IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11517

ENDPOINT PROTECTION MEASURING THE EFFECTIVENESS OF INSIDER THREAT REMEDIATION TECHNOLOGIES AND METHODOLOGIES

Mr.N.Karthikeyan[1], MS.N.Kalaiselvi [2], Mr.P.Nagarajan[3]

III BSC IT, Kaamadhenu Arts&Science College,Sathyamangalam[1]

Assistant Professor, Department of CA&IT, Kaamadhenu Arts&Science College,Sathyamangalam[2]

III BSC IT, Kaamadhenu Arts&Science College,Sathyamangalam[3]

Abstract: According to the research, employee training aimed at raising awareness of the importance of preserving the organization's sensitive data is ineffective.Furthermore, popular third-party cloud services make it much more difficult for employees to safeguard their company's secrets. As a result of this critical issue, a considerable market for software products that enable endpoint data security for these businesses has emerged. Endpoint protection platform (EPP), a conventional, negative endpoint protection strategy, and endpoint detection and response, a novel, positive endpoint protection method, will be discussed in our research (EDR). There will also be a comparison and evaluation of EPP and EDR in terms of mechanism and effectiveness.The study will also look at the benefits, flaws, and critical characteristics that a good security programme should have. The goal of this paper is to help small and large businesses better comprehend insider dangers in today's fast evolving internet, which is full with potential threats and attacks. This will also help businesses gain a better understanding of their employees' endpoints, allowing them to prevent data leaks in the future. It will also assist careless users in understanding the gravity of the problem they are facing and how they should protect their privacy while surfing the Internet while connected to the company's network.

INTRODUCTION:

Endpoint security, also known as endpoint protection, is a method of safeguarding computer networks that are remotely connected to client devices. Endpoints include many of the technological gadgets we use, such as cell phones, laptops, and tablets. Laptops, tablets, mobile phones, and other wireless devices connected to business networks present attack routes for security risks. When sending or receiving messages over the network, no one wants to be distracted or eavesdropped. As a result, endpoint security has emerged as a popular topic among cybersecurity researchers.

Laptop computers and cell phones have become an indispensible part of our daily lives. An enterprise's owner must determine some characteristics and standard techniques for safeguarding the most vulnerable endpoints. A hacker can gain access to company secrets by clicking on a phishing link in an e-mail, and a third-party 'cloud'service can easily become a hacker's target. In the same research, 53% of businesses said they had been the victim of an insider attack at least once in the previous year.Many businesses have been targeted in this manner in the recent past. Facebook, Sony, LinkedIn, and a slew of other well-known corporations are examples.

There are numerous methods and tools for defending an endpoint. We will concentrate on two of them in this paper: endpoint protection platform (EPP) and endpoint detection and response (EDR) (EDR). EPP is a security platform that includes anti-virus, anti-malware, data encryption, personal firewalls, and intrusion prevention systems. EDR has become a popular technique of identifying and responding to insider threats due to its unique features such as continuous monitoring, remediation, and no endpoint interference.

RELATED WORK:

The insider threat has long been regarded as one of the most serious issues in the realm of cybersecurity. Several tasks relating to the insider danger have been completed, and many studies have proposed various models and architectures for detecting the insider threat. Many specialists have attempted to identify threats by using new algorithms.

The author describes a framework that employs various modules to detect insider threats using algorithms and functional techniques. This function was also obtained by GP, an algorithm described in . Another mathematical method mentioned in purports to aid in the management of authorised administrators in order to detect insider threats. Some even suggest that we could detect the insider danger using a system-based architecture called directory virtualization. Machine learning is another important feature of the modern internet, and discusses a machine learning-based detection method.

In our article, we have provided distinct and extensive information regarding several forms of threat detection and response methods. Each one's functions, features, merits, and flaws are quickly and clearly understood by the reader. Furthermore, we have offered a comparison between EPP and EDR by collecting data and developing our own model. We evaluated them in a variety of settings and conditions to determine their full effectiveness and efficiency.Using our proposed approach, we can calculate the efficiency ratio formula for two products and forecast which one is more efficient under various conditions. We found the efficiency ratio equation in the proposed model. We created graphs and curves in Matlab to demonstrate the change in efficiency trend as different factors evolved. This will make it easier for our readers to comprehend our findings.

BENEFITS ANSD FEATURES OF ENDPOINT PROTECTION PLATFORM:

EPP is a traditional, signature-based, negative endpoint protection software. The major approach it employs to safeguard the endpoint is to compare the signatures of threats already stored in the database to evaluate whether or not they are hazardous. EPP is a combination of software tools and technologies that allow endpoint devices to be secure. Figure 1 depicts the key approach for dealing with the EPP threat. When a threat gets through the firewall, the Host Intrusion Detection System (HIDS) identifies it and determines whether or not it's harmful. Host Intrusion Protection System will mitigate the malicious ones (HIPS). The main aspects of EPP are listed in the next section.

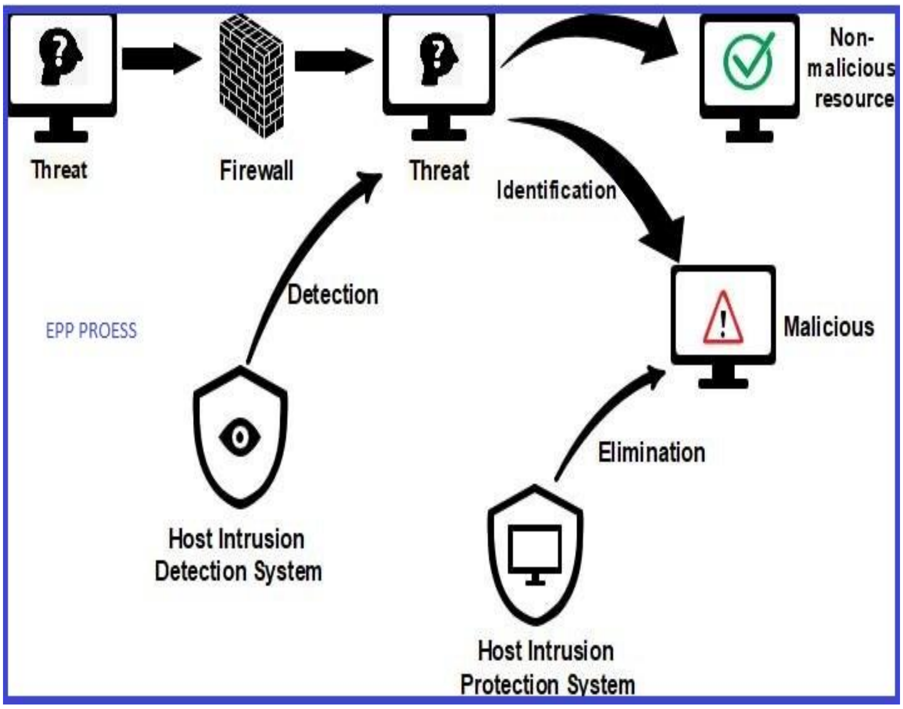

Figure 1: EPP address threats processing

The detection of the endpoint is the most important aspect of it. EPP features a full signature identity function, just like standard antivirus software. There are enormous amounts of the virus' signature database. This database can be used to identify each type of virus that has already been identified. Different algorithms are used in the matching process. Each security firm has its own set of algorithms for detecting threats. Detection is unquestionably an important aspect of endpoint security. However, no matter how cautious users are, viruses can still infiltrate the system or network through the endpoint. To keep their systems secure, organisations must prevent any risk of external intrusion through endpoints. The protection function seeks to eradicate the virus that has already infiltrated the system as a source of potential system damage. Attacks that take advantage of a fundamental flaw in standard endpoint security are becoming more common. They are unstoppable with current remedies. Figure 2 shows that the frequency of fileless attack is growing more rapidly than ever.

DOI: 10.17148/IJARCCE.2022.11517

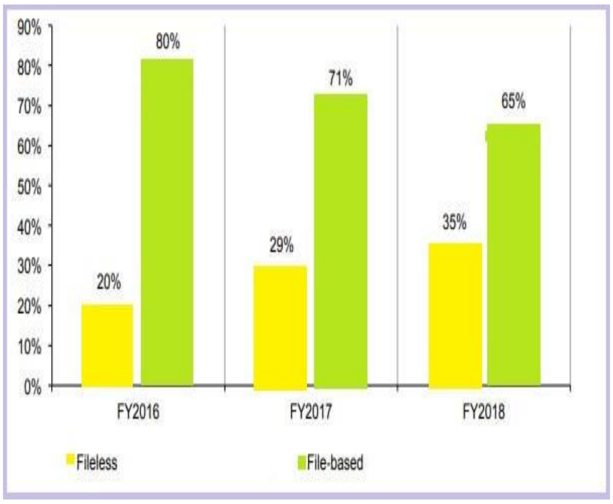

Figure 2: From 2016 to 2018, the number of fileless and file-based attacks increased

It's not enough to sit back and wait for standard security defences to identify assaults. Any organisation that wants to accomplish or improve real-time threat detection and incident response must engage in proactive threat hunting lead by human security professionals.Endpoint detection and response (EDR) software is a sophisticated form of positive endpoint protection. EDR isn't complete without threat intelligence. It can also provide anomaly detection and alerts, as well as cleanup of an infected internal network. They can also use machine learning to anticipate and evade the attack. The following sub-section lists the main aspects of EDR:

(Trusted one)
SERVER

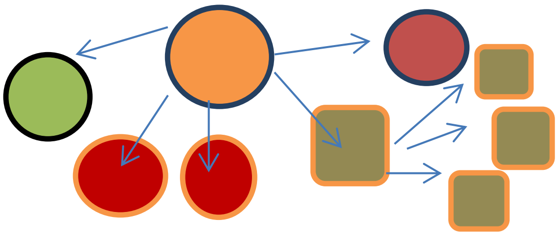

Figure 3: One trusted infected in EPP

Cyber Threat Intelligence (CTI) is also known as Threat intelligence, is information that is structured, evaluated, and refined concerning possible or ongoing attacks that pose a threat to a company. Avoiding risk is far safer and more dependable than placing accessible data and network at danger and then attempting to repair it. EDR isn't just a security programme; it also has a threat intelligence function that alerts businesses to potential hazards and dangers. It can give some danger information, which is collected by the EDR server. Instead of projecting the latent risk, this type of intelligence will aid in the eradication of the insider danger by evaluating information and data regarding previous insider threats.

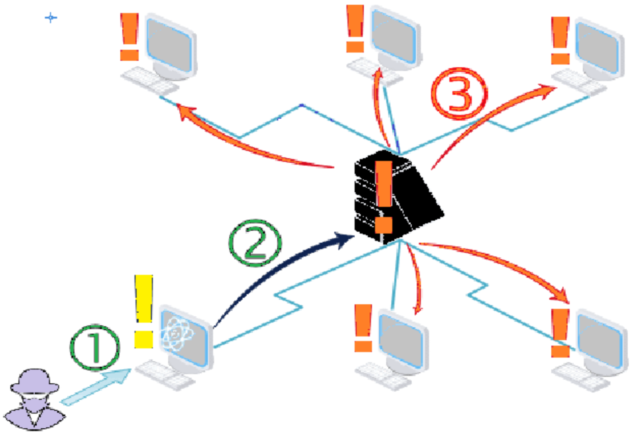

Figure 4:In entire internal network which process of insider threat infecting

DOI: 10.17148/IJARCCE.2022.11517

And, The virus's escalation stops once abnormal endpoints are cleaned up. One can believe that the entire system is clean and secure. The presence of the advanced virus, on the other hand, can act as an ink drop in clear water. It will quickly spread to the other side and contaminate the internal network.

CONCLUSION:

The reason for this is that most attacks are unable to penetrate the computer in depth due to the high detection rate. However, because EPP might slow down system operation, it must suffer a minor loss once it is activated. Even still, these losses are insignificant in comparison to the massive devastation that the incursion threatens. EPP and EDR, on the other hand, are the most popular and well acknowledged methods. We have a number of strategies in place to combat the threat of insiders. We discovered that their effects vary depending on the situation. When it comes to dealing with external dangers, EPP excels. EPP's component functions, such as HIDS, HIPS, and antiviruses, can successfully safeguard endpoints.The most critical and major issue, however, is that it is unable to guard against the insider threat. EPP is no longer the best choice when a malware infiltrates the internal network. EDR, on the other hand, can accomplish what EPP cannot. EDR has a lot of experience dealing with insider threats. It can gather various data and build intelligence to aid in the detection of aberrant endpoints and the elimination of insider threats. It also eliminates some of EPP's drawbacks, such as consuming too many resources. However, it is unable to perform the same functions as EPP.

REFERENCE:

[1] Margaret Rouse. “Endpoint security management”, Available: end point security management [Accessed: September .16,2018]

[2] TechTarget, “Endpoint security management.” Available: https://se archsecurity.techtarget.com/definition/endpoint-security-management [Accessed: March .11,2018]

[3] The Barkly team, “Endpoint Protection for the Mid-Market:3 Trends Driving Big Changes”, Available: https://blog.barkly.com/endpointprotection-trends-2018-mid-market[Accessed: July .15,2018]

[4] Barkly. “Endpoint Protection was the #1 spending priority in 2018”, pp1-2, 2018.

[5] Cybersecurity insiders. “2018 Insider threat report”, Available: htt ps://www.cybersecurity-insiders.com/portfolio/insider-threat-report/ [Accessed: March .11,2018]

[6] L. Xiangyu, L. Qiuyang, and S. Chandel, "Social Engineering and Insider Threats," 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing, 2017, pp. 25-34. Copyright © 2017, IEEE

[7] Zhang, Hongbin, et al. "An Active Defense Model and Framework of Insider Threats Detection and Sense." International Conference on Information Assurance & Security IEEE Computer Society, 2009:258261.

[8] DuetoC. Le, Sara Khanchi, A. Nur Zincir-Heywood, Malcolm I. Heywood, "Benchmarking evolutionary computation approaches to insider threat detection, “Proceedings of the Genetic and Evolutionary Computation Conference, Kyoto, Japan,2018, pp.1286-1293

[9] Yuqing Sun, Ninghui Li, Elisa Bertino, “Proactive defense of insider threats through authorization management, “Proceedings of 2011 international workshop on Ubiquitous affective awareness and intelligent interaction, Beijing, China,2011, pp.9-16