kriativ.tech

Edição Nº 9 – 11-10-2021
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
http://www.kriativ-tech.com
DOI: 10.31112/kriativ-tech-2021-10-58

Extended Detection and Response
Importance of Events Context

Pedro Ramos Brandao
Coordinator Professor at Instituto Superior de Tecnologias Avançadas –
pedro.brandao@istec.pt
João Nunes
Master Degree Student at Instituto Superior de Tecnologias Avançadas
joaovitor.nunes@my.istec.pt

Abstract: *In an increasingly dynamic and unpredictable world regarding IT security, it's essential to use adequate solutions that boost infrastructures protection, whether local, in the cloud, or hybrid. This article contextualizes the challenges of the new reality of remote work with traditional security solutions. Furthermore, it explains the importance of implementing a solution that has a holistic view of the infrastructure and correlates all suspicious or attack events. Thus, it enhances an improved and updated security to the current reality.*

Keywords: *XDR, EDR, SIEM, Correlation, Context, Cybersecurity*

Abstract: *The world is increasingly dynamic and unpredictable in terms of computer security. It is important to use appropriate solutions that enhance the protection of infrastructures, whether local, in the cloud, or hybrid. This article contextualizes the challenges of the new reality of teleworking with traditional security solutions and explains the importance of implementing a solution that has a holistic view of the infrastructure and correlates all suspicious or attack events to enhance security improved and updated to the present reality.*

Keywords: *XDR, EDR, SIEM, Correlation, Context, Cybersecurity*

I. Introduction

The arrival of the Coronavirus pandemic has changed the paradigm of global companies that have been constrained to change their strategies and accelerate their digital transformation so that their staff could work from home. Thus, new challenges have emerged for businesses as they adapt to an operating model. Working from home has become the 'new normal', and cybersecurity has become a significant concern.

A study [1] states that 73% of the people who began working from home did not receive any training on using corporate resources safely.

Within a remote working environment, the use of videoconferencing software and collaboration tools has increased dramatically, and this growth has further increased attackers' interest in exploiting security gaps, including in this video conferencing software. For instance, a vulnerability was found in the Microsoft Teams messaging service, which allowed the attacker to gain access to all of the organization's accounts.

Furthermore, employees often use personal accounts on free services such as Google Docs to exchange files, and they even use personal devices to access corporate data.

In short, it's pretty tricky to control the remote environment in which employees work, and attackers have adapted, innovated, and exploit all potential vulnerabilities within the corporate network. So, traditional computer security solutions have become ineffective.

The typical endpoint user equipment security solution (Endpoint Detection and Response or EDR), a security information and event management (Security Information and Event Management or SIEM) platform will be presented in this article.

In addition, a new tool for threat detection and response (Extended Detection and Response or XDR) will be presented, with the differentiating feature of providing a holistic and simple view of the entire technological framework and also being able to correlate all events that occur, improving detection effectiveness, minimizing false alerts, and simplifying its management.

II. Literature Review

According to Hassan *et al.* [2], EDR tools generate a high volume of false positives and delay investigation tasks. In addition, determining the integrity of these alerts requires tedious manual work. The large load of log retention resources also causes them to be excluded before the investigation is started.

According to Karantzas and Patsakis [3], EDR solutions collect data from the endpoints, then store it and process it in a centralized system. However, as the name suggests, only endpoint data is collected, and no network information is collected.

According to Slate [4], the large volume of endpoints in companies increases the likelihood of vulnerabilities being exploited. Typically, less importance is given to these when compared to other operations in the company.

According to Gonzalez *et al.* [5], current SIEM systems are pretty limited in response, and countermeasure actions are selected and implemented without conducting a comprehensive impact analysis of attacks.

According to Chopra and Mahapatra [6], the correlation and contextualization process involves registering the events to create a picture of the attack or security incident.

According to Vielberth and Pernul [7], SIEM uses only log data and machine-generated events, which causes a lack of information in the absence of human interaction.

According to Jauhiainen [8], *Extended Detection and Response* (XDR) is an approach to simplify technologies from a security team and administrative point of view. Previously, the technologies and tools used to be scattered and did not work as a single unified engine. Typically, XDR solutions cover cloud, network, and endpoint workloads.

III. Approach

A. Endpoint Detection and Response (EDR)

This built-in endpoint security solution combines continuous, real-time monitoring and data collection with automated responses based on rules and analytics. The expression was suggested by Anton Chuvakin [9] to describe emerging security systems that detect and investigate suspicious activity on hosts and endpoints, applying automation to enable security teams to identify and respond to threats quickly.

This system allows having a single, global view of the endpoints as well as of their activities. It provides a centralized and integrated platform for data collection, correlation, and analysis, as well as for coordinating immediate threat alerts and responses, and has the following primary functions [10]:

a) Monitoring and collecting potential threat activity data from endpoints;
b) Analyzing data and identifying malicious patterns;
c) Automatically respond to identified threats by removing or stopping them as well as sending alert notifications;
d) Analysis tools to scan for identified threats and to detect suspicious activities.

EDR adoption is expected to increase in the coming years, with a yearly growth rate of 26%. [11].

One of the drivers for the increase in EDR adoption is the increase in network-connected terminals. Another important driver is the increasing sophistication of cyberattacks, which focus on endpoints as easier targets to infiltrate into a network.

On average, an information technology (IT) department manages thousands of endpoints. These endpoints include computers, servers, tablets, smartphones, Internet of Things (IoT)

devices, and even wearables such as smartwatches and digital assistants.

A study of SANS [12] indicates that 44% of IT teams may manage up to 500,000 endpoints and that each endpoint is a potential entry point for cyberattacks. Hence, their visibility and protection are critical.

Though today's antivirus solutions can identify and block threats and, to some extent, create automation, multiple security tools working independently complicate the process of detecting and preventing attacks, significantly if they overlap and generate similar security alerts.

B. Security Information and Event Management (SIEM)

SIEM is a solution that aggregates and analyzes the activity of the different resources of the entire information technology infrastructure and was developed to help security administrators implement security policies and managing events from various sources.

Usually, a SIEM is made up of separate blocks:

a) Source device;
b) Event collection;
c) Event normalization;
d) Action rules;
e) Event Storage;
f) Monitoring

This type of solution provides real-time analysis of security events generated by network devices and applications, and it is also possible to automate the selection and implementation of countermeasures. Current response systems select and implement security measures without conducting a comprehensive impact analysis of attacks and response scenarios.

In general, a SIEM solution provides the following features:

a) Correlation rules: the success of an event detection by a SIEM depends on the power of the correlation rules;
b) Data sources: ability to collect events from multiple, diverse data sources in the infrastructure;
c) Real-time processing: the ability to handle real-time data under constant change;
d) The volume of data: Analyzing large volumes of data from different sources is essential to get more details on events;
e) Visualization: It helps in the interpretation and interactive exploration of the collected data;
f) Data analysis: It allows an analysis of equipment event patterns;
g) Forensic: It will enable the analysis and event and even the capture of packets of network connections that are considered malicious;
h) Complexity: they are typically difficult to implement and manage;
i) Risk analysis: it may include features to perform risk analysis on the managed infrastructure;
j) Reaction and reporting features: Actions that SIEM supports to react against security incidents and how they are expressed to the correlation mechanism.

Although this solution provides good resources in terms of correlation, storage, visualization, and performance and allows the automation of reactions, these are still limited and are put into practice without conducting a global analysis of the impact of attacks and response scenarios [13].

Current SIEMs handle large volumes of data, but none have all the required data to detect all incidents. In addition, they provide limited contextual information on their native events, and one of the main flaws is related to unstructured data and emails.

For instance, one may detect an increase in activity on an IP address, but there is no visibility into who created that traffic or which files were accessed. In this situation, context will make all the difference. Thus, it may be either trustworthy data transfer or information theft.

The lack of context in security alerts may lead to a high number of false positives, which will cause security teams to start ignoring events and suffering an actual attack potentially.

SIEM solutions are essential to the security ecosystem, but these are not infallible. They only have visibility into the incoming data, and with no further context on that data, teams generally check and validate false positives or insignificant problems.

Therefore, context is critical in the world of data security to know which battles to fight.

C. Extended Detection and Response (XDR)

It is an approach for threat detection and response, providing a global and straightforward view of the entire technological scope. Thus, it enables data visibility across networks, clouds, endpoints, and applications, applying analytics and automation to detect, analyze, hunt, and patch threats [14].

The central differentiating point of XDR is that it collects and correlates data from the entire infrastructure, including email, endpoints, servers, cloud workloads, and networks, enabling global visibility and advanced threat context. Therefore, threats can be analyzed, prioritized, pursued, and corrected to prevent data loss and security breaches.

As the visibility is increased, as is the threat context, events that would not have been addressed before can be correlated as a whole, allowing security teams to identify and eliminate or mitigate the severity and scope of the attack.

XDR consolidates multiple products into a cohesive, unified security incident detection and response platform, evolving endpoint detection and response solutions [15].

XDR solutions enhance security operations efficiency, improving detection and response by combining visibility and control across endpoints, the network, and even the cloud. It collects and filters the various telemetry streams, analyzing tactics, techniques, and other types of threats to simplify operational security resources, providing a threat-focused business context and supporting faster response.

In general, it provides features such as detection and response to targeted attacks, support for user and device behavior analysis, threat intelligence, allows the reduction of the need to analyze false-positive events by correlating and confirming these alerts automatically, it makes more accurate incident triage, allows prioritization of activities, and comprehensive infrastructure analysis.

Thus, the security team will have more information on the following points:

a) Detection: critical threats are combined with endpoint telemetry, and the collected security events are further analyzed on complex platforms;
b) Investigation: it allows the correlation of all relevant collected event information and provides support in identifying the problem's root cause;
c) Recommendations: it provides advice to deepen the investigation through further queries and allows for actions to be taken to either contain or remediate a detected risk or threat;
d) Hunting: it will enable querying a data repository containing sensor telemetry from various vendors to detect suspicious behavior and threats, and thus taking a resolution action;
e) It is possible to block known and unknown attacks by leveraging artificial intelligence-based analytics and behavioral threat protection to stop malware, exploits, and fileless attacks.

IV. Discussion

A. Event Context

The word context in the dictionary means "a set of circumstances surrounding an event or situation," In cybersecurity, understanding the context is being able to differentiate between detecting a real threat or a false positive. For example, it would be pretty difficult to protect the infrastructure if each suspicious event was investigated isolated.

EDR security systems generate numerous events from the endpoints, yet managing them would become quite complex without contextualization.

Conventional antivirus could not identify all the threats, and it was necessary to create something that would monitor the endpoint to detect suspicious behavior and alert a security analyst should it occur. However, despite the simple idea, collecting and analyzing all the endpoint data creates other data storage and processing problems.

The data collected is just data until the analysis is carried out. Since the threat landscape is constantly changing on the part of the attackers, all the automation rules created for analysis have to be refined and modified regularly. Assuming

that you have no storage issues and the rules are always up to date, there is one final hurdle: context.

In computer security, traditional rules and mechanisms do generate events in case of identified potential threats. The problem is that if there isn't a set of conditions, there will be an excess of events, and this way, security centers would be challenging to manage. Thus, adding context to events will make security management more effective and mitigate false positives [16].

Therefore, by implementing a solution with intelligent context, one gains the ability to correlate automatically or through artificial intelligence the system's different activities, and thus becomes possible to relate processes and their heritage, helping to describe step by step the detection of the malicious system's behavior. It also supports understanding how the detection and response logic can be implemented at the contextualization level and adjusting the number of events that the security team will receive on the status of their environment.

B. How does XDR differentiate from SIEM?

XDR is considered a SIEM successor.

SIEM's primary capability is collecting and analyzing large volumes of log events and other data. It's primarily a research tool, requiring security teams to do a great deal of analysis to conclude.

XDR is focused on threat detection and response. It differentiates by automatically responding to threats or, if that is not feasible, it speeds up investigation and analysis, improving response times.

XDR's differentiating feature is that it provides visibility into the entire attack lifecycle in correlation to the whole environment, from infiltration to lateral movement, cleanup, or mitigation.

Adopting EDR, SIEM, and other solutions independently do not provide the strategic context and correlation needed to assess the current threat environment meaningfully. The XDR solution could help in filling this gap.

V. Conclusion

There are more and more devices and software that company employees use, which are hosted in multiple locations, and hackers are becoming more innovative and inventive when it comes to exploiting vulnerabilities and preparing attacks. It is therefore essential for companies to be aware that they have to be ready for the unknown. Thus, the response to attacks has to be increasingly fast and effective. It becomes essential to implement simplified solutions that allow security teams to have a global view of the infrastructure and all its applications and the existence of context and correlation of events.

Although there are no infallible solutions in computer security, implementing XDR will improve the effectiveness of security operations.

VI. References

[1] Kaspersky, "How COVID-19 changed the way people work," 2020.

[2] W. U. Hassan, A. Bates, and D. Marino, "Tactical provenance analysis for endpoint detection and response systems," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2020-May, pp. 1172–1189, 2020, doi: 10.1109/SP40000.2020.00096.

[3] G. Karantzas and C. Patsakis, "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors," pp. 387–421, 2021, doi: 10.3390/jcp1030021.

[4] S. Slate, "Endpoint Security: An Overview and a Look into the Future," *Lat. Am. Polit. Hist.*, 2018, doi: 10.4324/9780429499340-15.

[5] G. González-granadillo, S. González-zarzosa, and R. Diaz, “Trends, and Usage in Critical Infrastructures,” 2021.

[6] M. Chopra and C. Mahapatra, "Significance of security information and event management (SIEM) in modern organizations," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 7, pp. 432–435, 2019.

[7] M. Vielberth and G. Pernul, "A Security Information and Event Management Pattern," *Fed. Minist. Educ. Res.*, vol. 1, no. November 2018, pp. 1–12, 2018.

[8] H. Jauhiainen, "Designing End User Area Cybersecurity for Cloud-based Organization," no. February 2021.

[9] A. Chuvakin, "Gartner Blog Network," 2013. https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-

detection-response/ (accessed July 2021).
[10] Mcafee, "What is Endpoint Detection and Response (EDR)? " 2021.
[11] "Endpoint Detection and Response - Global Market Outlook (2017-2026)," *Stratistics Market Research Consulting*, 2018. https://www.marketresearch.com/Stratistics-Market-Research-Consulting-v4058/Endpoint-Detection-Response-Global-Outlook-12066121/ (accessed July 2021).
[12] L. Neely and A. Torres, "Endpoint Protection and Response: A SANS Survey," *SANS Inst.*, no. June, p. 16, 2018.
[13] J. Petters, "What is SIEM? A Complete Beginner's Guide - Varonis," 2020. https://www.varonis.com/blog/what-is-siem/ (accessed July 2021).
[14] Cisco, “What is XDR? - Extended Detection and Response - Cisco,” 2021. https://www.cisco.com/c/en/us/products/security/what-is-xdr.html (accessed July 2021).
[15] Mcafee, "What Is XDR? Extended Detection and Response l McAfee," 2021. https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-xdr.html (accessed July 2021).
[16] "Endpoint Detection and Response (EDR): o caso do contexto | Security Report," 2019. https://www.securityreport.com.br/overview/endpoint-detection-and-response-edr-o-caso-do-contexto/#.YPc5kRNKj0p (accessed July 2021).