

Review on Intrusion Detection and Intrusion Prevention Systems

What is an Intrusion Detection System?

IDS is a system that monitors traffic for suspicious activities. It issues alerts on detecting suspicious system behavior. Any malicious program or lines of code get reported to the admin using an existing set of data. Although IDS triggers alerts for suspicious activities, it often gets exposed to false threats. It is the reason why an IT firm needs to fine-tune IDS when it installs the software.

How Does An IDS System Differ From IPS?

An intrusion detection system assesses network traffic and inspects signs of possible cyber-attacks. Intrusion prevention systems (aka IPS) inspect encrypted data packets. It can stop data packets from getting delivered based on the nature of network traffic.

The main difference between IPS and IDS is that the former is a control system. IDS is a system used for monitoring data traffic. IDS compares network activity to an existing threat database. IDS takes help from an individual to look at the data traffic.

What Are The Types Of IDS Systems?

- NIDS (aka network detection system) gets installed at checkpoints. NIDS monitors data traffic from all devices localized on the network.
- HIDS (aka host detection system) gets installed on multiple hosts or servers across the network. HIDS detects traffic from the specific device and alerts the system admin to detect suspicious activities.
- APIDS (aka protocol-based detection system) is an agent that resides on a pool of servers. It monitors data traffic by interpreting communication on app-based protocols.
- CIDS (aka Hybrid detection system) is the resultant combination of one or more IDS systems. It needs system admins to configure host agents with network protocols to get a complete view of the system.

Intrusion Detection Systems (IDS) Vs. Intrusion Prevention Systems (IPS)

Sr.No.	Intrusion Detection System	Intrusion Prevention System
1.	Intrusion detection systems are monitoring and detection tools.	An intrusion prevention system is a prevention control system.

2.	The tools of the Intrusion Detection System don't take action on their own.	The control system of IPS accepts and rejects the packets based on a certain ruleset.
3.	An intrusion detection system requires human intervention or another system to look at the results.	Intrusion prevention system requires regular updating of the new possible data threats.
4.	An intrusion detection system is not inline so traffic doesn't require to flow through it.	Intrusion Prevention System is inline where traffic needs to flow through it.
5.	There are two types of IDS: Network Intrusion Detection System (NIDS) and Host-based IDS (HIDS).	There are 4 types of IPS: Network-based IPS (NIPS), Wireless IPS (WIPS), Host-based IPS (HIPS) and Behavior IPS.

How to Choose the Best Intrusion Detection System?

There is numerous intrusion detection system available in the market but to choose the best among all the available system requires a lot of research. Here we have explained various factors you need to keep in mind while choosing the best intrusion detection system. These are mentioned as follows:

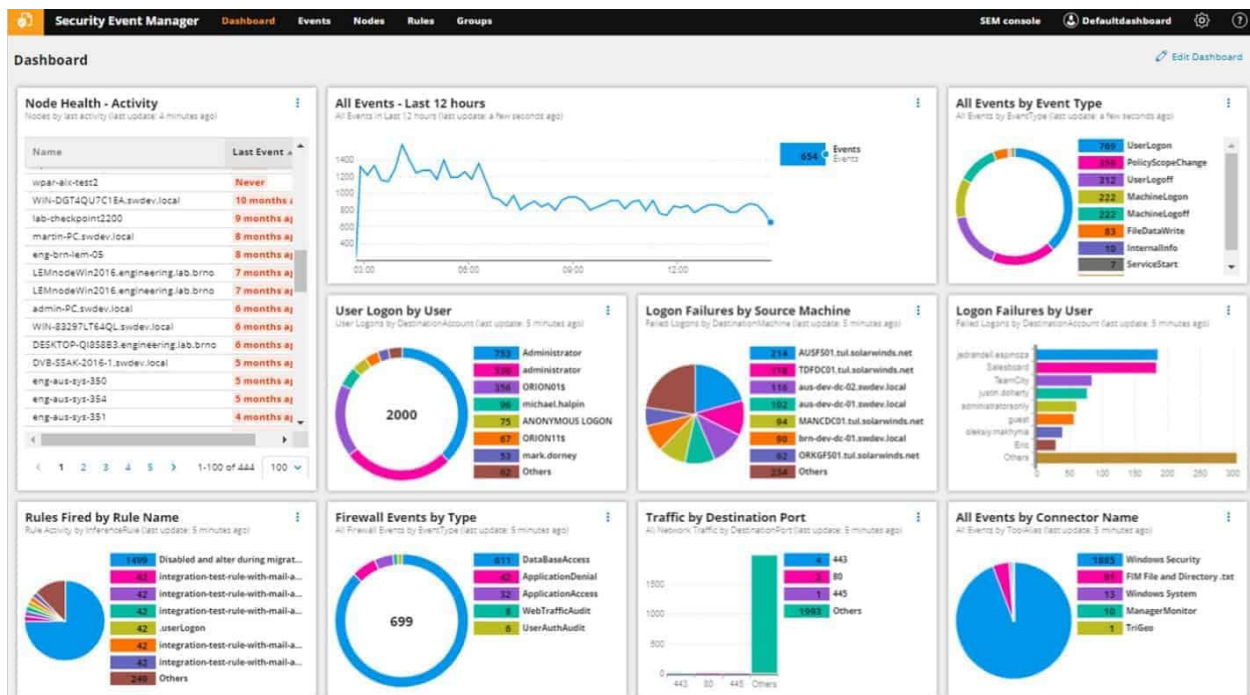
- First, try to research out your business needs and systems that are available.
- Is the IDS system going to support the current network?
- Consider the budget for both IDS/IPS systems.
- Wireless/Wired network support
- What happens If something goes wrong with the current system
- Whether the system can be scaled to bigger with the existing system
- Interoperability
- Timely updates to new or modified signature for prevention/detection of threats.

List of the Best Intrusion Detection Software

Here is the top 10 list of best intrusion detection software explained in a detailed manner as follows:

1. SolarWinds Security Event Manager

SolarWinds Security Event Manager is an IDS that runs on a windows server platform. It is best for clients who are having large businesses.



Source: <https://cdn.networkmanagementsoftware.com/wp-content/uploads/5-security-event-manager-main-dashboard.jpg>

Features:

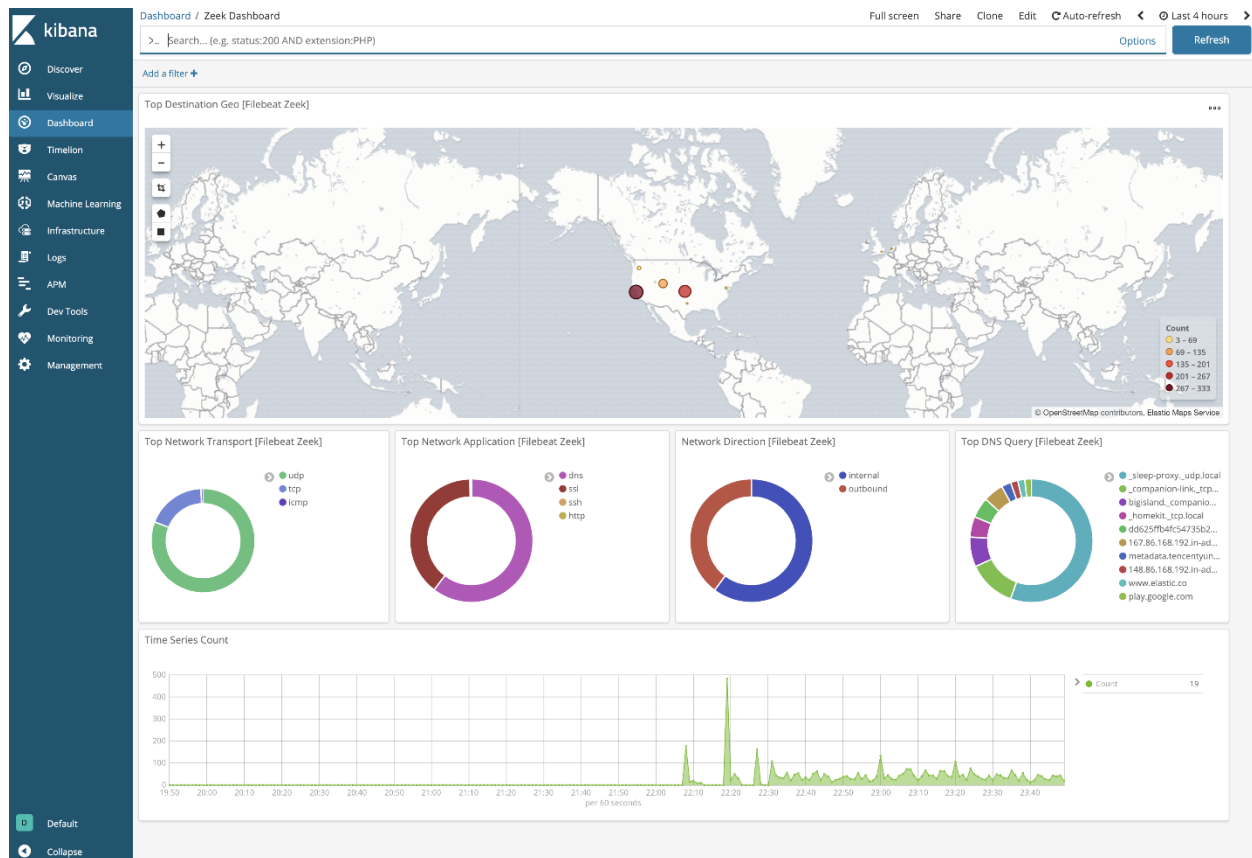
- Real-Time Monitoring
- Compliance Tracking
- Data Visualization
- User Activity Monitoring

Website: <https://www.solarwinds.com/security-event-manager>

Pricing: Pricing starts from \$2613 as a one-time payment with 30 days free trial.

Zeek

Zeek is also known as Bro which is a network-based intrusion detection system (NIDS) that operates on live traffic data. This tool can be installed freely on UNIX, Linux and Macintosh OS platforms.



Source: <https://www.elastic.co/guide/en/beats/filebeat/current/images/kibana-zeek.png>

Features:

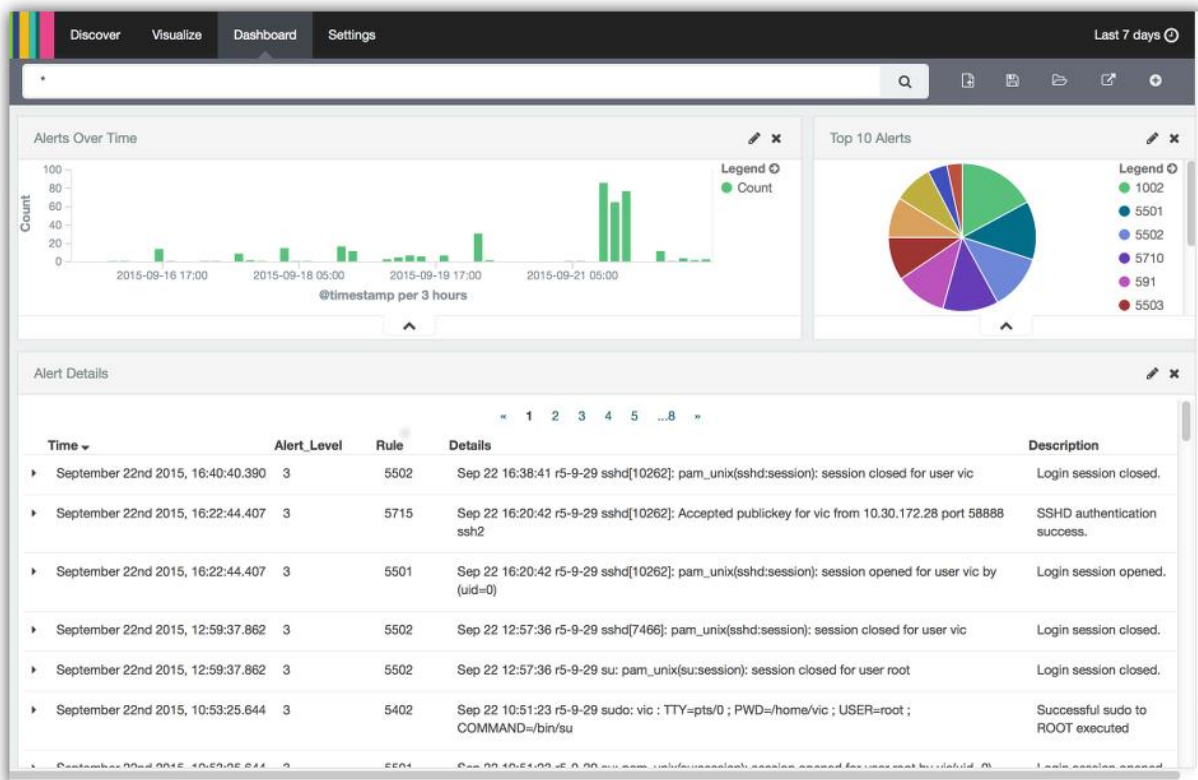
- Open Source with a BSD License
- Analysis of Real-Time Data
- Standard Interface
- IPv6 Support

Website: <https://zeek.org/>

Pricing: Zeek is open-source which is available free to use.

OSSEC

OSSEC is an open-source Host-based Intrusion detection system that is free for usage. It can be run on UNIX, Windows, Macintosh OS and Linux platforms but doesn't have a user interface.



Source: <https://vichargrave.github.io/assets/images/final-dashboard.png>

Features:

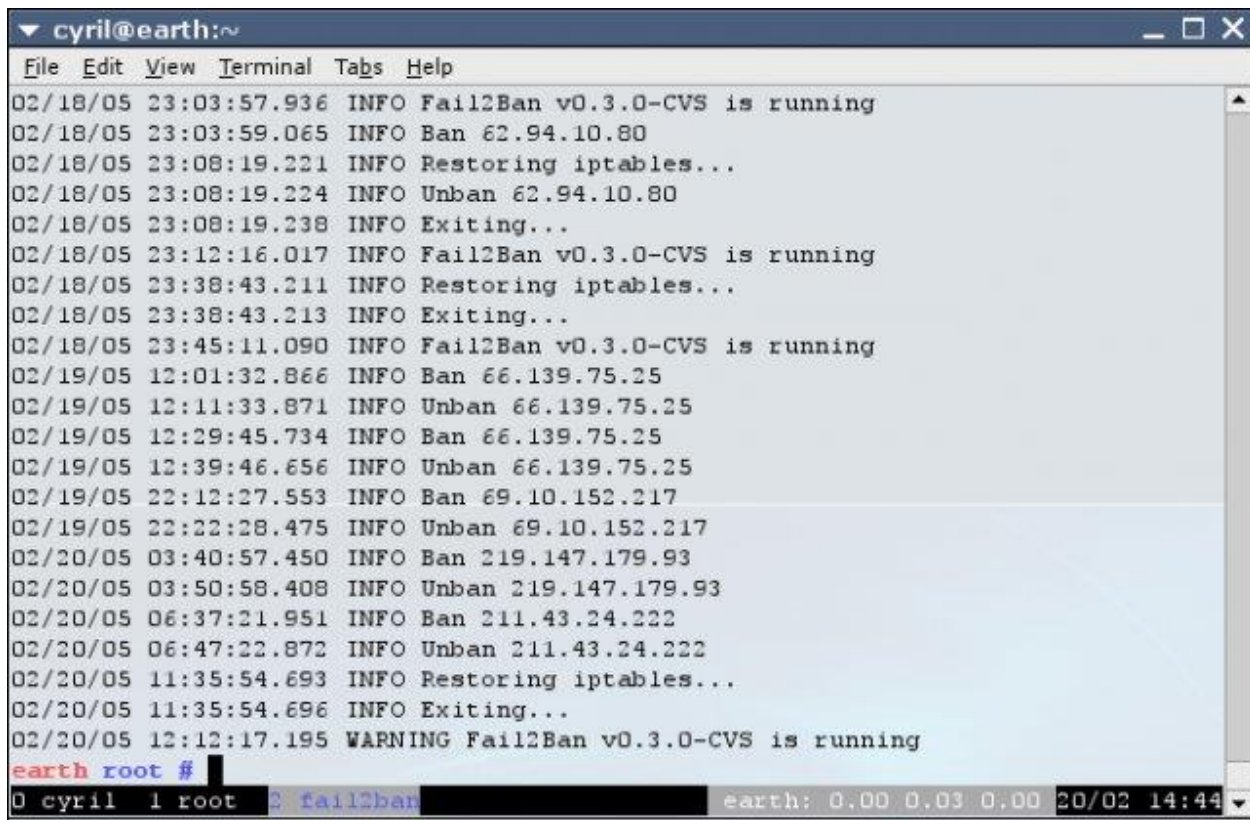
- It is open source
- Log Based IDS
- Active Response
- Malware and Rootkit Detection

Website: <https://www.ossec.net/>

Pricing: As it is open-source it is free to use.

Fail2Ban

Fail2Ban is a lightweight and free Intrusion prevention system that runs on the command line interface and is available on UNIX, Macintosh OS and Linux platforms.



```
▼ cyril@earth:~
File Edit View Terminal Tabs Help
02/18/05 23:03:57.936 INFO Fail2Ban v0.3.0-CVS is running
02/18/05 23:03:59.065 INFO Ban 62.94.10.80
02/18/05 23:08:19.221 INFO Restoring iptables...
02/18/05 23:08:19.224 INFO Unban 62.94.10.80
02/18/05 23:08:19.238 INFO Exiting...
02/18/05 23:12:16.017 INFO Fail2Ban v0.3.0-CVS is running
02/18/05 23:38:43.211 INFO Restoring iptables...
02/18/05 23:38:43.213 INFO Exiting...
02/18/05 23:45:11.090 INFO Fail2Ban v0.3.0-CVS is running
02/19/05 12:01:32.866 INFO Ban 66.139.75.25
02/19/05 12:11:33.871 INFO Unban 66.139.75.25
02/19/05 12:29:45.734 INFO Ban 66.139.75.25
02/19/05 12:39:46.656 INFO Unban 66.139.75.25
02/19/05 22:12:27.553 INFO Ban 69.10.152.217
02/19/05 22:22:28.475 INFO Unban 69.10.152.217
02/20/05 03:40:57.450 INFO Ban 219.147.179.93
02/20/05 03:50:58.408 INFO Unban 219.147.179.93
02/20/05 06:37:21.951 INFO Ban 211.43.24.222
02/20/05 06:47:22.872 INFO Unban 211.43.24.222
02/20/05 11:35:54.693 INFO Restoring iptables...
02/20/05 11:35:54.696 INFO Exiting...
02/20/05 12:12:17.195 WARNING Fail2Ban v0.3.0-CVS is running
earth root #
0 cyril 1 root 0 fail2ban earth: 0.00 0.03 0.00 20/02 14:44
```

Source: https://upload.wikimedia.org/wikipedia/commons/7/7b/Fail2ban_screenshot.jpg

Features:

- Log File Analysis
- Open Source
- Automatic blocking of suspicious IP addresses
- Compatible with Unix and Macintosh OS Systems

Website: http://www.fail2ban.org/wiki/index.php/Main_Page

Pricing: It is open-source that is free to use.

Snort

Snort is a well-known Network-based Intrusion Detection/Prevention System that has a huge community of users. It is widely accepted as many other available Intrusion detections and Prevention systems are built to be compatible with it.

```

C:\Snort\bin>snort -d
Running in packet dump mode

    ---= Initializing Snort ===-
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{2E0BCA4B-09DB-4CB0-AA47-9B8957A92FDD}".
Decoding Ethernet

    ---= Initialization Complete ===-

,,_  -*> Snort! <*-
o"  )~ Version 2.9.11.1-WIN32 GRE (Build 268)
'...' By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2017 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using PCRE version: 8.38 2015-11-23
      Using ZLIB version: 1.2.3

Commencing packet processing (pid=13336)
WARNING: No preprocessors configured for policy 0.

```

Source: <https://www.itprc.com/wp-content/uploads/2018/06/snort.png>

Features:

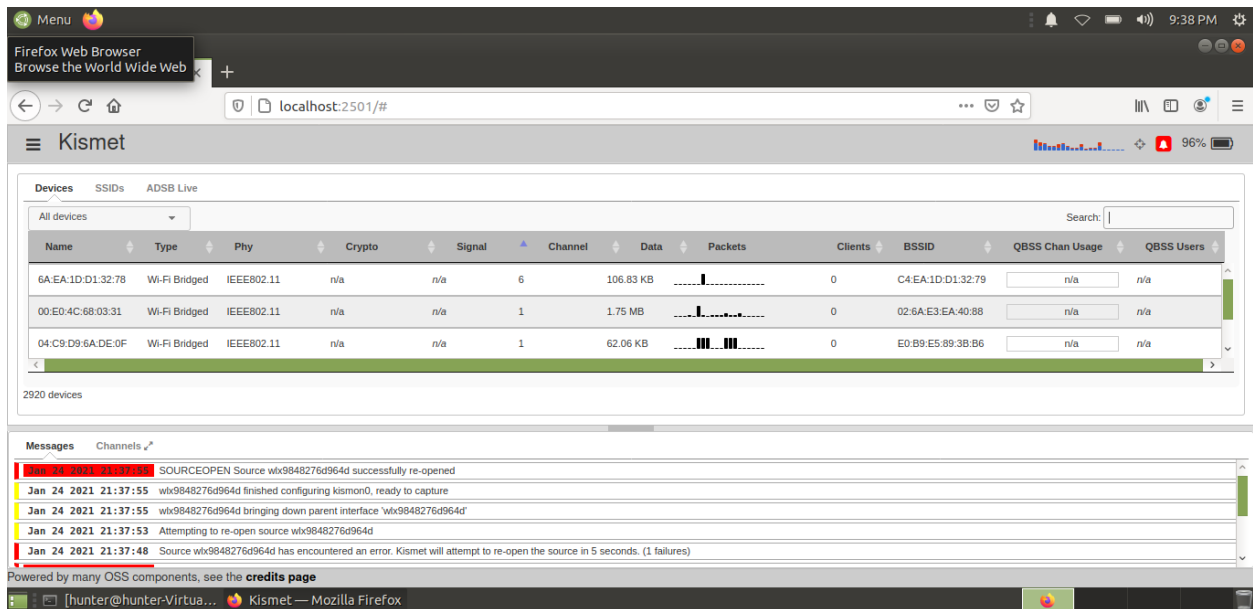
- Open Source
- Cross platform which runs on all operating systems.
- Huge library of prebuilt detection rules.
- Rules can be easily implemented.

Website: <https://www.snort.org/>

Pricing: Snort is free to use but the rule subscriptions starts from \$29.99 for personal use to \$399 for business use annually for both of them.

Kismet

Kismet is a wireless network detector, packet sniffer and IDS which is different from other wireless network detectors. It is the most widely used open-source wireless monitoring tool.



Source: https://upload.wikimedia.org/wikipedia/commons/f/f2/Kismet_Web_UI.png

Features:

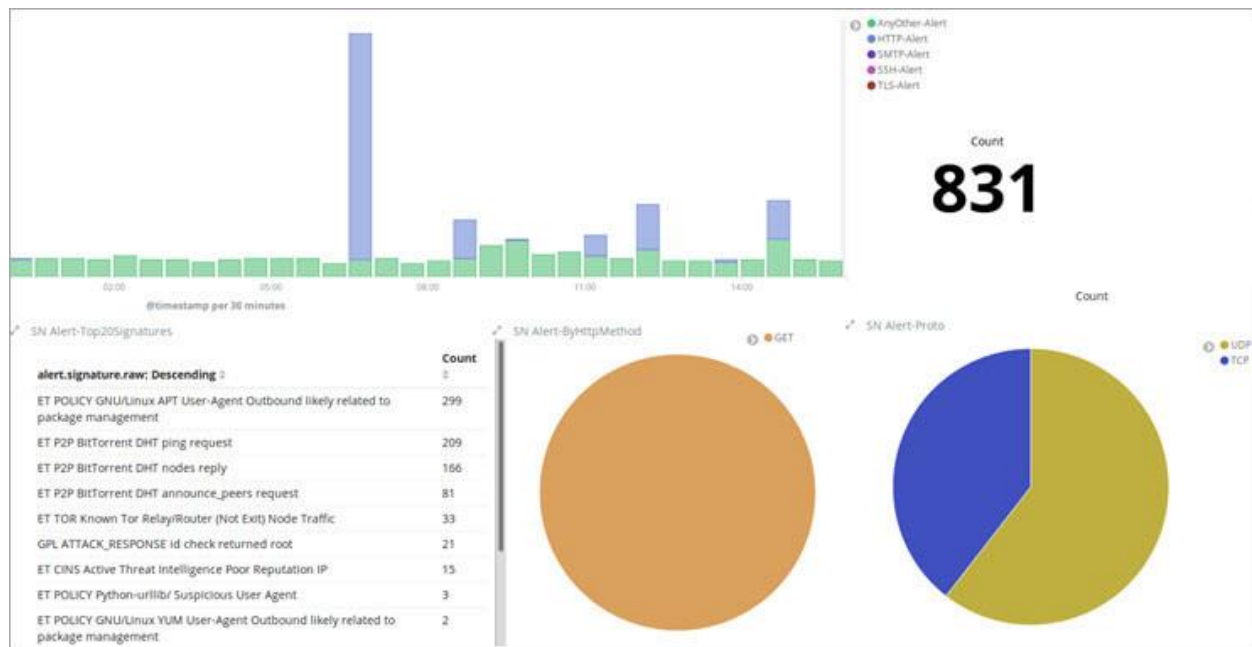
- Open Source Wireless Monitoring Tool
- 802.11 Packet Sniffers
- Client/Server Model Architecture
- Runs on FreeBSD, Linux, NetBSD, OpenBSD and Macintosh OS.

Website: <https://www.kismetwireless.net/>

Pricing: It is open source free software that is distributed under the GNU General Public License.

Suricata

Suricata is an open-source network detection engine that is capable of inline intrusion prevention, offline pcap processing, network security monitoring and real-time intrusion detection.



Source: <https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/12/Suricata.jpg>

Features:

- Open Source
- Lua Scripting
- Automatic detection of protocol
- Integrates easily with the network and can be embedded within numerous open-source and commercial solutions.

Website: <https://suricata.io/>

Pricing: It is freely available to use.

Security Onion

Security Onion is a free open source Linux-based distribution system that combines with other security tools and intrusion prevention systems within the custom-made Linux distribution. This tool includes such as Zeek, Snort, Suricata and other open source security tools.



Source: <https://www.itprc.com/wp-content/uploads/2018/06/security-onion.png>

Features:

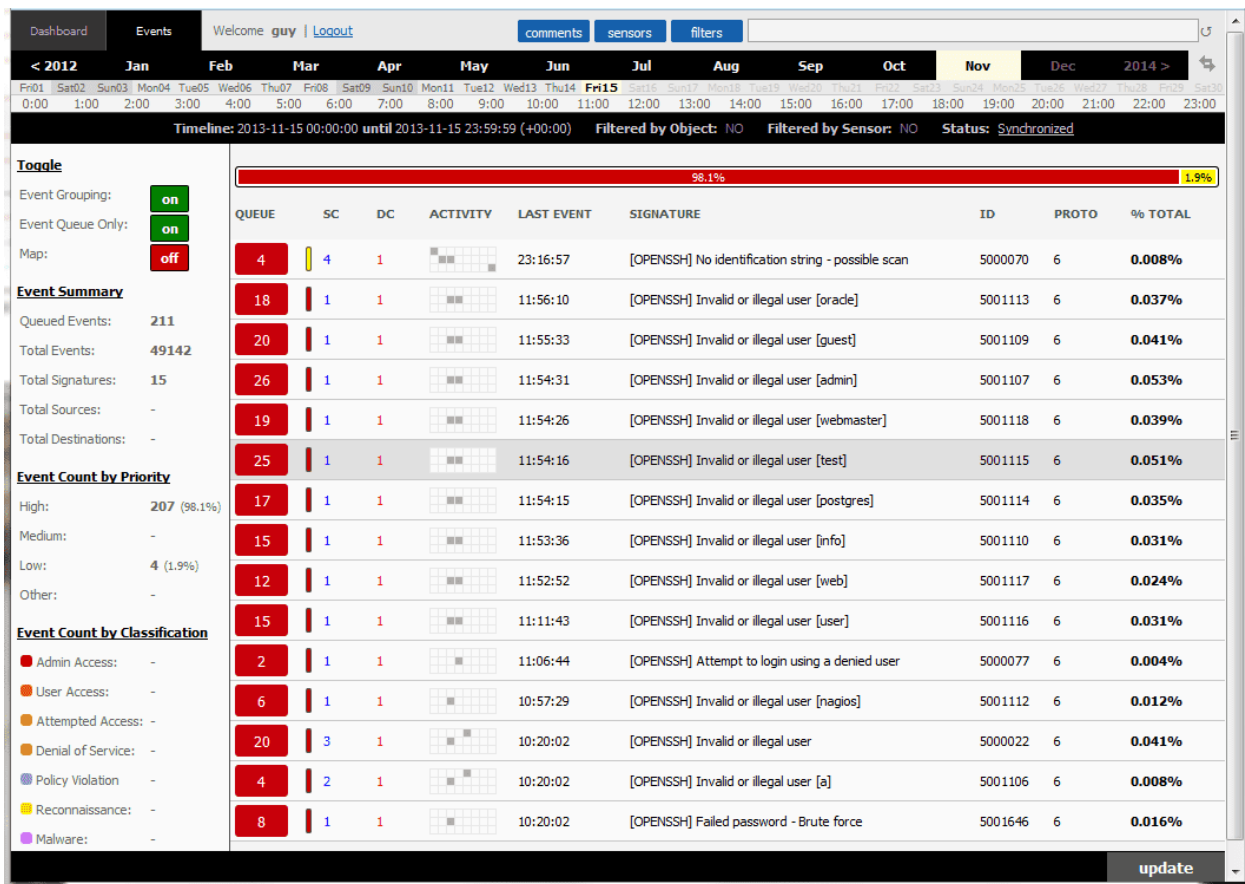
- Network Security Monitoring
- Log Management
- Open Source Linux Distribution
- Integrates with multiple tools.

Website: <https://securityonionsolutions.com/>

Pricing: It is open-source IDS that is available free to use.

Sagan

Sagan is an open-source free Intrusion Prevention System that mines log files for event data. It can be run on various platforms like Linux, Macintosh OS and UNIX.



Source: <https://securityonline.info/wp-content/uploads/2017/09/sagan.png>

Features:

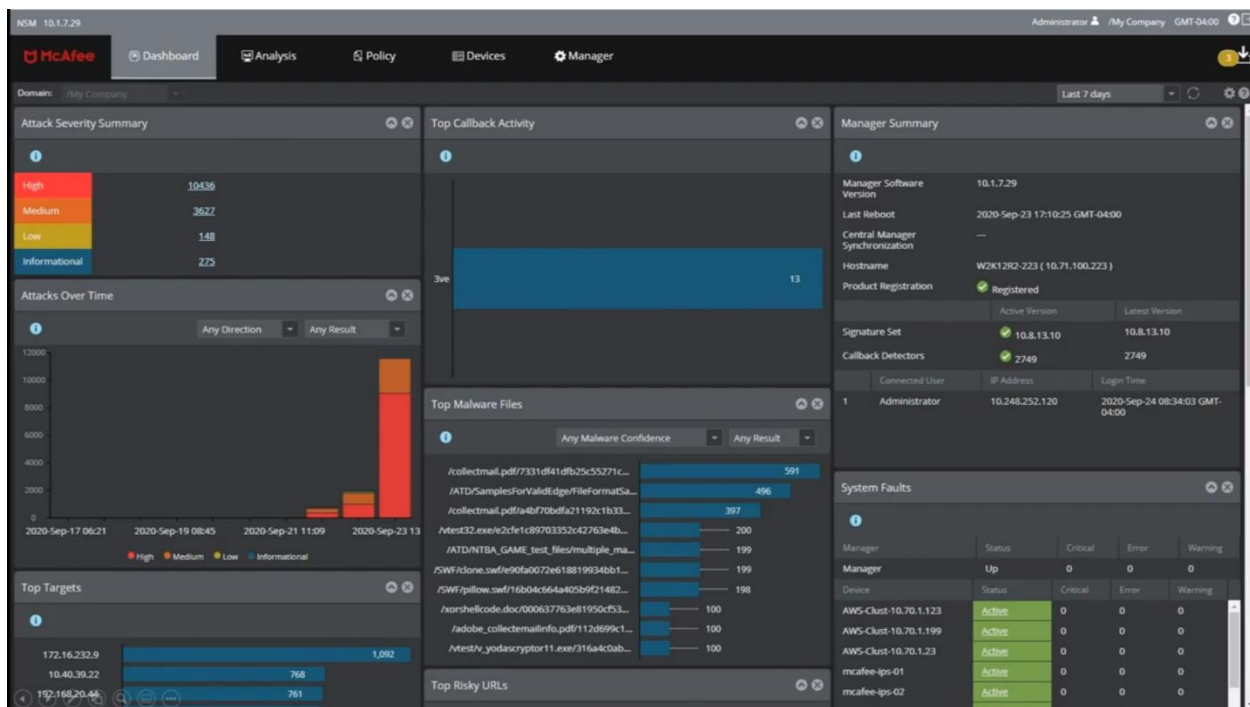
- Open Source
- It is lightweight
- Compatible with Snort data
- Integrated with multiple third-party tools.

Website: https://quadrantsec.com/sagan_log_analysis_engine/

Pricing: It is open source so it is free to use.

McAfee Network Security Platform

McAfee Network Security Platform is not an open-source network intrusion detection system. It comes with very high pricing as compared to others with focused development, support access and other benefits which are not available with other freeware open-source systems.



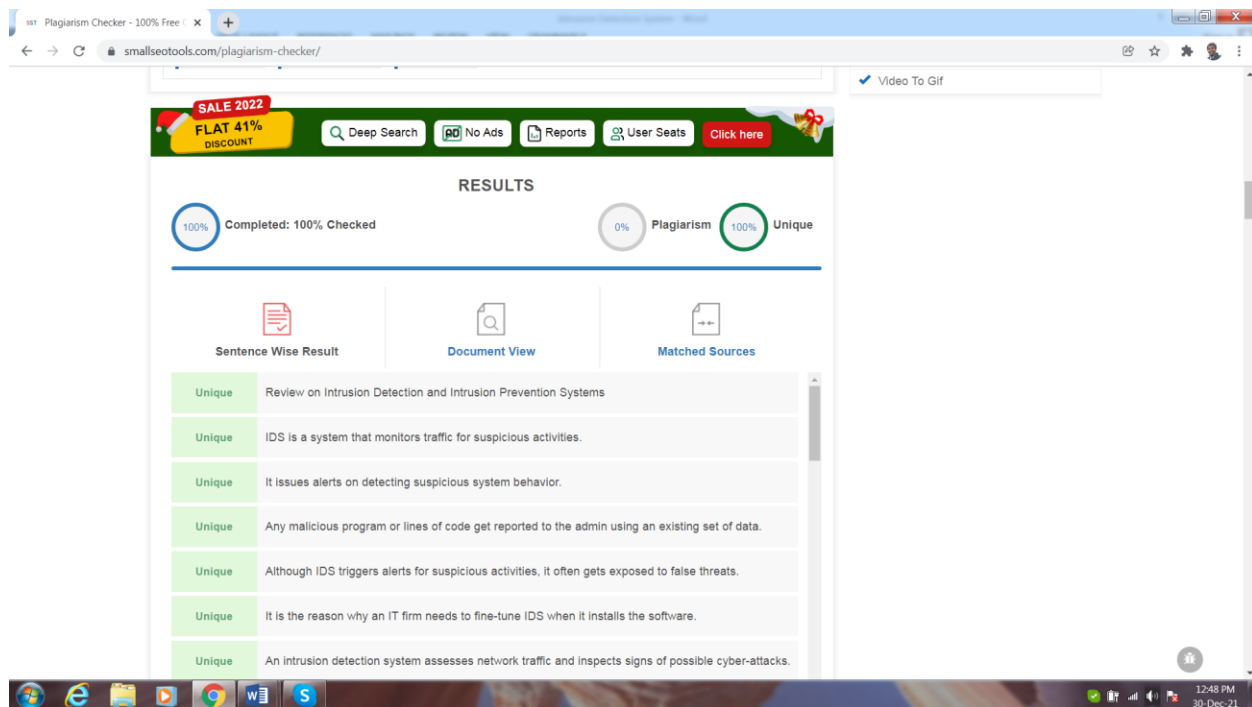
Source: <https://gdm-catalog-fmapi-prod.imgix.net/ProductScreenshot/163c4b91-7231-4e1c-a211-a44e78953941.png?ixlib=react-9.0.3&ch=Width%2CDPR&auto=format>

Features:

- Easy to use
- Network Traffic Inspection
- Network Analysis with extended Botnet Intrusion Detection.
- Advanced protection against threats.

Website: <https://www.mcafee.com/enterprise/en-us/products/network-security-platform.html>

Pricing: It is highly expensive that starts from \$10,995.



Factor	Author's Rating (1-5)	Publisher Rating (1-5)
1. Is this content better than the top 10 results for the given keyword?	4	
2. Does this content have a better format, point of view and outline than the top 10 results?	4.5	
3. Does this content have any data points to back up your statements?	4	
4. Does this content cover all the related queries and questions available in the search results?	5	
5. Did you avoid superfluous content and made your point straight, easily understandable and useful for the reader?	5	