A Comparison of Intrusion Detection Tools and why these are important for SMB's

Kim André Næss, Dale Peregrino Bada, Muhammad Javed Iqbal
Cyber Security
Noroff University College
Kristiansand, Oslo, Norway
kim.naess@stud.noroff.no, dale.bada@stud.noroff.no, muhammad.iqbal@stud.noroff.no

***Abstract*—This state-of-art review paper will examine the most popular Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) applicable for Small and Midsize Businesess (SMB).**

This review has 3 key objectives. Firstly, it will define and identify what kind of network security threats are most prevalent and most urgent for SMBs' to address. Secondly, this paper will identify what open source software are available for SMBs' to manage and mitigate identified threats. Then in the third final part, it will review how these open source software addresses the identified network threats.

Each tools' features, capabilities, advantages and limitations will be compared. How each system fare with regards to manageability, cost effectiveness and return of investment, will also be taken into consideration. With all above parameters being equal, should be able to determine which IDS/IPS are most suitable for SMBs'.

***Index Terms*—Intrusion Detection Tools (IDS), Small Business, Malware, Ransomware, Machine Learning**

I. Introduction

A. A brief background and history

IDS and IPS are a category of network tools or systems to detect and prevent malicious network activities. One of the earliest network based security defenses was firewall. Firewalls limited filter packets. Thus were IDS' introduced, which had the capability to inspect and validate individual packet and validate signatures of different indicators of compromise (IOC). Which are able to alert the administrators of positively identified malicious communication. Later, the integration of detection and prevention (IDS and IPS) in a single systems or devices like next-generation firewalls, further enhancing the security postures of organizations where these systems are deployed.

B. Evolving Threat Landscape and Countermeasures

IDS were initially installed on a host server, then specific network IDS devices gained even more popularity by providing IDS and IPS functionality in an integrated and more conveniently deployable and manageable unit.

C. Detection and Prevention for SMBs'

Notes - :
Think more about this part....

SMBs may also choose to omit certain features and functionalities SIEMs offer, and choose a solution based on open source software with comparable functionality. As such, the scope of this state-of-art review are open source IDS systems. Though occasionally, this paper will look at how an IDS relates to a larger tool chain, systems or technologies. This is inevitable as security relies on a layered approach, and reliance on a single tool, method or policy is bad practice. It is also relevant to assess an IDS as part of a companies infrastructure roadmap as the company scales up. SIEMs' are typically deployed in larger Enterprise IT environments. SIEMs takes center the stage in a companies Security Operations Center (SOC). These are often complex systems due to business process integration, or systems integration with IT Service Management tools like SolarWinds, ServiceNow og Jira, to name a few. All of the above drives cost of ownership up. Some may opt to subscribe to SOC as services to reduce cost.

D. Addressing SMBs' most prevalent network threat with IDS

Malware and ransomware, is identified in the Norsis [1] threat report for 2021 as a prevalent threat. Malware and Ransomware pose difficult challenge as they apply various techniques to obfuscate their existence on the host. With Polymorphic and Metamorphic code, malware are able hide while at rest on the host and when initiating communication on the network. And they can also piggy-back on trusted network sessions. Rendering the binary signatures used to identify them unusable using above mentioned techniques. On the other hand IDS and IPS main function is to detect, alert and prevent threats that are traversing the network. Therefore it is crucial that IDS and IPS are deployed together with other security tools and systems to be able to maximize its utilization. Larger network may also benefit from properly segmented and architecturally designed with security in mind. As always, a layered security approach must be applied.

II. Reviewing IDS Systems for Small and Midsized Businesses

A. Merits vs Operational Constraints of Intrusion Detection Systems

1) OSSEC: OSSEC is a host based intrusion detection system (HIDS) which is a free and open-source intrusion detection tool for monitoring system events, and filtering unwanted traffic. OSSEC capabilities is supported with the most used operating systems for businesses, which run on Linux, Windows or Mac OS. The system is free to use and this makes it ideal for small businesses, that might have a tight budget to finance their investments. The features that OSSEC home page [2] is claiming to have is Log based Intrusion Detecion(LIDs), Rootkit and Malware Detection, Active Response, Compliance Auditing, File Integrity Monitoring (FIM) and System Inventory.

2) Suricata: According to [3] Suricata is the second most popular IDS tools used, only bypassed by SNORT in popularity. Containing features like hardware acceleration and multithreading to perform spesific functions more effectivley.

Suricata has according to Techfunnel article [4] all of the mentioned capabilities of OSSEC and is claimed to be fast and could also detect advanced threats. This capabilities are also supported by a literature review paper on IDS [5] where the advantages of Suricata are mentioned along with additional benefits like filtered events and alarms, automatic protocol detection, application layer data collection to name a few. The downsides however are something that a small business should take into consideration as the CPU usage is high, and it has a smaller supported community compared to SNORT. The installation process is also mentioned as complex, and the need for special competence in this area for a small business may be needed.

3) Snort: As of 2022, there are 2 major versions of Snort installation base, namely Snort 2.X and Snort 3.X. There are 3 key, and perhaps the most noticeable, differences between Snort 2 and Snort 3. It has to do with performance optimization, detection rules and software distribution. With regards to performance, Snort 3 code base has been refactored and optimized and it also now support multi-threading. Enabling Snort 3 to perform packet analysis multi-threaded. Snort 3 has also improved Rules syntax and parsing using LUA programming language [6]. Since Snort3 was first introduced not too long ago, in 2021-01-19, the Snort 2.X installation base can be expected to have a long tail. Even though Snort 3.X introduced many meaningful improvements, Snort 2.X still do function and is still a supported product. Both by the its vendor, other service providers, the Open Source community and its users. For instance, the publicly available rules set are still being maintained and updated for both Snort 2.X and 3.X.

Network packets are processed by Snort in 5 stages. Stage 1 is the is called the ”Packet”, where the network packet is accepted by the system for processing. Stage 2 is the ”Decoder” which determines what protocol is used and performs protocol header analysis where is can identify malformed header. This stage prepares the packet for further inspection. Stage 3 is the ”Preprocessor” where the packet is normalized using Snort plug-ins. Plug-ins that allow Snort to process specific type of network traffic. Pre-processing entails eliminating anti IDS and IPS techniques and re-formats the packets for easier analysis where Snort rules can be applied. Stage 4 is where the ”Detection” is performed. This stage makes use of the rule sets available and applies it using a decision tree to determines if a packet is malicious. This stage has the ability to send an alert or prevent an intrusion by accepting or dropping the packet. Stage 5 is the ”Log and Verdict” stage that performs the traffic logging. The logs can be forwarded to a log processor like Splunk or compatible SIEM. The article ”Deep Packet Inspection for Intrusion Detection Systems: A Survey” by Tamer AbuHmed et al. thoroughly describes the intrusion detection process and expands in detail the algorithms used by the system [7].

Snort - Detecting Malware and Ransomware

It has to be stated that AI and Machine Learning within the problem domain of intrusion detection continuous to be regarded an experimental [8] endeavour at this point in time. In that there seem to be no established superior method, algorithm or process to automatically calibrate detection rules and algorithm to be used in IDS and IPS. However, studies has indeed proven that a Machine/Deep Learning is a viable solution. And that Machine and Deep Learning methodologies can indeed be used with Snort packet captures for analysis, albeit not in real-time. A real-time solution will require both high bandwidth network, high capacity storage and high compute capability. Snort, together with other Open Source Software can be utilized to automate the capture, detection and alert functionalities in near real time. A HIDS/HIPS solution can be implemented with Snort, OSSIM, a few Python Libraries and some custom scripts. A similar NIDS/NIPS is possible provided network, storage and compute requirements are met.

4) Zeek: According to [9] Zeek (previously known as Bro) is an intrusion detection system that differs from others in that it focuses on network analysis. Unlike rules-based engines, which are meant to identify exceptions, Zeek searches for dangers and generates warnings. Zeek is an open-source, passive network traffic analyser. Zeek is widely used by operators as a network security monitor (NSM) [10] to aid in the investigation of suspicious or malicious behaviour. Zeek also provides support for a broad variety of traffic analysis activities outside of the security area, such as performance assessment and troubleshooting. Extracting data from HTTP sessions, detecting malware by interacting with external registries, reporting vulnerable versions of software visible on the network, recognising popular online apps, detecting SSH brute-forcing, checking SSL certificate chains, and much more are all included into Zeek. V-A

Zeek - Malware detection using Zeek IDS

As we know that Zeek is an open source Intrusion detection system which is primarily used detection of malwares and suspicious activities over the network. Zeek also work as a network monitoring tool for analysis of traffic. Even though Zeek does offer common capabilities like signature-based intrusion detection systems (IDS), its scripting language allows for a far wider range of very varied techniques to uncovering harmful activities. Anomaly identification, semantic misuse detection, and behavioral analysis are all examples of this. Intrusion detection using Zeek goes beyond typical signature-matching, yet the system still includes a comparable signature engine that can be used in the same way as previous systems. In addition, Zeek employs a flexible signature language of its own.

Zeek - Architecture for detection of malware and malicious activities.

As it examines network traffic, it looks for anomalies. Zeke is a fully functioning IDS, but not a full-fledged IPS. Only UNIX-like platforms are supported by Zeek Figure: 1 depicts the structure of Zeek. In addition to libpcap and the Event Engine, it also includes the Policy Script Interpreter.

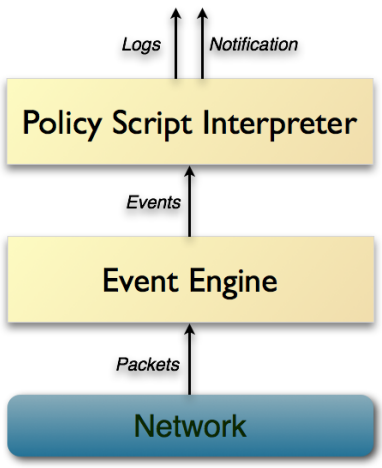

Fig. 1: Zeek Architecture [11]

Libpcap: Zeek captures network packets using the libpacap packet capture library. Insignificant network traffic [12] is put under stress by this.

Event Engine: Libpcap sends filtered traffic to the event engine. IP header checksum verification is one of the integrity checks performed by this layer to ensure that packets are properly generated. As a result, the network layer analyzer can access the complete IP packet. It communicates with the policy layer through events.

Policy Script Interpreter: Zeek policy scripts (rules) are written in a unique Zeek language that does not depend on standard signature detection. It examines the network to look for anomalies.

Zeek - A Powerfull Malware Detector

Because of Zeek's ability to identify deception attacks as well as attacks concealed by normal TCP segmentation, Zeek-ids can do application-level deep packet inspection, Zeek can discover and analyze tunnels, and Time Machine, a high-performance packet bulk recorder with a Zeek interface, may boost forensic capabilities. By using Zeek IDS we can easily detect different types of malware of different categories because of its anomaly based interpreter which reads the behavior of packet and analyze it. Based on the architecture of Zeek IDS yes it is capable of detecting ransomware attacks [13].

Zeek is a powerful tool for detection of malware and malicious activities because of its anomaly based detection features [14]. Features of Zeek makes it valuable and perfect for detecting anomalies and malware . Features of Zeek which makes it detect malwares at high efficiency are:

- It gathers, analyses and correlates log data.
- Searches for system alterations like those made by rootk-its.
- Automated response actions may be initiated by an active reaction.
- Alerts that may be customised and sent in real time

As discussed, zeek is a very powerful tool for detection of malwares but zeek some of the drawbacks of zeek is that it does not provide any GUI support and is difficult to deploy so its deployment in small businesses without an dedicated IT team is difficult.

III. Ethical Issues

Privacy, Anonymisation, Data Confidentiality, Reputation & GDPR EU perspective

A considerable complication concerning the utilization of IDS tools due to laws in some countries surrounding privacy. This due to the GDPR laws which companies regardless of their size could be fined a substantial amount for not being compliant with. That could lead to a significant financial blow or in worst case bankruptcy for some companies. One of the latest cases from Spain showing that Google got fined 10 million Euro, for violation of the GDPR rules. [15] If this fine was given a smaller company than Google, for the same violation, this could hurt the company tremendously. Although a smaller company possibly surviving the financial blow, the reputational damage could lead to more financial loss.

Regardless of IDS systems aid to improve the security by detecting vulnerabilities and attacks to prevent compromising systems, not all the information are supposed to be seen or supervised by everyone on the same system or network. One solution for this issue could be Encryption, but as a survey from Khraisat, Gondal, Vamplew and Kamruzzaman state that the encrypted traffic makes it difficult to detect attacks. [16] This makes it complicated due to the GDPR rules, because if the normal traffic on a system is not encrypted, this is available in plain text for anyone not only on the system but to intruders as well. To restrict all parties within a company having access to view the traffic from IDS, a user role and permissions could be something to look into further for this matter.

From a small business owner, or an service provider point-of-view, are there any ethical issues or ramifications that must be considered when deploying Intrusion Detection Systems? The short answer is; Yes there are some ethical considerations that must be addressed when deploying IDS. This question can be approached as formal technicality or in a more philosophical manner.

From a philosophical perspective, we can regard ethics as a framework. A tool to help us navigate and resolve conflicting ideas and value judgement. From where Kantianism, Utilitarianism and Contrarianism lend their specific views on ethics, which has helped form and define how our modern society is governed and policed [17].

Ethics, although primarily a subjective set of beliefs used. It does manifests as individual values our policy makers adheres to. Whom then forms a common cultural set of values and beliefs in their individual arenas and communities. Which then translates to the cultural norms influencing and defining our politics, rules and regulations. And by that our daily lives and businesses.

Thus, one can say that ethics are already built into the common set of laws and regulations business, and individuals alike, are protected by and must adhere to. This is how ethics are formalized and applied in the ”real world”. Directly influencing the business domain. And in the case of CyberSecurity, where IDS and monitoring logs captures user information, GDPR compliance provisions ethical concerns to be addressed [18].

GDPR in Practice From Norwegian SMB Perspective

How GDPR affects local business can be quite complicated. Where the business is located determines how GPDR affects a business and what GDPR compliance are required. GDPR is a regulation for EU member states and its citizens. Therefore, any business that caters towards EU citizens must comply. While businesses that processes or store personal identifiable informaton [19] (PII) can technically be required to comply [20].

A business residing in Norway however must comply with national regulations concerning personal data as mandated by the Norwegian Data Protection Authority (DataTilsynet). Although Norways has its own national regulations for personal data, it does comply with the GDPR regulations is a great degree and can be regarded as proxy implementation of GDPR.Datatilsynet may also require a dedicated ”Data Proctection Officer” depending on the nature of the business [21].

In practice, a SMB in Norway that implements IDS which collects and stores PII, must comply with Datatilsynets regulations. At the minimum, the initial ”Data Protection Impact Assessment” must be conducted. Furthermore, there some regulations and compliance which are sector specific, ekomforskriften for electronic communications services [22] and finansforetaksloven [23] for financial institutions. Also important to mention is the special regulation [24] for businesses that provides services to certain public institutions or institutions with national import.

From a business and a service provider point of view, the there are are few tenets which must be complied: Each individual users must able to request for their PII to be purged...

IV. Summary

1) Reliable and Well Supported And Well Supported: Along with technical specs, features and functionalities, the product and vendor reliability and confidence define the key factors that are assessed and evaluated prior to implementation and deployment. Specially for a crucial component that goes into a security system. Having Cisco Systems, a large Fortune500 company, and a leading network security vendor, provides Snort the trust and confidence in troves. For example, the backbone of Snort is its Rules which enables Snort to detect malicious network sessions. The basic Snort installation provides a basic set of rules. This rules are publicly available for free as provided and maintained by the researchers from Cisco Talos Intelligence Group, whom are the official content creators for Snort. Cisco Systems, together with a large and engaged Open Source community, provides a freely available vailable version of the product for non-enterprise or SMB users.

Snort's 3 main features or mode of operation, as ofted cited in many Snort tutorial blog post entries, how-to videos on YouTube and Wikipedia are; Packet Sniffer, Packet Logger and Network Intrusion Detection System mode [25]. However, Cisco Systems themselves often refer to Snort as an Intrusion Prevention System in their documentation [26] and Cisco Talos Intelligence Group's YouTube video [27]. As a packet sniffer, it is capable to capture, interpret and process packets akin to Wireshark and tcpdump. As a packet logger Snort can capture network packets (without analyzing) and store them for further analysis.As an Intrusion Detector, Snort has the ability to log events, trigger alerts and other systems it can integrate with like SIEMs. As an Intrusion Prevention System, it can drop packets from the network or trigger other systems that are able to execute preventive measures.

2) IDS/IPS - Installation: Lets establish a scenario where we want to address the issue of general intrusion and more specifically malware and ransomware. In this scenario we want to alert malicious network intrusion. At the same time detect malware prevent file extraction from a specific on-site file server.

One simple way to achieve this objective is to implement Snort as an inline NIDS/NIPS inside the SMB network, right behind a firewall. A dedicated AT&T OSSIM server as SIEM alert and monitoring dashboard. And a dedicated server to run malware analysis on automated with Python scripts and libraries.

The Snort NIDS/NIPS can be configured to perform packet logging regularly with specific interval. This is necessary to capture data that can be used for malware analysis. A static analysis, automated with Python scripts utilizing OpenSource libraries for Machine and Deep Learning, read Windows Portable Executables (PE) etc.

There are different methods to apply Machine Learning to perform malware analysis as described in Alessandro Parisi's "Hands-On Artificial Intelligence for CyberSecurity" [8] while A YouTube video by Motasem Hamdan describes basic installation of Snort [28]

V. Conclusion

Security best-practice rely on a holistic and layered approach...

Follow-up - !!!

The following items are statements from the abstract that we must address:

- Review how these open source software addresses the identified network threats
- IDS features, capabilities, advantages and limitations will be compared.
- How each system fare with regards to manageability, cost effectiveness and return of investment
- Determine which IDS/IPS are most suitable for SMBs

Follow-up - to-do!!!

- Provide evidence for security best-practices to further elaborate and support the statement.
- Provide concrete examples where IDS and IPS are ineffective against malware and ransomware.

With all the limitations inherent to IDS and IPS taken into consideration. The most effective, cost effective and manageable systems is...

Follow-up - to-do!!!

- Insert name of IDS/IPS here when all the review has been conducted.

The IDS an IPS systems must also be protected along with the logs and packet capture data they store.

APPENDIX A:

REFERENCES

[1] Norsis, "Norsis trusler trender 2021 digital," 2021. [Online]. Available: https://norsis.no//wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf

[2] C. Robertson, "Practical ossec," 7 2011. [Online]. Available: https://sansorg.egnyte.com/dl/xuh7dAtqWw

[3] L. Reznik, Intelligent security systems. Standards Information Network, Sep. 2021.

[4] M. Chrisos, "Top best intrusion detection systems for business," 2022. [Online]. Available: https://www.techfunnel.com/information-technology/top-best-intrusion-detection-systems-for-business

[5] M. Ozkan-Okay, R. Samet, Ö. Aslan, and D. Gupta, "A comprehensive systematic literature review on intrusion detection systems," IEEE Access, 2021.

[6] J. Munshaw, "Snort blog: The major differences that set snort 3 apart from snort 2," 8 2020. [Online]. Available: https://blog.snort.org/2020/08/snort-3-2-differences.html

[7] T. Abuhmed, D. Mohaisen, and D. Nyang, "A survey on deep packet inspection for intrusion detection systems," 03 2008.

[8] A. Parisi, Hands-on artificial intelligence for cybersecurity : implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt, 2019. [Online]. Available: https://ereader.perlego.com/1/book/1031674/3

[9] J. Strand, "Detecting malware beacons with zeek and rita - black hills information security," 2022. [Online]. Available: https://www.blackhillsinfosec.com/detecting-malware-beacons-with-zeek-and-rita/

[10] A. Ferriyan, A. H. Thamrin, K. Takeda, and J. Murai, "Encrypted malicious traffic detection based on word2vec," Electronics, vol. 11, no. 5, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/5/679

[11] "Zeek offical landing page," 2019. [Online]. Available: https://docs.zeek.org/en/v3.0.14/_images/architecture.png

[12] T. J. Shimeall and J. M. Spring, Chapter 12 - Recognition Strategies: Intrusion Detection and Prevention, T. J. Shimeall and J. M. Spring, Eds. Boston: Syngress, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9781597499699000122

[13] D. A. Bhosale and V. M. Mane, "Comparative study and analysis of network intrusion detection tools," in 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). IEEE, Oct. 2015. [Online]. Available: https://doi.org/10.1109/icatcct.2015.7456901

[14] S. Haas, R. Sommer, and M. Fischer, "Zeek-osquery: Host-network correlation for advanced monitoring and intrusion detection," ICT Systems Security and Privacy Protection, vol. 580, pp. 248 – 262, 2020.

[15] "Gdpr enforcement tracker - list of gdpr fines," Available at https://www.enforcementtracker.com/ETid-1176 (2022/20/05).

[16] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, vol. 2, no. 1, Jul. 2019. [Online]. Available: https://doi.org/10.1186/s42400-019-0038-7

[17] S. D. Courtland, "Hobbesian applied ethics and public policy."

[18] L. Haberkorn, "The ethics of gdpr - science editor," 2019. [Online]. Available: https://www.csescienceeditor.org/article/the-ethics-of-gdpr/

[19] E. Commission, "What is personal data? — european commission." [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

[20] B. Wolford, "Does the gdpr apply to companies outside of the eu? - gdpr.eu." [Online]. Available: https://gdpr.eu/companies-outside-of-europe/

[21] Datatilsynet, "Hvem må ha personvernombud? — datatilsynet," 2019. [Online]. Available: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvem-ma-ha-personvernombud/

[22] Lovdata, "Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) - lovdata," 2021. [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2004-02-16-401

[23] ——, "Lov om finansforetak og finanskonsern (finansforetaksloven) - lovdata," 2016. [Online]. Available: https://lovdata.no/dokument/NL/lov/2015-04-10-17?q=finans%20forskrift%20IT

[24] ——, "Lov om nasjonal sikkerhet (sikkerhetsloven) - lovdata," 2018. [Online]. Available: https://lovdata.no/dokument/NL/lov/2018-06-01-24?q=sikkerhetsloven

[25] Wikipedia, "Snort (software) - wikipedia," 4 2022. [Online]. Available: https://en.wikipedia.org/wiki/Snort_(software)

[26] Cisco, "Firepower management center snort 3 configuration guide, version 7.0 - getting started with snort 3 intrusion policies [cisco firepower management center] - cisco." [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/70/snort3/config-guide/snort3-configuration-guide-v70/getting-started-intrusion.html

[27] C. T. I. Group, "(1207) snort 101 - youtube," 2 2020. [Online]. Available: https://www.youtube.com/watch?v=W1pb9DFCXLw

[28] M. Hamdan, "(1216) snort ids / ips complete practical guide — tryhackme - youtube," 3 2022. [Online]. Available: https://www.youtube.com/watch?v=pvPdOO2VcwM&t=870s

APPENDIX B:

A. Zeek Pros and Cons

Pros:

- Zeek is a traffic analysis tool that is completely flexible and expandable. To express any analytic job, Zeek offers a domain-specific, Turing-complete scripting language.
- A low-cost alternative to pricey proprietary technologies, Zeek operates on commodity hardware. Zeek is a network monitoring tool that goes well beyond the capabilities of most other tools, which are often confined to a narrow collection of pre-programmed analytic activities.
- As a platform for gathering and analysing network data, Zeek is best suited to the task at hand.
- The transaction data provided by Zeek is the company's biggest selling point. This means that if a network interface is being monitored, Zeek will create a collection of high-fidelity, highly annotated transaction logs by default. In a judgment-free, policy-neutral way, these logs explain the protocols and activities on the network.

Cons:

- ZeeK/Bro's deep packet inspection consumes a lot of resources, which is a drawback if you're looking for flexibility. In terms of threat intelligence, Snort and Suricata are the two most popular options. The community is continuously attempting to make Bro more user-friendly because of this.