On the Perception of Risk Assessment in Intrusion Detection Systems

Mario Golling[1], Robert Koch[1] and Gabi Dreo Rodosek[1]

Abstract: Especially in the area of Intrusion Detection, the concept as well as the understanding of the term "risk" is of fundamental importance. Generally, risk assessment represents an important means of evaluating certain situations, plans, events or systems in a systematic and comprehensive procedure. As in other areas, within the field of IT security, the systematic assessment process (risk analysis) also aims at recommending how to allocate available resources. Referring to this, both, the categorization of traffic (whether traffic has to be classified as an attack or not - “benign vs. malicious”) as well as a corresponding estimation of the expected damage (severity) are of central importance. Therefore, within this publication, the authors address the following questions in detail: (1) To what extent are the detection results of different IDSs comparable - with regard to the assessment of the risk / extent of damage - or are there strong deviations? (2) How do both vendor-dependent and vendor-independent alerts address the topic of risk assessment and enable the implementation of a comprehensive risk concept? To this end, at the heart of this paper, an overview as well as an evaluation of important representatives of open source IDSs is presented, focusing on methods for risk assessment resp. risk rating including cross-vendor risk rating and the Common Vulnerability Scoring System (CVSS). Furthermore, the paper also contains a brief demise of the most important representatives of commercial IDSs.

Keywords: Network Security, Intrusion Detection, Risk Rating, Risk Assessment, Risk Severity

1 Introduction

Generally, risk assessment represents an important means of evaluating certain situations, plans, events or systems in a systematic and comprehensive procedure. As in other areas, within the field of IT security, the systematic assessment process of risk analysis also aims at recommending how to allocate available resources to perform in-depth analyzes or to develop appropriate counter-measures in order to minimize total exposure. With regard to Intrusion Detection Systems (IDSs)/Intrusion Prevention Systems (IPSs) risk assessment is particularly important as it represents an important means of evaluating the current situation wrt. IT security and to focus on important alerts rather than to treat all alerts in the same way (especially if the resources are insufficient to investigate all alerts in depth). Following these considerations, the various methods of important representatives of IDSs are presented and differentiated from each other within this paper. To this end, this paper is structured as follows: Section 2 contains an overview of important representatives of open source IDSs as well as vendor-independent approaches. Section 3 then briefly deals with commercial IDSs in the same way, before the paper is concluded in Section 4.

[1] Munich Network Management Team (MNM-Team), Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, D-85577 Neubiberg, {mario.golling, robert.koch, gabi.dreo}@unibw.de

2 Risk Rating in Popular Open Source IDSs

Selection Criteria

In the field of open source IDSs, a wide variety of systems and procedures are present. Unlike commercial systems, that are subject to various market analysis, an overview of important representatives of open source IDSs is, for the lack of generally accepted data, far more difficult. Nevertheless, due to the page limitations of this paper, we are obliged to reduce the range of systems, especially in terms of their number. Table 1 briefly illustrates the reasons/motivations for the systems selection.

Tab. 1: Popularity of Open Source IDSs

SOURCE	SNORT	SURICATA	BRO	PRELUDE
Debian Popularity Contest (higher numbers represent greater popularity)	914	83	not included	25
Alienvault Blog: Open Source Intrusion Detection Tools: A Quick Overview *This investigation only covers Snort, Suricata and Bro*	*"The de-facto standard for IDS"*	*"What's the only reason for not running Snort? If you're using Suricata instead"*	*"Starting to gain a larger community following"*	not mentioned
Pathan: The State of the Art in Intrusion Prevention and Detection *Only those 4 open source NIDS are listed*	*"Snort is considered as the de facto standard of the IDS/IPS with millions of downloads and is the most extensively deployed IDS worldwide"*	*"The high-performance Suricata IDS [. . .] has been advanced as an open-source improvement for the popular Snort"*	*"widely used as an intrusion detection system" "distinguishes itself from Snort by offering high-speed network capability"*	*"Prelude is a security information management system [... and] can collect alert data from other security applications or generate its own alert data"*
Intrusion Detection Case Study *Only those 4 open source NIDS are listed*	included	included	included	included
Comparison of Open Source Network Intrusion Detection Systems *Investigation was limited to Snort, Bro, Suricata*	included	included	included	not included
Evaluation studies of three intrusion detection systems under various attacks and rule sets	*"The open source IDS commonly used are Snort, Suricata, and Bro"*			not included

For the sake of clarity, within this Section, we divided the systems into single-IDSs (Snort, Suricata and Bro) and cross-manufacturer approaches (Prelude and Common Vulnerability Scoring System (CVSS). As it will be shown later, CVSS is not a system per se. Instead, it is a cross-systems/cross-vendor approach, which, due to its importance, has to be covered in this paper, too.

Individual Open Source IDSs

Snort

Snort is an open source NIDS originally written by Martin Roesch. Although the first version was focussing on signature-based detection only, the current version of Snort also includes other detection techniques (protocol-based as well as anomaly-based Intrusion Detection).

Snort is generally considered as the de facto standard for Intrusion Detection [Pa14]. Snort is a packet sniffer and logger that features rule-based logging to perform content pattern matching and is capable of detecting a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts etc. Snort has real-time alerting capabilities and a detection engine, which is programmed using a simple language that describes per packet tests and actions. See Figure 1 for an impression of a Snort rule. By default, alert messages of Snort typically include a priority level with a

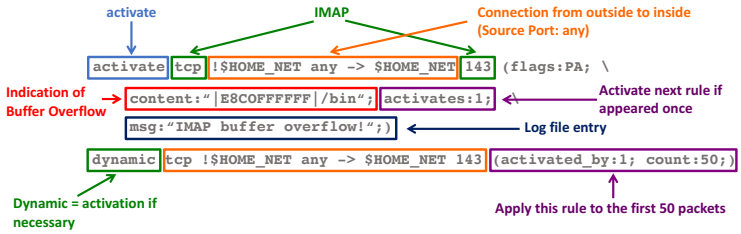


Fig. 1: Example of a Snort Rule (with minimum explanation)

gradation in four categories (high, medium, low, very low). For this, an integer value called *Priority* is used. A value of 1 (high) is the most severe and 4 (very low) is the least severe. Listing 1 shows an example of a Snort alert (with a priority of 2).

List. 1: Example of a Snort alert

```
[**] [1:497:11] ATTACK-RESPONSES file copied ok [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
03/09-20:34:00.379435 205.206.231.13:80 -> xxx:61607
TCP TTL:43 TOS:0x0 ID:54613 IpLen:20 DgmLen:1492 DF
***A**** Seq: 0xD8357B2D Ack: 0x49F73C5E Win: 0x2220 TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0884][Xref => http://www.
    securityfocus.com/bid/1806]
```

In principle, the priority of Snort allows to use numbers greater than 4 as well. Snort itself describes the priority by means of an integer value, hence also allowing values greater than 4. For this, the default priorities assigned by Snort can be overwritten locally by the user. This can, for example, be useful to adapt Snort to the local environment. As Snort, for instance, by default assigns a priority of 3 to Telnet activities, using a higher priority level may be wise, if telnet connections are not a rarity in the investigated network [OBB05]. However, it can be assumed that only a few users are making use of this. With the help of attack taxonomies such as Common Vulnerabilities and Exposures (CVE), an even more detailed prioritization can be made, e.g., by using the CVSS. This is described in more detail at the end of this Section.

Suricata

In contrast to Snort, which is per default limited to use rule sets written in a specific format, Suricata is capable of using additional formats, too. Suricata uses multithreading, which makes it faster than other IDSs. With regard to risk rating, Suricata provides a range of values from 1-255, which is almost exclusively reduced to the values 1-4 in practice. This

is mainly due to the fact, that - while Suricata is able to use rules from different sources (to provide the best rule set possible) - the Suricata developers intended to support the same rule language used in the Snort rules [Al11], which, in practice, is often the case. Listing 2 illustrates some examples of Suricata alerts.

List. 2: Examples of Suricata alerts [Se13]

```
03/10/2011-13:58:00.924783 [**] [1:2009702:4] ET POLICY DNS Update From External net
    [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {UDP}
    192.168.100.37:53 -> 192.168.100.35:53
03/10/2011-13:58:30.921484 [**] [1:410:5] ICMP Fragment Reassembly Time Exceeded [**]
    [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.100.35:11 ->
    192.168.100.37:1
03/10/2011-13:58:47.715668 [**] [1:2009702:4] ET POLICY DNS Update From External net
    [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {UDP}
    192.168.100.37:53 -> 192.168.100.35:53
```

Bro

From its origin, Bro is a traffic analyzer, which can also be used as an IDS. Bro has gained its reputation mainly due to its stateful protocol capabilities [Pa14]. Bro detects intrusions by first parsing network traffic to extract its application-level semantics and then executing event-oriented analyzers that compare the activity with patterns deemed troublesome. The detection includes specific attacks: Those defined by signatures (*knowledge-based detection*), but also those defined in terms of events and unusual activities (*behavior-based*); e.g., certain hosts connecting to certain services, or patterns of failed connection attempts. The important feature of Bro that differentiates it from other IDSs, such as Snort (at least from the initial version of Snort), is that Bro scripts can be written to understand application semantics and could be trained to look for anomalies (*behavior*) [Ba06]. As actions to alerts, Bro supports a whole series of options, such as logging, email notification, dropping the traffic or adding geo data to the message. For the actual risk assessment, however, there are no mechanisms (neither a proprietary model nor a manufacturer-independent method such as CVE/CVSS).

Cross-Vendor Approaches

Prelude/Intrusion Detection Message Exchange Format (IDMEF)

The Prelude Intrusion Detection System differs from the approaches described so far as it is a Security Information Event Management (SIEM) system. Prelude collects, normalizes, sorts, aggregates, correlates, and reports all security-related events independently of the product brand or license [CS14]. Prelude can either make use of different types of sensors (other security applications, such as Snort) or use own components for evaluation. Similar to Snort and Bro, an open source version with limited performance (called Prelude OSS) as well as a commercial version (Prelude Pro) is available. Sensors feed their data to the Prelude Manager with the use of the Intrusion Detection Message Exchange Format (IDMEF). As the “Lingua Franca” for Security Incident Management [Co03], IDMEF and its associated protocols enable a common language used to discuss Intrusion Detection events as a basis for cross-product event correlation. For that purpose, the manager collects and normalizes IDMEF data and makes it available to output plugins. Essentially, normalization allows all collected events to be stored in the same database in the same format [Ya09]. With regard

to risk rating, IDMEF in turn uses 4 Severity Levels (info, low, medium, high). However, IDMEF may also include a reference to a vulnerability database (such as the Open Source Vulnerability Database), and thus, ultimately, to the Common Vulnerability Scoring System (CVSS). For a summary and an overview of the mutual interdependencies, see also Figure 2.

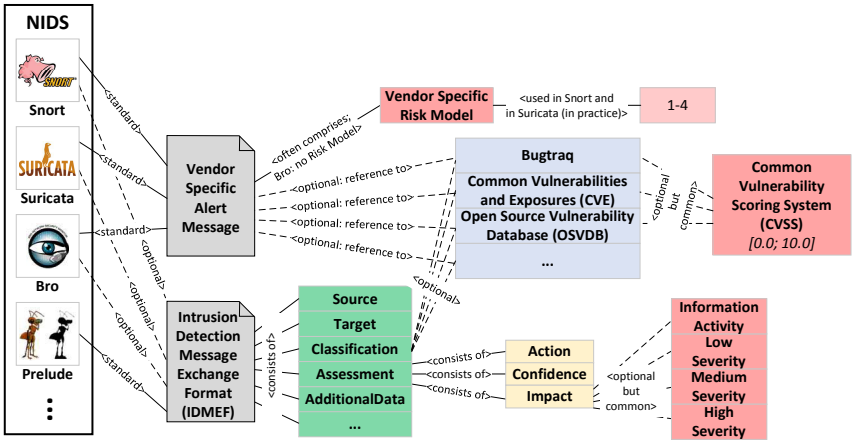


Fig. 2: Relationship between Bro, IDMEF and CVSS, in particular with regard to Risk Assessment

Common Vulnerability Scoring System (CVSS)

CVSS was commissioned by the National Infrastructure Advisory Council (NIAC), a working group of the U.S. Department of Homeland Security, in 2005 and is currently managed by the Forum of Incident Response and Security Teams. In the development of CVSS among others, the following entities have been involved: CERT, Cisco, DHS / MITRE, eBay, IBM, Microsoft, Qualys, or Symantec. As depicted in Figure 3, CVSS consists of different groups: Base, Temporal and Environmental, each comprising a numeric score ranging from 0 to 10, with 10 being the most severe.

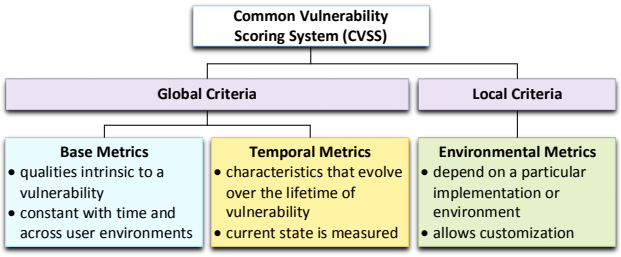


Fig. 3: Main areas of CVSS

The Base group represents the intrinsic qualities of a vulnerability [MSR17]. The Temporal group reflects the characteristics of a vulnerability and may change over time. Generally, base as well as temporal metrics are specified by vulnerability bulletin analysts, security product vendors, or application vendors [MSR17] and therefore can be considered as *global criteria*. In contrast to this, the Environmental group represents the characteristics of a vulnerability with regard to the user's environment (*local criteria*). Each group consists of

multiple separate categories. Base Metrics consists of: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality Impact, Integrity Impact and Availability Impact. Temporal Metrics consists of Exploitability, Remediation Level and Report Confidence. Environmental Metrics consists of Security Requirements (to customize depending on the importance of the affected IT asset, measured in terms of confidentiality, integrity, and availability) and Modified Base Metrics (enable to adjust the Base metrics).

Overview of Risk Rating Models of Open Source IDSs and Cross-Vendor Approaches
For the sake of clarity, the four considered IDSs are listed and distinguished within Table 2.

Tab. 2: Overview of Open Source Risk Rating Models

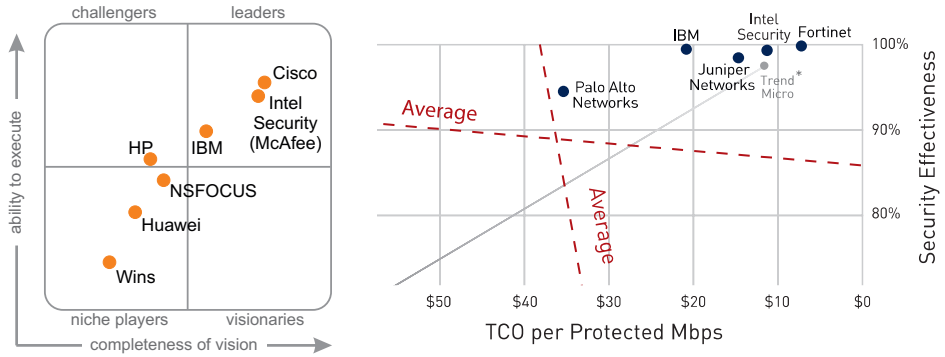
SNORT	SURICATA	BRO	PRELUDE/ IDMEF	CVSS
by default, simple model with 4 classifications: • high (1), • medium (2), • low (3), • very low (4)	simple model: • theoretical classification area: 1-255 (1 = high, 255 = low) • in practice: 1-4 (see Snort)	Bro itself offers no mechanisms for risk rating (neither a proprietary model nor a manufacturer-independent method such as CVSS)	simple model with 4 classifications: • info (0), • low (1), • medium (2), • high (3)	complex model consisting of 3 main classes of severity: • Base Metrics • Temporal Metrics • Environmental Metrics Overall scoring has an interval from 0 to 10.

3 Risk Rating in Commercial IDSs

Similar to Section 2, this Section presents commercial IDSs, whereby often much less information is available on how these systems evaluate alerts (in terms of motivation etc.). There are also no generally accepted cross-manufacturer approaches.

Selection Criteria
With regard to the risk rating of commercial IDSs, a restriction has been made to those systems that have been evaluated in the current study of Gartner called "Magic Quadrant for Intrusion Prevention Systems" as particularly outstanding (leaders and challengers; see [HYD13]). Figure 4a depicts the latest version. Other studies such as the well-known NSS-study (see [NS16] and Figure 4b) have not been taken into account. For the latter, “irregularities”, such as the very high detection rates (> 99%) were the reasons. In general, the fact that (i) the Gartner study has also acquired considerable importance outside the “pure scientific area” and (ii) the Gartner study is also free to obtain (in some parts) - which is often not the case with many other analyses (these costs quickly 5,000 USD or more) - were the driving factor.

Individual Commercial IDSs
Cisco
In contrast to simple models (like the one of Suricata/Snort, in which, by default, only



(a) Magic Quadrant for IDSs

(b) NSS Labs' 2016 Security Value Map for Data Center Intrusion Prevention System

Fig. 4: Overview of important Commercial IDSs

four values are used), Cisco uses a slightly more complex risk rating model, realized as an integer value in the range from 1 to 100 [Ci09]. Here, the greater the security risk, the higher the value [Ci09]. Three subcomponents are used within the overall risk rating formula:
Signature Fidelity Rating is a variable, which in turn can contain values from 1 to 100, measuring the accuracy of the signature. The Signature Fidelity Rating is assigned by Cisco, but can be modified by the user depending on the environment, such as the OS, service, application, or patch level. With regard to applications, it may also occur that a legitimate application produces traffic that mimics the behavior of an exploitation of a network vulnerability.
Alert Severity Rating describes the damage if the attack succeeds. Its value is again predefined with four degrees: *Information* (25, generally poses no immediate threat), *Low (50, somewhat unusual on most networks)*, *Medium (75, should generally not be seen on the network)* and *High (100, indicative of an active attack or an obvious precursor to an attack)*.
Target Value Rating is used to modify the risk rating based on the target of the attack and is therefore user-defined. This allows the user to increase the risk of an event associated with a critical system and to deemphasize the risk of an event on a low-value target [Ci09]. A *Low Asset Value* corresponds to a score of 75, a *Medium Asset Value* to 100, a *High Asset Value* to 150 and a *Mission Critical Asset Value* is assigned a scoring of 200.
The corresponding overall risk rating formula is as follows:

$$\textit{Risk Rating} = \frac{\text{Signature Fidelity Rating} * \text{Alert Severity Rating} * \text{Target Value Rating}}{100 * 100 * 100} \tag{1}$$

with the final results that exceed 100 being rounded down to 100 [Ba11].

Intel Security/McAfee
The Network Security Platform of McAfee assigns a default severity to every attack using a numbering score from 0 to 9, based on the immediate effect, or impact, on the target

system [Mc15]. The guidelines in assigning severity levels are very similar to those used in many open security forums [Mc15]. Table 3a describes the numbering scheme as well as the mapping to indicate Informational, Low, Medium, and High. Table 3b illustrates McAfee's attack categories and corresponding severity ranges.

Tab. 3: McAfee's risk assessment perception

(a) Alert numbering scheme of McAfee's Network Security Platform [Mc15]

INFORMATIONAL	LOW	MEDIUM	HIGH
0	1-3	4-6	7-9

(b) Excerpt from McAfee's attack categories and corresponding severity ranges [Mc15]

CATEGORY	THREAT TYPE	RANGE USED IN NETWORK SECURITY PLATFORM
Reconnaissance	Host sweep	4-4
	Port scan	4-4
	OS Fingerprinting	6-6
Exploits	Buffer Overflow	7-9
	Bot	7-9
	DoS	3-5
	DDoS Agent Activity	7-9
	Worm	6-9
Policy Violation	Unauthorized IP	5-5
	Covert Channel	5-5
	Command Shell	4-4

IBM
At IBM, the individual security events also receive a severity level; here, in the categories of High, Medium and Low [IB17]. Integrated into the IBM Network IPS is also a Snort system. The severity of these rules is also specified in terms of the categories High, Medium and Low. The corresponding Network IPS appliance provides alerts with the use of the categories Low, Medium and High as well.

Trend Micro
Trend Micro's TippingPoint has a classification mechanism, which for instance serves as a basis for the ability to color code the security reports. Table 4 illustrates the different severity levels.

Tab. 4: Severity Levels of TippingPoint

SEVERITY LEVEL	DESCRIPTION	COLOR USED FOR THE REPORTS
Critical	attacks that must be looked at immediately	Red
Major	attacks that must be looked as soon as possible	Yellow
Minor	attacks that should be looked at as time permits	Cyan
Low	traffic that is probably normal, but may have security implications	Gray

Overview of Risk Rating Models of Commercial IDSs
Table 5 summarizes the various commercial risk rating models.

4 Conclusions and Outlook

Today, numerous IDSs and IPSs are available, sometimes tailored to special scopes of application. Although risk rating approaches are integrated (partially) in some of the major

Tab. 5: Overview of Commercial Risk Rating Models

CISCO	JUNIPER	TIPPINGPOINT	MCAFEE	IBM
complex model consisting of: • accuracy of the signature (Signature Fidelity Rating) • damage if the attack succeeds (Alert Severity Rating) • target impact (Target Value Rating) aggregated risk rating model, realized as an integer value in the ranging from 0 to 100 • 1 = very low • 100 = very high	simple model represented by five groups: • Critical (Severity 1) • Major (Severity 2) • Minor (Severity 3) • Warning (Severity 4). • Informational (Severity 5)	simple model consisting of: • Critical (Number 4) • Major (Number 3) • Minor (Number 2) • Low (Number 1)	simple model consisting of a rating from 0-9 and 4 superclasses: • High (Number 7-9) • Medium (Number 4-6) • Low (Number 1-3) • Informational (Number 0)	simple model consisting of 3 severity levels: • High • Medium • Low

IDSs, their current functionality and exploitation is not sufficient. In the paper, we presented and compared different well-known open source as well as commercial IDSs including cross-vendor approaches and their respective risk rating capabilities. In this respect, there is a notable deviation, in particular with respect to the graduation (scale) as well as the underlying motivation. Besides those syntax-related differences, there are also differences in the area of semantics. It thus may happen that manufacturer A classifies an incident as serious and manufacturer B as medium. CVE/CVSS only partly changes this, since an CVE/CVSS-evaluation must first be made by a person and thus is only available with a certain time delay after the first occurrence.

Currently, we are working on the design of a generally applicable risk rating component which is able to process alert information of all major open source as well as proprietary IDSs presented based on IDXP, the Intrusion Detection Exchange Protocol (IDXP), the recommended transport protocol for IDMEF. In a further step, we also aim to assess their criticality wrt. the monitored network and pre-defined risk patterns. By that, intrusion alarms can be prioritized and evaluated based on, e.g., pre-defined SLAs or risk values. This enables multi-layered and more sophisticated Intrusion Detection reactions: e.g., an alarm which may be a false alarm can be dropped, if an incorrect decision based on it would generate a higher financial damage than missing a true alert would do (e.g., because the penalty that has to be paid when a service is deactivated (as part of a counter-measure) - by far - exceeds the expected damage).

References

[Al11] Albin, Eugene: A comparative analysis of the snort and suricata intrusion-detection systems. Master's thesis, Monterey, California. Naval Postgraduate School, 2011.

[Ba06] Babbin, Jacob: Security log management: identifying patterns in the chaos. Syngress, 2006.

[Ba11] Barker, Keith: , Protecting Critical Resources with Target Value Ratings (TVRs), August 2011. http://www.pearsonitcertification.com/articles/article.aspx?p=1739167, last seen on 11.01.2017.

[Ci09] Cisco Systems: , Cisco IPS Risk Rating Explained, 2009. http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd80191021.pdf, last seen on 07.04.2017.

[Co03] Corner, DS: IDMEF-" Lingua Franca" for Security Incident Management Tutorial and Review of Standards Development. SANS Institute, 2003.

[CS14] CS Group: , Prelude: Security Information and Event Management, 2014. http://www.prelude-siem.com/en/, last seen on 11.01.2017.

[HYD13] Hils, Adam; Young, Greg; D'Hoinne, Jeremy: , Magic Quadrant for Intrusion Prevention Systems, December 2013. http://www.gartner.com/technology/reprints.do?id=1-1OAVJS3&ct=131217&st=sb, last seen on 11.01.2017.

[IB17] IBM: , IBM Security Network Intrusion Prevention System (IPS): Configuring general settings for security events, 2017. https://www.ibm.com/support/knowledgecenter/SSB2MG_4.6.1/com.ibm.ips.doc/tasks/configuring_general_settings_for_security_events.htm, last seen on 11.01.2017.

[Mc15] McAfee: , McAfee Network Security Platform 8.2, 2015. https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25605/en_US/NSP-8275-8275-Virtual-IPS_Release-Notes_revB_en-us.pdf, last seen on 11.01.2017.

[MSR17] Mell, Peter; Scarfone, Karen; Romanosky, Sasha: , A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2017. http://www.first.org/cvss/cvss-guide.pdf, last seen on 11.01.2017.

[NS16] NSS LAbs: , Data Center Intrusion Prevention System Test, 2016. https://www.nsslabs.com/research-advisory/security-value-maps/2016/data-center-ips-svm-graphic/, last seen on 11.01.2017.

[OBB05] Orebaugh, Angela; Biles, Simon; Babbin, Jacob: Snort cookbook. O'Reilly Media, Inc., 2005.

[Pa14] Pathan, Al-Sakib Khan: The State of the Art in Intrusion Prevention and Detection. CRC Press, 2014. http://books.google.de/books?hl=de&lr=&id=o39cAgAAQBAJ&oi=fnd&pg=PA115, last seen on 11.01.2017.

[Se13] Sebastien Damaye: , Suricata-vs-snort/Test-cases/Fragmented-packets, November 2013. http://www.aldeid.com/wiki/Suricata-vs-snort/Test-cases/Fragmented-packets, last seen 11.01.2017.

[Ya09] Yasm, Curt: , Prelude as a Hybrid IDS Framework, 2009. http://www.sans.org/reading-room/whitepapers/awareness/prelude-hybrid-ids-framework-33048, last seen on 11.01.2017.