UDC 004.7.056.5

The methods of decreasing FP in Anomaly based Intrusion Prevent System by using of complex information about information system

Anton Kudin[1], Olga Grigorieva[2] and Svitlana Nosok[3]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"; National Bank of Ukraine, Kyiv, Ukraine, e-mail: pplayshner@gmail.com.*
[2] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" Kyiv, Ukraine, e-mail: olga.grygorieva.fb83@gmail.com*
[3] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" Kyiv, Ukraine, e-mail: nos.sv.ol@gmail.com*

Abstract
The main aim of this work is to optimize the efficiency of intrusion detection using complex analysis of indicators in information system by reducing the number of false positives, as well as the development of a universal technique for such optimization. Using laboratory environment with installed SIEMs Wazuh and Splunk we test the proposed optimization methods and proposed newly methodic for decreasing rating false/positive for some intrusion detecting systems.

Keywords: False Positives Optimization; Intrusion Detection Systems (IDS); Anomalies Detection; Comprehensive Behavioral Analysis; Security Information And Event Management (SIEM); Signatureless Intrusion Detection Methods

Introduction

Early intrusion detection is the main task of anything cybersecurity system. One problem of their building is decreasing ratio false/positive. This connected with some theoretical and practical problems. Such problems are:

1. Theoretical:
   - indistinguishability of anomalies caused by different types of events (which anomalies are attributed to attacks);
   - existing models do not clearly answer and give no recommendations on the choice of parameters, the limits of the scales for measuring parameters, etc.;
   - existing models do not fully consider the problem of working with primary / processed data (including the choice of the optimal solution for speed / accuracy);
   - inconsistency of these observations from sensors with different metrics thus, not the creation of a single metric, but optimal solutions in space without any metric (general theory of optimal algorithms);
   - trust and credibility of the data sensors.
2. Practical:
   - practical absence of introduction of modern models in commercial systems, predominant use of signature systems, complexity of introduction of the systems based on detection of anomalies

While the rising popularity of cloud data centers is understandable and leaves no arguments against them except for maybe privacy issues, the outsourced SOC matter is questionable. The period of pandemic caused a rapid increase in demand for third-party security services, but as some surveys show, compared to 37% of companies that used outsourced services in 2021, current 22% look less appealing [1]. Whatever statistics may be, it is also undoubtful that both small and unspecialized companies will continue to use such SOC`s help for managing their security due to cost and staff saves. It is often easier to use the already set-up mechanism than to build one from scratch, and though the third-party specialists may need more time to get familiar with a new infrastructure and will deal

with all the sensitive data in the company, the outsourced SOC benefits can make up for it. The process of configuring security systems to effectively detect anomalies and threats may be trickier with the outsourced SOC than with its in-house version, but it will either way obviously create a huge number of false positives. Although, skilled in-house experts are more likely to overcome this problem by thorough tuning, this is not always an option.

Trends in Cloud Data Centers and outsourced SOCs: Impact on Intrusion Detection Quality

Unsurprisingly, the key goal of each security system which relies on SIEM in the matter of finding anomalies, is to reduce the noise or false positive level. Thus, when speaking about efficiency of any detection set-up, we mean the level of false positive alerts it creates. The fewer false positives, the better the system.

To explore the problem, some fresh tendencies are worth mentioning:

1. Rising importance of communication channels in cloud

When relying mainly on cloud services for security or other issues, one must understand that if due to any reason a cloud is unreachable, the whole work stops inevitably. Among such reasons are of course the dreadful DDoS attacks that harm the availability of company`s resources, bringing up not only financial but also reputational damage. According to [2], DDoS attacks remain in the top10 of cloud security risks, hence, protection of communication channels between cloud and its clients are of a great importance. To mitigate them IDS usage and Firewall Traffic Inspection can be offered, as well as anomaly search and IP blocking, all of which will bring more false positive alerts. Unfortunately, even respectable companies like Cloudflare cannot propose more than manually adding exceptions or changing the sensitive level of the detection rule for cases, when legitimate traffic is classified as malicious [3].

2. Increasing IOC`s source authenticity requirements

By trusting immense lists of IOCs of arguable origin, a company decreases its detection efficiency and leaves both experts and system resources overwhelmed. IOC data bases should be not only updated frequently, but also validated for their confidence score and authoritative origin. Different methodologies can be used to evaluate IOC`s confidence score, for example as described in [4] or other ML based decisions. Another option is to analyze the cyber kill chain [5], which in fact can also be automated via ML. Although, a lot of companies are jealous when it comes to sharing a rather valuable experience of fighting against cyber threats, some open-source platforms for accounting IOC exist. Several examples include OpenIOC Framework, MISP, IBM X-FORCE, SANS Internet Storm Center, numerous open Github solutions etc.

3. Trusted attacker

As cloud services gained their popularity, they became of a great use not only to regular users, but also to hackers, which lead to an issue of a malicious user enjoying the same privileges inside the cloud service as a legitimate user. Moreover, a system is unlikely to check in-depth for example the internal traffic, than the one, coming from outside. As [6] states, “over 35% of cloud security incidents occurred from attackers’ use of valid, compromised credentials”. These statistics reveal a significant problem of mitigating such insider-like attacks, especially taking in consideration the fact that such actions may not be as obviously evil as other incidents. The question arises: How to distinguish such a user's activity from normal? Best practices include giving the least needed privileges to users, implementing some behavioural detection algorithms, and using the DSPM (Data Security Posture Management) approach that can prevent sensitive data breaches [7]. Just as finding anomalies can be the key, it will also create more detection noise.

4. Comprehensive analysis of user behavior

Owing to the advanced nature of modern cyber-attacks, a traditional signature-based attitude towards detection of deviations from normal user behaviour needs more comprehensive treatment. Hackers no longer threaten only high privileged accounts, they prefer to play safe and gradually gain more and more access to the system by starting with lower profile users that often don't get the security attention they need. Hopefully, protection measures are aware of the described risks and some solutions are already presented. Oracle`s CASB (Cloud Access Security Broker) Cloud Service for example has User Behavior Analytics (UBA) module that is able to perform “dynamic, user-risk scoring based on continual assessment

of user behavior", create access patterns and control users` usage of applications [8]. Other changes, including any privileges or security configuration, are also crucial to monitor and validate. IBM QRadar too offers similar UBA service [9] that utilises ML abilities to extract a behavior model from historical data of user activities. Another great instance of UBA implementation is Exabeam, which also by means of ML can detect deviations from established baselines.

5. Increasing volumes of telemetry data

In response to new attacks, specialists are forced to add more detection rules, log sources, checks, all of which multiples telemetry data annually. At some point the company's resources are exhausted, and it no longer has full control over the situation. "38% of companies operate with limited awareness of what's happening in their software", states [10]. Excessive log gathering otherwise means not all of them are actually used or useful in investigations. Among already mentioned problems [10] also remarks that "telemetry data is unstructured; varying formats make it hard to use; data preparation is time-consuming and sensitive data in logs may lead to compliance violations".

6. Not only IOC, but also other telemetry data should be considered comprehensively

It follows from the previous paragraph that all data can be gathered in vain when used without thought. For achieving early anomaly detection, it's never enough to conduct just IOC monitoring or other signature-based detection, as the whole landscape should be taken into account. Security specialists must observe not merely one alert, but rather the sequence of seemingly legitimate actions that result in some attack. This can be done by means of complex detection rules, based on the knowledge of previous attack schemes, for example such as MITRE propose. Alternatively, ML algorithms or neural networks can be fed with normal system activities and therefore learn to detect such suspicious patterns. Considering current tendencies in cloud services, we can only conclude that all of them demand a more comprehensive approach to detecting anomalies and broadening information we gather from systems, which in turn creates more false positive alerts unless we have the wisdom to tune the detection systems even more carefully or use advanced automated detection algorithms.

Limitations of statistical methods decreasing

The need to increase the size of the sample (the analyzed data) in order to reduce the error of the first kind follows directly from the Chebyshov theorem (or the law of large numbers) [28, 29], namely, with an increase in the number of observations, various random deviations of random values are equalized, therefore, with the probability that the arithmetic mean of the observation results tends to 1 will be arbitrarily little different from the arithmetic mean of the characteristic under investigation in the entire statistical general population.

We have the next one. Let $X_1, \dots X_n$ – independent equally distributed random variables with mathematical expectation M and variance. Then for each $\varepsilon > 0$ if $n \to \infty$ likelihood

$$P\left(\left|\frac{X_1+\cdots+X_n}{n} - M\right| < \varepsilon\right) \to 1 \qquad (1)$$

Even more, we can estimate the sample size n from the central limit theorem, which states that the distribution of a random variable $\sqrt{n}(\theta_n - \theta)$ (де θ_n – some statistic of random value, received with sample size of n, a θ – its theoretical analog) have asymptotic normal distribution with (a, σ^2) parameters. Then we have a clear statement of the optimization problem to determine the required amount of experimental data with some rate false/positive. The effect of increasing the number of different types of observed data on reducing the false/positive rate requires further explanation. First, such an increase makes it possible to more clearly define the theoretical distribution of experimental data. Secondly, as a rule, it allows in certain cases to move from statistical intrusion detection methods to deterministic ones, which in turn sharply reduces the false/positive rate. A simple example can be an additional analysis of the location of the analysis subjects (IP addresses) at the statistical limit of the number of false authorization attempts.

Experimental results discussion

Now we have a great problem with good dataset for experimental expectation new methods of intrusion detection. Datasets available to a wide range of researchers, such as KDD98, KDDCUP99, DARPA 1999, NSLKDD and others, just do not meet the above requirements. They are outdated, and therefore

do not show modern examples of events, let alone attacks; their size may be insufficient; the number of types of attacks and their balance leaves much to be desired; the information may not be sufficient or it may not be suitable for processing in the necessary ways. So we created own laboratory stand for giving our dataset. Then as part of the detection of unsuccessful remote login via SSH in Windows 11, 4 rules were created that, when triggered, create events:

- ssh_failed_WIN: fires if there were at least 5 failed logins in 5 minutes, critical Low
- ssh_failed_WIN_anomaly_hours: fires if there were at least 3 failed logins in 5 minutes, and during non-working hours, criticize Medium
- ssh_failed_WIN_anomaly_ip: triggers if there were at least 3 failed logins in 5 minutes, and from an unknown address, criticizes Medium
- ssh_failed_WIN_anomaly_hours_and_ip: triggers if there were at least 2 failed logins in 5 minutes, and during non-working hours, critical High

As result of experiment the following rules was created (see fig. 1).

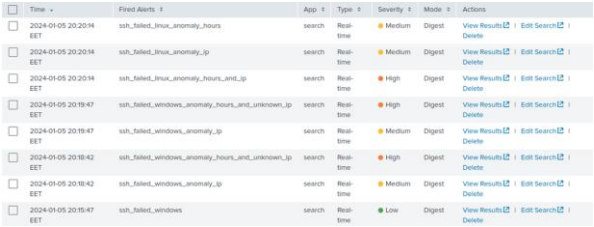

Figure 1: Examples of triggering by created rules

Acknowledgements

We express our gratitude to the entire team of Institute of Physics and Technology Institute and team of CRDF grant G -202102-67499.

Conclusions

We consider one problem decreasing false/positive rate in modern IDS based on fully using monitoring data on the functioning of the information system. The main idea is complex application of statistical and deterministic intrusion detection methods, which is clearly demonstrated by the example of the analysis of statistics of failed user authentication attempts. Another interesting approach is used of universal for all information systems indicators: the time of the event and the location (geography, IP address) of the event taking place. It is the complex application of these two indicators that significantly improves the effectiveness of intrusion detection. We also payed attention to the practical side of the work: a test bench was deployed based on two different types of protection systems - SIEM Splunk and Wazuh, and simulations of various attack scenarios, practical application of the proposed methods were carried out, and a methodology was developed that practically proves the effectiveness of the developed rules/methods of intrusion detection.

References

[1] Intrusion Detection System (IDS) [Електронний ресурс] // GeeksForGeeks – Режим доступу до ресурсу: https://www.geeksforgeeks.org/intrusion-detection-system-ids/ (дата звернення: 18.12.2023).

[2] A Survey on Secure Network: Intrusion Detection & Prevention Approaches [Текст] / A. Choubey, N. Thakur – International Journal of Engineering & Scientific Research Volume 4, Issue 8. – August 2016. – P. 74-88.

[3] What is the difference between signature-based and behavior-based intrusion detection systems? [Електронний ресурс] // Accedian – Режим доступу до ресурсу: https://accedian.com/blog/what-is-the-difference-between-signature-based-and-behavior-based-ids/ (дата звернення: 29.10.2023).

[4] Класифікація методів виявлення аномалій в інформаційних системах [Текст] / І.В. Рубан, В.О. Мартовицький, С.О. Партика – Системи озброєння і військова техніка, 2016, № 3(47) ISSN 1997-9568 – 102с.

[5] Survey of intrusion detection systems: techniques, datasets and challenges [Текст] / A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman – Springer Open Cybersecurity (2019) 2:20 – 22 с.

[6] How do antimalwares work and why they are not sufficient anymore [Електронний ресурс] // FlashStart – Режим доступу до ресурсу: https://flashstart.com/the-limits-of-traditional-antivirus-systems-why-they-are-not-sufficient-anymore/ (дата звернення: 29.10.2023).

[7] MITRE ATT&CK Matrix for Enterprise [Електронний ресурс] // MITRE – Режим доступу до ресурсу: https://attack.mitre.org/matrices/enterprise/ (дата звернення: 29.10.2023).

[8] A survey on anomaly and signature based intrusion detection system (IDS) [Текст] / A. Gangwar, S. Sahu – Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 4(Version 1), April 2014, pp.67–72 – 6 с.

[9] Signatureless Anomalous Behavior Detection in Information Systems [Текст] / V. Tkach, A. Kudin, V. Zadiraka & I. Shvidchenko – ISSN 1019-5262. Кібернетика та системний аналіз, 2023, том 59, №5 – ст.100–112 –12 с.

[10] Метод Виявлення Аномальної Поведінки в Локальній Мережі [Текст] / В. І. Батинчук, О. М. Барановський – XIV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених, 2018, 112-113с.

[11] Виявлення Аномалій в Телекомунікаційному Трафіку Статистичними Методами [Текст] / Т. Радівілова, Л. Кіріченко, М. Тавалбех, А. Ільков – Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 2021, ст. 183–194.

[12] Machine Learning for Anomaly Detection: A Systematic Review A. B. Nassif, M. A. Talib, Q. Nasir, F. M. Dakalbab [Текст] / IEEEXPLORE – Digital Object Identifier 10.1109/ACCESS.2021.3083060 – 43с.

[13] Top 8 Most Useful Anomaly Detection Algorithms For Time Series And Common Libraries For Implementation [Електронний ресурс] // SpotIntelligence – Режим доступу до ресурсу: https://spotintelligence.com/2023/03/18/anomaly-detection-for-time-series (дата звернення: 18.12.2023).

[14] Система виявлення аномалій методами інтелектуального аналізу даних [Текст] / О. Хомич – Магістерська дисертація 2022 – 91с.

[15] Survey Threat Hunting: Focusing on the Hunters and How Best to Support Them [Текст] / M. Fuchs, J. Lemon – SANS Whitepaper, April 2023

[16] Top 10 Cloud Security Risks & Solution in 2023 & How to Tackle Them [Електронний ресурс] // Appinventiv – Режим доступу до ресурсу: https://appinventiv.com/blog/cloud-security-risks-and-solutions/ (дата звернення: 29.10.2023).

[17] Handle a false positive [Електронний ресурс] // CloudFare – Режим доступу до ресурсу: https://developers.cloudflare.com/ddos-protection/managed-rulesets/adjust-rules/false-positive/ (дата звернення: 29.10.2023).

[18] Indicators of Compromise Confidence Scoring Method [Текст] / V. Tkach, O. Baranovskyi, A. Kudin, N. Godavarti, O. Kliok, S. Modali – The 12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 7-9 September, 2023, Dortmund, Germany – 9с.

[19] How to Defend With the Courses of Action Matrix and Indicator Lifecycle Management [Електронний ресурс] // SecurityIntelligence – Режим доступу до ресурсу: https://securityintelligence.com/how-to-defend-with-the-courses-of-action-matrix-and-indicator-lifecycle-management/ (дата звернення: 29.10.2023).

[20] “Authorized” to break in: Adversaries use valid credentials to compromise cloud environments [Електронний ресурс] // SecurityIntelligence – Режим доступу до ресурсу: https://securityintelligence.com/posts/adversaries-use-valid-credentials-compromise-cloud-environments/ (дата звернення: 29.10.2023).

[21] Avoiding the Storm | How to Protect Cloud Infrastructure from Insider Threats [Електронний ресурс] // SentinelOne – Режим доступу до ресурсу: https://www.sentinelone.com/blog/avoiding-the-storm-how-to-protect-cloud-infrastructure-from-insider-threats/ (дата звернення: 29.10.2023).

[22] The Importance of User Behavior Analytics for Cloud Service Security [Електронний ресурс] // Oracle – Режим доступу до

ресурсу: https://www.oracle.com/assets/user-behavior-analytics-3497541.pdf (дата звернення: 29.10.2023).
[23] QRadar User Behavior Analytics [Електронний ресурс] // IBM – Режим доступу до ресурсу: https://www.ibm.com/docs/en/qradar-common?topic=app-qradar-user-behavior-analytics (дата звернення: 29.10.2023).
[24] How to Maximize Telemetry Data Value With Observability Pipelines [Електронний ресурс] // DevOps IBM – Режим доступу до ресурсу: https://devops.com/how-to-maximize-telemetry-data-value-with-observability-pipelines/ (дата звернення: 29.10.2023).
[25] Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems [Текст] / Cheng-Yuan Ho, Yuan-Cheng Lai, I-Wei Chen, Fu-Yu Wang, and Wei-Hsuan Tai – IEEE Communications Magazine March 2012 – 146-154с.
[26] Reducing false positives in intrusion detection by means of frequent episodes [Текст] / L.O. Gigstad - Master's Thesis Department of Computer Science and Media Technology Gjøvik University College, 2008 – 95с.
[27] Discovery of Frequent Episodes in Event Logs [Текст] / M. Leemans, W. M.P. van der Aalst – International Symposium on Data-Driven Process Discovery and Analysis – November 2014 – 15с.
[28] Павловский З. Введение в математическую статистику / [Текст] Пер. с польского. – М.: Статистика, 1967. – 285 с.
[29] Тюрин Ю.Н., Макаров А.А. Анализ данных на компьютере / [Текст] М.: Финансы и статистика, 1995. – 384 с.
[30] Emphasis on the Minimization of False Negatives or False Positives in Binary Classification – Sanskriti Singh [Електронний ресурс] // Arvix – Режим доступу до ресурсу: https://arxiv.org/pdf/2204.02526.pdf (дата звернення: 18.12.2023).
[31] Using Root Cause Analysis to Handle Intrusion Detection Alarms [Текст] / Klaus Julisch – IBM Zurich Research Laboratory, 2003 – 148с.
[32] Reduction of False Positives in Intrusion Detection Based on Extreme Learning Machine with Situation Awareness [Текст] / Donald A. Burgio - Doctoral dissertation, 2019 – 139с.
[33] Wazuh About us [Електронний ресурс] // Wazuh – Режим доступу до ресурсу: https://wazuh.com/about-us/ (дата звернення: 18.12.2023).