snort and Suricata. In a way, Bro is both a signature and anomaly-based IDS. Its analysis engine will convert traffic captured into a series of events. An event could be a user login to file transfer protocol (FTP), a connection to a website or practically anything. The power of the system is what comes after the event engine, and that's the Policy Script Interpreter. This policy engine has its own language (Bro-Script) and it can do some very powerful and versatile tasks.

If you're an analyst and you've wondered "How can I automate some of my work?" then this is the tool you've been looking for. Want to download files seen on the wire, submit them for malware analysis, notify you if a problem is found, then blacklist the source and shutdown the user's computer who downloaded it? Want to track the usage patterns of a user after they've contacted an IP from a reputation database? Again, then this is the tool for you.

If you're not an analyst then this tool will have a challenging learning curve. Since it was developed as a research tool, it didn't initially focus on things like GUIs, usability, and ease of installation. While it does numerous cool things out of the box, many of those things aren't immediately actionable and may be difficult to interpret.

There's no native GUI, but there are third-party open source tools available for a web front end to query and analyze alerts coming from Bro-IDS. Consider ELK stack.

Bro summary:

- Great community support
- According to Bro's website, features include:
  - » Comprehensive traffic logging and analysis
  - » Powerful and flexible event-driven scripting language (Bro scripts)
  - » Deploys on UNIX®-based systems, including Linux, FreeBSD®, and MacOS
  - » DNS/FTP/HTTP/IRC/SMTP/SSH/SSL/other protocol support
  - » Fully passive traffic analysis with network tap or monitoring port
  - » Near-real-time and offline analysis
  - » Cluster support for large-scale deployments
  - » Comprehensive IPv6 support
  - » IDS-style pattern matching
  - » File extraction
  - » Extensible architecture
  - » Analysts can use Bro for automation (file extraction, malware analysis, blacklisting, track usage patterns, research work, etc.

*Bro is now Zeek, but much of their documentation still goes by the long-standing name Bro.

Host-based IDS (HIDS)

Host-based intrusion detection systems (HIDS) work by monitoring activity occurring internally on an endpoint host. HIDS applications (e.g. antivirus software, spyware-detection software, firewalls) are typically installed on all internet-connected computers within a network, or on a subset of important systems, such as servers. This includes those in public cloud environments.

HIDS search for unusual or nefarious activities by examining logs created by the operating system, looking for changes made to key system files, tracking installed software, and sometimes examining the network connections a host makes.

The first HIDS systems were basic, usually just creating MD5 hashes of files on a recurring basis and looking for discrepancies, utilizing a process dubbed file integrity monitoring (FIM). Since then, HIDS have grown far more complex and perform a variety of useful security functions and will continue to grow. This includes modern endpoint response (EDR) capabilities.

If your organization has a compliance mandate, such as for PCI DSS, HIPAA, or ISO 27001, then you may require HIDS to demonstrate file integrity monitoring (FIM) as well as active threat monitoring.

Since local HIDS can be compromised at the same time the OS is, it is very important security and forensic information leave the host and be stored elsewhere ASAP to avoid any kind of tampering or obfuscation that would prevent detection.

OSSEC

In the realm of full-featured open source HIDS tools, there is OSSEC and not much else. The great news is OSSEC is very good at what it does and is rather extensible.

OSSEC runs on almost any major operating system and includes client/server based management and logging architecture, which is very important in a HIDS system.

OSSEC's client/server architecture incorporates this strategy by delivering alerts and logs to a centralized server where analysis and notification can occur even if the host system is taken offline or compromised. Another advantage of client/server architecture is the ability to centrally manage agents from a single server. Since deployments can range from one to thousands of installations, the ability to make global changes from a central server is critical for an administrator's sanity.

When discussing OSSEC (and other HIDS) there is often anxiety over installing an agent or software on critical servers. It should be noted that the installation of OSSEC is extremely light (the installer is under 1MB) and the majority of analysis actually occurs on the server which means very little CPU is consumed by OSSEC on the host.

OSSEC also has the ability to send OS logs to the server for analysis and storage, which is particularly helpful on Windows machines that have no native and cross-platform logging mechanisms.

OSSEC summary:

- Great community support
- According to OSSEC's website, features include:
  - » File integrity monitoring (FIM)
  - » Log monitoring collects, analyzes, and correlates system logs
  - » Rootkit detection, which searches for system modifications similar to rootkits
  - » Active response can invoke automated response action when alerts are triggered
  - » Client/server architecture
  - » Multi-platform support (Linux, Windows, MacOS, etc.)
  - » Supports compliance requirements for FIM
  - » Near-real-time and configurable alerts
  - » Integration with current infrastructure
  - » Centralized server for mass policy management
  - » Agent and agentless monitoring
- A plugin for OSSEC is available for AlienVault USM

Samhain Labs

Samhain is probably the only HIDS open-source that gives OSSEC a run for its money. But it's very much the case of "same but different" when comparing the two. Samhain has the same client/server architecture but doesn't require it like OSSEC does. The agent itself has a variety of output methods, one being a central log repository but includes others like Syslog, email, and RDBMS. There is even an option to use Samhain as a standalone application on a single host.

Another important difference is where analysis occurs. Unlike OSSEC, the processing occurs on the client itself, which has operational implications. From a practical point of view, care must be taken it doesn't overload a busy server and interfere with operations. From the security point of view, having the brains on the endpoint invites hackers to deactivate the tool so warnings aren't issued.

Samhain summary:

- Great community support
- According to Samhain's website, features include:
  - » File integrity monitoring (FIM)
  - » Log file monitoring and analysis
  - » Rootkit detection
  - » Port monitoring
  - » Detection of rogue SUID executables and hidden processes
  - » Multi-platform support
  - » Centralized logging and maintenance
  - » Client/server architecture (mostly)
  - » Variety of output methods (e.g. syslog, email RDBMS)
  - » Can be used as a standalone application on a single host

OSQuery as a security tool

OSQuery is a difficult to classify security tool. It is part host intrusion detection, part file integrity monitoring, part system monitor. Basically, OSQuery exposes important operating system configuration elements and status in a high-performance relational database. Administrators can write SQL queries to explore operating system data. OSQuery builds SQL tables representing abstract concepts such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events or file hashes.

If this sounds both powerful and complex, you're right. OSQuery is the ultimate "roll your own" tool for system administration and security applications where insight into what is happening on your endpoints is needed. Administrators can query the database to figure out, for example, which systems have a particular malware process running on them or if files have been modified in specific ways by a threat actor. But you'll need third party tools and script development to get the most out of OSQuery.

OSQuery summary:

- Endpoint visibility tool allows remote query of details of configurations
- Tool is under active development and used by many security vendors
- Requires extensive scripting or third party scripts to get true value from the tool
- According to OSQuery's website, features include:
  - » Supports Windows, Linux, MacOS, FreeBSD
  - » Exposes entire endpoint configuration as a relational database for query by external applications
  - » File integrity monitoring (FIM)
  - » Malware/signature detection via YARA
  - » Process auditing
  - » APIs for remote management (via your scripts or third party scripts)
  - » Log collection via Syslog

File integrity monitoring (FIM) only

Many file integrity monitoring (FIM) tools get categorized with HIDS since FIM involves threat detection, so let's talk about them.

FIM is a tool that validates operating system and specified application file integrity by comparing current versions with known valid versions, alerting your administrator whenever they are modified. This is important because changes on critical servers often signal a breach has occurred.

Some FIM tools are actively developed while others haven't been updated in years. Open Source Tripwire® and AFICK are two open-source FIM options. For standalone Unix-based systems, consider checking out rootkit-finding file integrity checkers, such as chkrootkit, rkhunter, or Unhide. The unique rootkit-finding mechanism makes these solutions worth considering. Proprietary solutions are also available for Windows.

The AlienVault USM platform provides built in FIM capabilities to drive threat detection technologies and to help accelerate your cybersecurity compliance efforts.

Final thoughts

Hopefully this guide has helped you understand some of your open source options. As shown here, there's never before been so many choices or a broader set of tools available. With careful planning, and a plan for ongoing maintenance, you can improve your network security with these tools.

> **If you are going the open source route, it will be very important to stay "tuned in" to the developments in cybersecurity. The current moment finds us in the middle of an evolution in our approach to security.**

We are seeing endpoint detection and response (which is partly addressed by OSQuery), machine learning based user behavioral analytics, and even honeypots and deception moving from experimental technologies used by cutting-edge large enterprises to more mainstream deployments. As these become more commonplace, and new ones are developed, you'll need to further augment your open source strategy with new tools, or hope that the community adds support for them into a product you have already deployed.

How AlienVault USM can help

The AlienVault USM platform delivers built-in intrusion detection systems tools as part of an all-in-one unified security management console. It includes built-in host intrusion detection (HIDS), network intrusion detection (NIDS), as well as cloud intrusion detection for public cloud environments including AWS and Microsoft Azure, enabling you to detect threats as they emerge in your critical cloud and on-premises infrastructure.

To ensure that you are always equipped to detect the latest emerging threats, AT&T Alien Labs security research team delivers continuous threat intelligence updates directly to the USM platform. This threat data is backed by the AlienVault Open Threat Exchange® (OTX™)—the world's first open threat intelligence community.

AlienVault USM helps you:

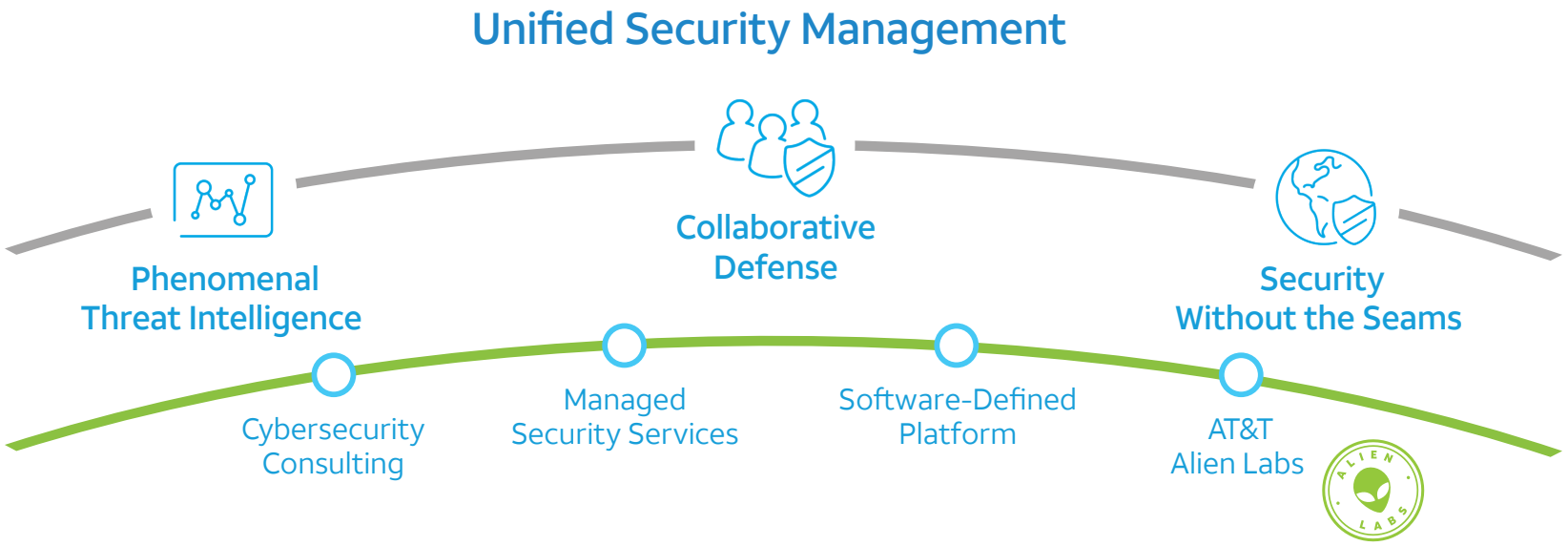
- Leverage intrusion detection for any environment with built-in cloud IDS, network IDS, and host-based IDS, including file integrity monitoring (FIM)
- Use the Kill Chain Taxonomy to quickly assess threat intent and strategy
- Make informed decisions with contextual data about attacks, including a description of the threat, its method and strategy, and recommendations on response
- Use automatic notifications so you can be informed of key threats as they happen
- Work more efficiently with powerful analytics that uncover threat and vulnerability details—all in one console

AlienVault® Unified Security Management® (USM) by AT&T Cybersecurity delivers powerful threat detection, incident response, and compliance management in one unified platform. It combines all the essential security capabilities needed for effective security monitoring across your cloud and on-premises environments, including continuous threat intelligence updates.

Features	AlienVault USM	Traditional SIEM
Management		
Log management	✓	✓
Event management	✓	✓
Event correlation	✓	✓
Reporting	✓	✓
Security monitoring technologies		
Asset discovery	Built-in	$$ (3rd-party product that requires integration)
Network IDS	Built-in	$$ (3rd-party product that requires integration)
Host IDS	Built-in	$$ (3rd-party product that requires integration)
File integrity monitoring	Built-in	$$ (3rd-party product that requires integration)
Cloud monitoring	Built-in	$$ (3rd-party product that requires integration)
Incident response	Built-in	$$ (3rd-party product that requires integration)
Endpoint detection and response	Built-in	$$ (3rd-party product that requires integration)
Vulnerability assessment	Built-in	$$ (3rd-party product that requires integration)
Additional capabilities		
Continuous threat intelligence	Built-in	$$ (3rd-party product that requires integration)
Unified management console for security monitoring technologies	Built-in	$$ (3rd-party product that requires integration)

About AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning – helping to enable our customers around the globe to anticipate and act on threats to protect their business.



This document is intended to include general information for beginners learning about open source intrusion detection. Use of names of third party companies in the document are for informational purposes only and do not constitute any endorsement by AT&T Cybersecurity.

AT&T Business