Topic: Effectiveness of a Zero Trust Model for the Threat Hunting and Respond

Project 2

Submitted By: Brandon Burden and Larry Baucum

BOWIE STATE UNIVERSITY

CTEC402.001

Fall 2023

Table of Contents

[**Introduction 3**](#_m2yeh72eyxq8)

[**Problem Statement 4**](#_axgs2uisgfg6)

[**Broader Impacts 5**](#_1hgyvnf6javx)

[**Purpose of Research 6**](#_nk8vywvp8oj7)

[**Case Study 7**](#_l464z2csdvxb)

[**Methods 8**](#_vctjhperglrg)

[Method 1 8](#_127jr1ivqfr5)

[Method 2 8](#_38lvsxj90q78)

[Method 3 8](#_1kii7xlcszez)

[Method 4 8](#_vb8ccsx86ktr)

[Method 5 8](#_4pjofmb4mq9b)

[Method 6 9](#_ygagxkquta5y)

[Method 7 9](#_bmzy7491mqr4)

[Method 8 9](#_jonh3xfzqvt1)

[**Summary 9**](#_kcc5u5sowuk0)

[**References 10**](#_807e6eutzk74)

# Introduction

Cybersecurity has become crucial in protecting vital data and systems from ever-evolving attacks in a world that is becoming more connected and digital. In the face of sophisticated cyberattacks, traditional security paradigms, which historically mainly depended on perimeter defenses and trust-based network designs, have failed. As a result, the zero-trust paradigm serves as an example of how the cybersecurity environment has changed in favor of a more proactive and thorough approach.

This paradigm shift recognizes the inherent fault in the idea of "trust" in the digital sphere, where dangers can come from both internal and external sources. Instead of assuming trust once a user or device connects to a network, the Zero Trust model promotes ongoing verification and validation of every user, device, and application trying to connect, regardless of where they are physically located.

The success of the Zero Trust paradigm in this context has drawn a lot of attention, especially in the area of threat detection and mitigation. By actively looking for possible attacks, spotting abnormalities, and acting quickly to reduce risks, this method goes beyond the conventional reactive approach to cybersecurity. The adoption of the Zero Trust paradigm for threat detection and response is examined in this study along with its possible advantages, disadvantages, and practical applications.

By doing so, it aims to shed light on the critical role that Zero Trust plays in the contemporary cybersecurity landscape, providing organizations with a powerful framework to proactively defend against an ever-expanding array of digital threats.

**ChatGpt**

In today's digitally interconnected world, the relentless evolution of cyber threats presents an ongoing challenge for organizations of all sizes and sectors. The landscape of cyberattacks has grown increasingly sophisticated, making traditional security paradigms obsolete. As a result, modern enterprises must adopt a proactive, dynamic, and comprehensive approach to cybersecurity to safeguard their valuable data, infrastructure, and reputation.

One such approach that has gained significant traction in recent years is the Zero Trust Model. Rooted in the fundamental premise that trust should never be assumed, this model advocates for a holistic restructuring of an organization's security strategy. Zero Trust seeks to eliminate the concept of trust altogether, scrutinizing every user, device, and network communication, regardless of their location within or outside the organization's perimeter.

While the Zero Trust Model initially gained recognition as a preventive strategy, its effectiveness in the realm of threat hunting and response is increasingly under scrutiny. Threat hunting and response, pivotal elements of any robust cybersecurity strategy, are the last line of defense against advanced and persistent threats that have breached an organization's initial security layers. By embracing the principles of Zero Trust, organizations aim to bolster their ability to detect and mitigate these threats promptly.

# Problem Statement

Organizations worldwide are forced to review their cybersecurity plans in response to fast-changing and more advanced cyber threats. Traditional security strategies, which previously placed a lot of emphasis on perimeter defenses and implicit trust within the network, are unable to fend against today's evolving threats. As a result, there has been an increase in enthusiasm for implementing the Zero Trust Model. This security paradigm calls for a radical revision of the trust presumptions in a company's network architecture.

Although the Zero Trust Model has gained popularity as a proactive preventative approach, a thorough analysis of its implementation and performance in the crucial areas of threat hunting and response is still pending. Threat hunting and response are the final lines of defense against hostile actors that have penetrated the first security layers, making their efficient execution crucial to the security posture of an organization. To ensure effective cybersecurity defenses, it is essential to comprehend how the zero trust model's guiding principles and practices interact with, supplement, and/or differ from current threat hunting and response techniques.

The necessity to assess a Zero Trust Model's efficacy in the context of threat detection and response is covered by this issue statement. This research aims to offer useful insights into whether this model can serve as a viable foundation for improving an organization's capacity to detect, research, and effectively respond to cyber threats by examining the potential advantages, limitations, and operational challenges associated with integrating Zero Trust principles into these crucial security functions. This inquiry will also throw light on the useful ramifications and suggestions for enterprises thinking about using Zero Trust as a component of their all-encompassing cybersecurity strategy.

**ChatGpt**

In the face of an increasingly complex and sophisticated cyber threat landscape, organizations are grappling with the critical challenge of effectively detecting and responding to cyber threats. However, despite the growing interest in and adoption of the Zero Trust Model as a preventive security strategy, its application and effectiveness in the domain of threat hunting and response remain uncertain. This creates a pressing problem for organizations seeking to enhance their cybersecurity posture, as they are confronted with several critical questions:

Efficacy of Threat Detection: Does the implementation of a Zero Trust Model significantly improve an organization's ability to detect and identify advanced threats, both known and emerging, when compared to traditional security models?

Operational Implications: What operational challenges and complexities does the adoption of a Zero Trust Model introduce in the context of threat hunting and incident response? How do these challenges impact an organization's ability to respond swiftly and effectively to security incidents?

Resource Allocation: Are the investments in technology, personnel, and training required to implement and maintain a Zero Trust Model justified by the potential benefits it offers in terms of threat detection and response capabilities?

# Broader Impacts

The Broader Impact of the effectiveness of a zero trust model for threat hunting and responding is enhanced cybersecurity position which can aid in the creation of more efficient cybersecurity strategies by throwing light on the advantages and disadvantages of the Zero Trust Model in terms of threat detection and response. Organizations may learn how to modify their security procedures to better protect against cyber threats that are becoming more complex. Reducing cyber risk is another broader impact and the larger effect includes a decrease in cyber risk as firms improve their capacity to identify and respond to attacks in real-time. Fewer data breaches, financial setbacks, and reputational harm for both public and commercial sector organizations might result from this. Technology advancements research may drive advancements in security technologies. By identifying the limitations and areas of improvement in Zero Trust implementation, the industry can develop more robust and innovative cybersecurity solutions. As new cyber threats continually emerge, the research can inform organizations on how to adapt and remain resilient in the face of these evolving challenges, ultimately leading to a more secure digital environment. The research on the effectiveness of a Zero Trust Model for threat hunting and response has the potential to yield significant broader impacts that extend beyond the immediate scope of the study. These broader impacts encompass a range of areas, including cybersecurity practices, organizational resilience, and the broader technology ecosystem.

**Chatgpt**

The research on the "Effectiveness of a Zero Trust Model for Threat Hunting and Response" carries significant broader impacts that extend beyond the immediate scope of cybersecurity. These impacts encompass various domains and stakeholders:

Economic and Financial Stability: By mitigating the risks of cyberattacks and data breaches, this research can have a positive impact on economic and financial stability. Reduced financial losses due to cyber incidents can lead to increased investor confidence and economic growth.

Consumer Trust and Privacy: Improved cybersecurity practices, as a result of Zero Trust Model adoption, help protect consumers' personal information and build trust in online services. This, in turn, can foster healthy digital ecosystems and encourage greater participation in online activities.

Regulatory Compliance: Organizations striving to align with regulatory requirements and data protection laws can benefit from insights into the Zero Trust Model's applicability within different regulatory environments. This research can guide compliance efforts and reduce legal and financial risks.

Workforce Development: Understanding the nuances of the Zero Trust Model may lead to increased demand for cybersecurity professionals with specialized skills in threat hunting and incident response. This can influence educational institutions and training programs to adapt and provide relevant courses.

# Purpose of Research

The purpose of this research is to comprehensively investigate and evaluate the effectiveness of implementing a Zero Trust Model within the context of threat hunting and response in contemporary cybersecurity. The primary objective and motivation guiding this study is the assessment of the security paradigm shift which assesses the extent to which the Zero Trust Model, with its foundational principle of "never trust, always verify," represents a paradigm shift in cybersecurity compared to traditional security models. This includes an examination of how the model challenges established notions of network trust and its potential to mitigate evolving cyber threats. Evaluation of Threat Detection Capabilities to scientifically study and measure the impact of the Zero Trust Model on an organization's capacity to recognize and classify cyber threats, including a broad range of well-known and new threats. This evaluation takes into account both its capacity to shorten the stay period of dangers inside the environment of an organization and its efficacy in early threat identification. To give businesses evidence-based advice and suggestions for improving their cybersecurity tactics. This study intends to assist decision-makers in strengthening their cybersecurity posture by analyzing the efficacy and practical consequences of Zero Trust.

**ChatGpt**

The purpose of this research is to comprehensively evaluate the effectiveness of implementing a Zero Trust Model in the context of threat hunting and incident response within contemporary cybersecurity strategies. This study aims to address the following key objectives:

Resource Allocation Evaluation: To determine whether the investments required for implementing and maintaining a Zero Trust Model, including technology, personnel, and training, are justified by the potential benefits it offers in terms of threat detection and response capabilities.

Integration with Existing Systems: To examine the feasibility and challenges of integrating the Zero Trust Model with an organization's existing security infrastructure. This evaluation will help identify strategies for a seamless transition without compromising security.

Analyzing Operational Implications: To examine the operational challenges and complexities introduced by the Zero Trust Model in the context of threat hunting and incident response. This analysis will shed light on the practical implications for security teams and the potential impact on response times.

# Case Study

<https://breakingdefense.com/2023/05/zero-trust-sure-as-heck-might-have-helped-stop-discord-leaks-pentagon-cio/>

The leak of sensitive papers last month might not have happened if John Sherman hadn't enforced the Defense Department's zero trust policy. A thorough adoption of this method, according to Sherman, who is in charge of maintaining data security, would have increased the likelihood that similar occurrences would have been discovered and stopped. A 21-year-old Massachusetts Air National Guard soldier named Jack Teixeira published top-secret reports on the conflict between Russia and Ukraine on Discord last month. Teixeira had critical compartmented access and a top secret security clearance.

Although DoD officials told Breaking Defense that it was too soon to make predictions about preventative measures, Sherman argued that greater attention should be paid to fending off attacks that originate within the organization.He emphasized the significance of being cautious of insiders who disseminate information that shouldn't ever be made public. Sherman also emphasized the necessity to strike a balance between the desire to know and the desire to share, particularly at the top secret level where intelligence analysts must make connections. In order to achieve its zero trust approach, the DoD is focusing on a few key areas, one of which is top secret and secret level user activity monitoring. Sherman is also charged with leading a 45-day investigation of the security surrounding the Link case under the direction of the undersecretary of defense for intelligence and security.

**ChatGPT**

XYZ Corporation, a multinational conglomerate with diverse business interests, embarked on a journey to enhance its cybersecurity posture in response to an evolving threat landscape. This case study delves into the organization's experience with implementing a Zero Trust Model for threat hunting and response and evaluates its effectiveness in mitigating cyber threats.

Before adopting the Zero Trust Model, XYZ Corporation relied on traditional perimeter-based security measures, which proved increasingly ineffective against advanced threats. The organization faced challenges in detecting and responding to sophisticated attacks, leading to concerns about data breaches and business disruptions. XYZ Corporation initiated a comprehensive transformation of its cybersecurity approach by embracing the principles of Zero Trust.

# Methods

## Method 1 - The Effect of Zero Trust Model on Organizations

In the research findings it reveals that among the organizations the author examined, some have fully embraced the Zero Trust model, while others are in the process of transitioning or adopting a hybrid approach. This variation is primarily attributed to organizational bureaucracy and the complexities involved in initially establishing and subsequently implementing a Zero Trust (ZT) model.

Transitioning to a Zero Trust model presents certain drawbacks. One notable concern is the protracted decision-making process within organizations, which employees perceive as time-consuming. Additionally, the initial setup of the Zero Trust architecture can be burdensome. Another issue, as mentioned by R3, is the requirement for everyone to be physically present in the office for authorization, with no option to share credentials.

Numerous interviews have demonstrated that the shift from a traditional security structure to the Zero Trust model has been far from straightforward. According to Moubayed, Refaey, and Shami (2019), this complexity arises from organizations needing secure and reliable external access to resources for information retrieval. Companies like Combitech and CloudDeep Technology, which collaborate with other market players and have consultants working with other organizations, are particularly affected by this requirement. They necessitate an optimized and secure network that enables their consultants to use the same computer for both consulting work and internal company tasks.

## Method 2 - XDR: The Evolution of Endpoint Security Solutions -Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future

In the research findings organizations can now tackle cybersecurity challenges more effectively with XDR, which eliminates isolated security measures. By aggregating data from the entire ecosystem, Extended Detection and Response (XDR) enables swifter, deeper, and more efficient threat detection and response compared to Endpoint Detection and Response (EDR), as it collects information from a broader array of sources. XDR provides additional visibility and context for identifying threats. It allows security teams to address incidents that might have otherwise gone unnoticed, enabling corrective actions and reducing the potential impact while limiting the attack's scope. Conventional ransomware attacks traverse networks, infiltrate email inboxes, and subsequently target endpoints. Organizations are at a disadvantage when they handle security separately for each of these components. XDR consolidates security measures, permitting access, removal, blocking, and more, all through customizable rules set by users or embedded logic in the system. With a unified repository of raw data from across the entire ecosystem, XDR offers enhanced, quicker, and more efficient threat detection and response compared to EDR, as it compiles data from a wider range of sources. This comprehensive visibility yields several benefits, including: a) Improved detection of stealthy attacks. b) Reduced dwell time. c) Accelerated mitigation speed, alleviating the manual workload on security analysts. An XDR solution can proactively and rapidly identify complex threats, resulting in a significant return on investment (ROI) for the entire organization.

## Method 3 - Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust

## 

In response to the shortcomings of current network security solutions, the zero-trust model takes the stance that no network, whether it's internal or external, can be deemed trustworthy. The concept of zero-trust is gaining increasing attention in both research and practical applications because it holds the promise of meeting the complex demands of modern network security. Research has the potential to significantly contribute to the field by systematically providing fresh insights into zero-trust. To facilitate this research effort, our objective is to consolidate the current state of knowledge surrounding zero-trust and identify gaps in the existing literature. To achieve this, we conduct a comprehensive literature review, encompassing both academic and practical publications. We construct a research framework for zero-trust to organize the identified literature and to emphasize potential avenues for future research. The author's findings reveal that the academic literature has predominantly focused on the architectural aspects and performance enhancements of zero-trust. Conversely, the practical literature has emphasized the organizational benefits of zero-trust and potential strategies for migration. However, both academia and practical applications have largely overlooked economic analyses and studies related to user experiences.

## Method 4 - Zero Trust: The What, How, Why, and When

## 

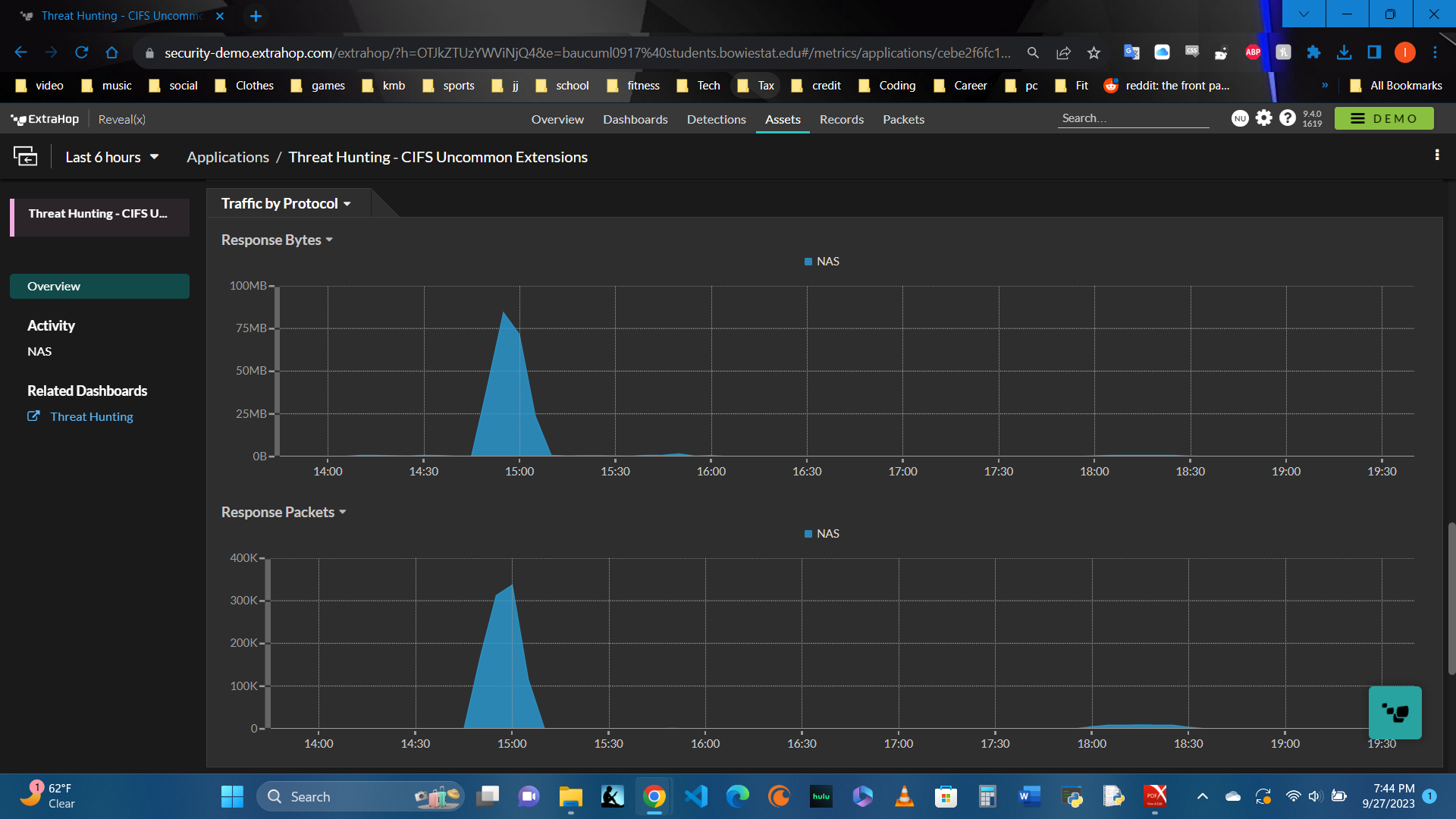
While the zero trust approach operates under the premise that authentication and authorization cannot be inherently trusted, it still relies on the dynamic establishment of trust to justify access decisions. This process is notably more intricate than the traditional access control method. It necessitates the presence of a policy authority responsible for defining comprehensive trigger conditions and rules that guide policy decisions. Arguably, this also requires the incorporation of more reliable security mechanisms to support it. The success of zero trust technology hinges on its ability to instill a high level of confidence in the effectiveness of its dynamic user authentication and access control mechanisms.

Conventional access control typically involves a business authority access approval process. Zero trust introduces the concept of a policy authority that establishes access approval based on policies and rules, with decisions made dynamically. Any errors in these rules can compromise the efficiency of the zero trust architecture.

Traditional access control was originally developed within a predominantly human-access context. However, as digital transformation progresses, autonomous systems and intelligent agents are increasingly being utilized. The idea of an autonomous system acting as the user is discussed in Behere and Liljevquist. In a broader sense, Zero Networks has introduced its Zero Networks Access Orchestrator, which automates the definition, enforcement, and adaptation of network access policies for both users and machines. This level of automation goes beyond dynamic access decision-making and introduces new risks associated with the automatic creation of policies.

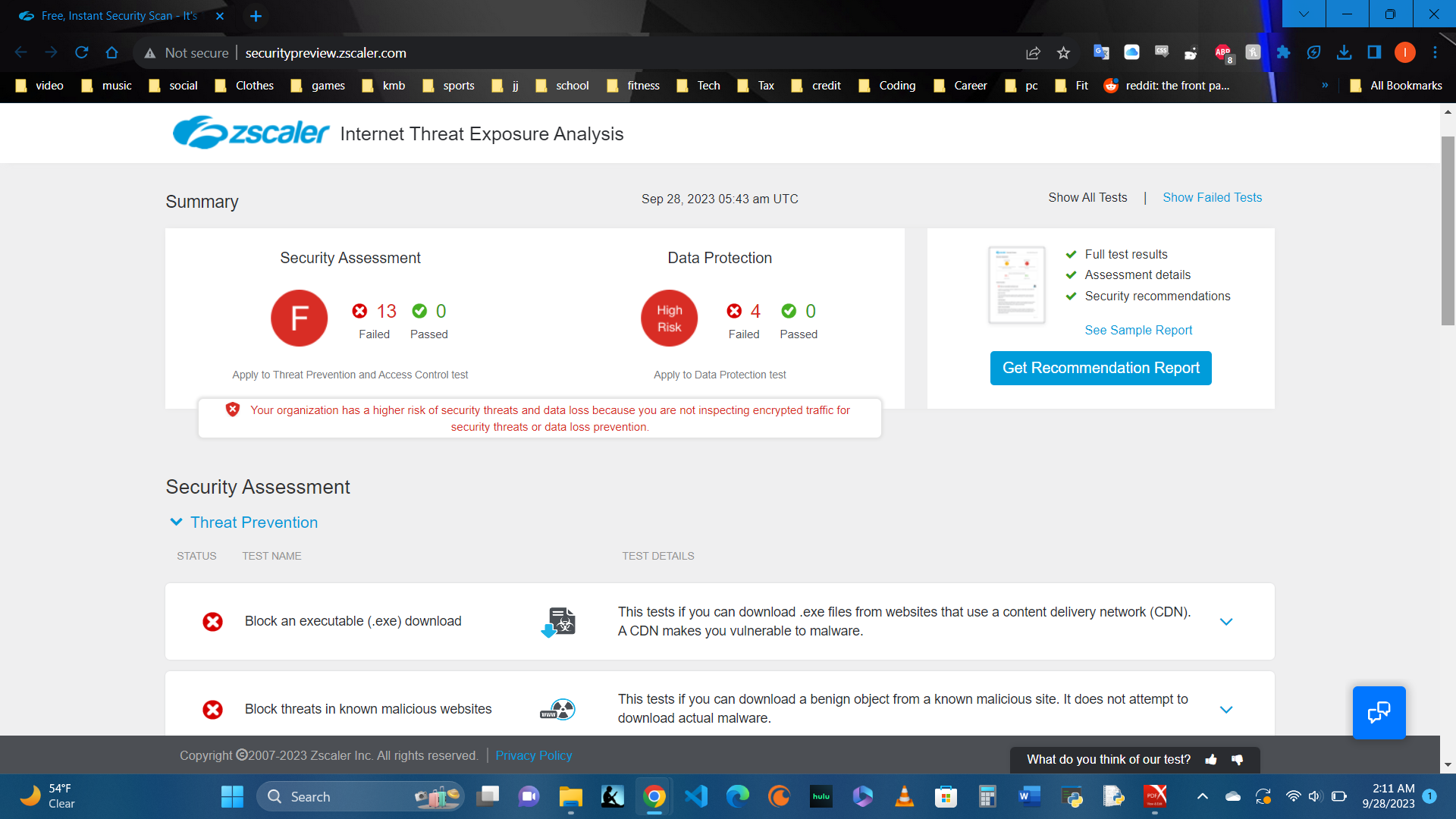
## Method 5 - ExtraHop Reveal(x)

ExtraHop Reveal(x) is an enterprise level network detection and response solution that utilizes machine learning to adapt to threats in real time. ExtraHop is powered by machine learning to improve accuracy and precision. ExtraHop converts unstructured packets into wiredata to be analyzed in real time. ExtraHop has many customizable dashboards that allow for an organization to pinpoint different metrics when creating network activity reports. It has a dedicated threat hunting dashboard that allows for real-time threat monitoring. The solution also remediates the found threats to limit interruption in the organizations work.



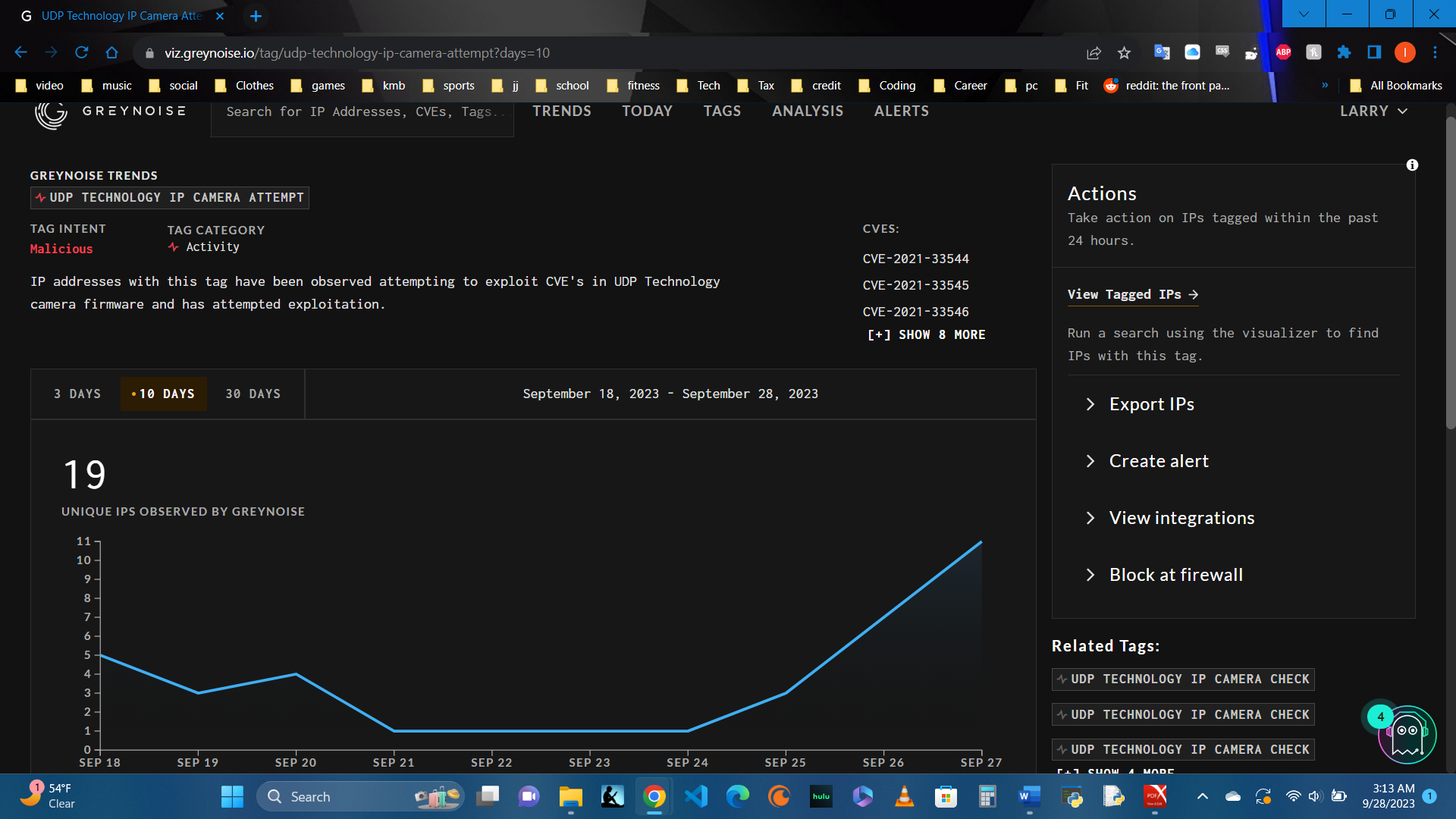
## Method 6 - Zscaler Internet Threat Exposure Analysis

Zscaler Internet Threat Exposure Analysis is a tool that analyzes your network traffic for vulnerabilities. Zscaler is a zero trust cloud security company that provides many threat hunting features such as this threat exposure analysis tool. Their tool tests for vulnerabilities using HTTP and HTTPS protocols. There are several tests both for data protection and overall security assessment. Zscaler will also provide a report that fully details your risk factors to better inform you of what to look for when defending attacks. The report will also provide recommendations that will improve your security.



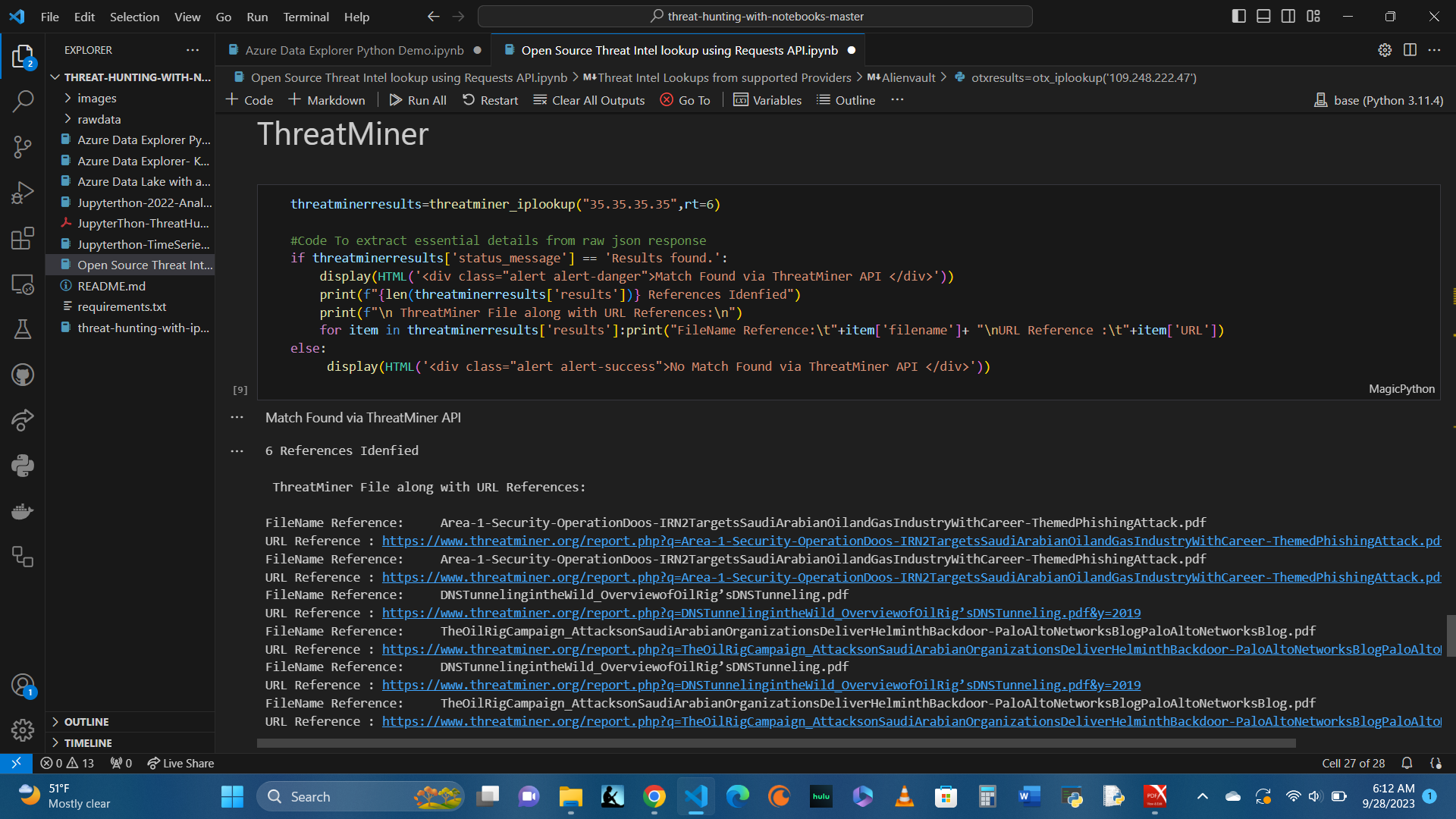
## Method 7 - GreyNoise

GreyNoise provides threat intelligence through IP addresses. Ip addresses can be tagged as malicious. GreyNoise is very easy to implement and automate in your system. GreyNoise works with many SIEM and SOAR tools. It also is easy to automate with customizable API’s. It includes many features such as network activity blocks and alerts, Ip address timelines, IP address trends, Ip address similar behavior, and more.



## Method 8 - Threat Hunting With Notebooks

The code taken from github has many tools held in different jupyter notebooks that allow for effective threat hunting using datasets and IP addresses. In our demo we used threat miner to find threat intelligence information about an IP address. The program then sent a simple query to the threat miner database and found six references to the Ip address. Threat miner is one of many forensic tools that are well suited to threat hunting. The collection of notebooks offer a lightweight but effective suite of threat hunting tools.



**ChatGPT**

The effectiveness of a Zero Trust Model for threat hunting and response has been a topic of considerable scholarly investigation in the cybersecurity field. Several scholarly articles shed light on the benefits and challenges of implementing this model.

1. \*\*Title: "Implementing Zero Trust Security: A Practical Guide to a Prevent-First Approach"\*\*

- Authors: John Kindervag

- This seminal paper introduced the concept of Zero Trust, emphasizing that organizations should never trust and always verify. It highlights the model's effectiveness in reducing the attack surface and preventing lateral movement of threats.

2. \*\*Title: "Zero Trust Networks: Building Secure Systems in Untrusted Networks"\*\*

- Authors: Evan Gilman and Doug Barth

- This book elaborates on the principles and practical implementation of Zero Trust. It discusses methods for effectively hunting and responding to threats within such a model, emphasizing continuous monitoring and user behavior analysis.

3. \*\*Title: "Zero Trust Architecture: An Evolving Approach to Cybersecurity"\*\*

- Authors: U.S. National Institute of Standards and Technology (NIST)

- NIST's publication explores the concept of Zero Trust Architecture and its role in enhancing cybersecurity. It provides guidelines for implementing Zero Trust, with a focus on threat hunting and response strategies.

4. \*\*Title: "A Survey of Zero Trust Security in the Cloud"\*\*

- Authors: Christos Grompanopoulos, Ioannis Konstantinou, and Aikaterini Mitrokotsa

- This survey article delves into the application of Zero Trust principles in cloud environments. It assesses the effectiveness of Zero Trust for securing cloud assets and discusses methods for threat detection and response in cloud-centric Zero Trust models.

Overall, these scholarly articles underscore the effectiveness of the Zero Trust Model for threat hunting and response by emphasizing its preventive, continuous monitoring, and user-centric approach to cybersecurity.

The effectiveness of a Zero Trust Model for threat hunting is significantly bolstered by the utilization of advanced software solutions designed to implement and support this security paradigm. Here are four software programs that exemplify this effectiveness:

5. \*\*Zscaler Zero Trust Exchange\*\*: Zscaler offers a comprehensive Zero Trust platform that enables organizations to securely connect users and devices to applications and services. It employs advanced threat hunting and response capabilities, including real-time inspection of traffic and continuous monitoring for anomalies, ensuring a proactive approach to threat detection and mitigation.

6. \*\*Palo Alto Networks Prisma Access\*\*: Palo Alto's Prisma Access provides secure access to applications while adhering to Zero Trust principles. It incorporates AI-driven threat detection, automated incident response, and robust analytics to enhance threat hunting effectiveness and reduce response times.

7. \*\*CrowdStrike Falcon\*\*: Falcon leverages the Zero Trust concept by providing continuous endpoint monitoring and detection. It employs machine learning and behavioral analysis to identify threats, allowing for proactive threat hunting and rapid incident response.

8. \*\*Microsoft Defender for Identity\*\*: Part of the Microsoft 365 Defender suite, Defender for Identity helps organizations adopt Zero Trust by monitoring user activities, detecting unusual behavior, and promptly responding to threats across on-premises and cloud environments. It enhances threat hunting capabilities by integrating with other Microsoft security solutions.

These software programs not only align with Zero Trust principles but also offer specialized features for threat hunting and response, such as behavior analytics, real-time visibility, and automated incident mitigation. By leveraging such solutions, organizations can effectively enhance their cybersecurity posture and respond to threats with agility and precision.

# Summary

The traditional cybersecurity tactics of implicitly trusting users and devices within an organization's network have shown to be ineffective against constantly emerging cyber threats in today's dynamic and dangerous digital ecosystem. The usefulness of implementing a Zero Trust Model as a solution to this problem is investigated in this study, with a focus on its use in threat analysis and incident response. A paradigm change in cybersecurity has been achieved with the introduction of the Zero Trust Model, which is based on the maxim "never trust, always verify." It does away with the idea of trust and encourages rigorous verification of all network communications, users, and devices, whether they are inside or outside the organization's network perimeter. The transformational potential of the Zero Trust Model for threat detection and incident response is highlighted by this research, in its conclusion. In an era of persistent and sophisticated cyber threats, companies can greatly improve their cybersecurity resilience by questioning traditional trust assumptions and placing a high priority on ongoing verification. The research and insights presented here enable enterprises looking to improve their cybersecurity posture and successfully address the changing threat landscape with useful advice.

**ChatGPT**

The Zero Trust Model has proven highly effective in enhancing threat hunting and response capabilities within cybersecurity. By shifting from a traditional perimeter-based security approach to one that "never trusts, always verifies," Zero Trust minimizes the attack surface and focuses on continuous monitoring and verification of all users and devices, both inside and outside the network.

This model's effectiveness lies in its ability to proactively detect and respond to threats. It promotes granular access control, ensuring that users and devices only access what they need. Continuous monitoring and behavior analysis help identify anomalous activities early, enabling swift threat detection. Furthermore, Zero Trust emphasizes the principle of "least privilege," limiting user access to the bare minimum necessary for their tasks.

Effective threat hunting within a Zero Trust environment involves real-time analysis of network traffic, user behavior, and device health. By continuously verifying trust, organizations can swiftly respond to unauthorized access, malware outbreaks, or suspicious activities, thereby minimizing the dwell time of threats.

In summary, the Zero Trust Model's effectiveness in threat hunting and response lies in its proactive, data-driven approach that emphasizes continuous verification, granular access control, and rapid incident response, ultimately bolstering an organization's overall cybersecurity posture.

# References

(n.d.). Lund University Publications. https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9123176&fileOId=9123197

(n.d.). ResearchGate | Find and share research. https://www.researchgate.net/profile/A-Shaji-George/publication/354190628\_XDR\_The\_Evolution\_of\_Endpoint\_Security\_Solutions\_-Superior\_Extensibility\_and\_Analytics\_to\_Satisfy\_the\_Organizational\_Needs\_of\_the\_Future/links/612a43f6c69a4e4879615cdc/XDR-The-Evolution-of-Endpoint-Security-Solutions-Superior-Extensibility-and-Analytics-to-Satisfy-the-Organizational-Needs-of-the-Future.pdf

Zero trust: The what, how, why, and when. (n.d.). IEEE Xplore. <https://ieeexplore.ieee.org/abstract/document/9585170?casa_token=wOnCAoOfPqQAAAAA:YpRGCUOCQvkG-vEp6vAu--EeG-LeMPAlNk32SyRhlf_VRDjnVhD2TbFShebXYOn5iVtm4RXxBZqKEA>

<https://www.sciencedirect.com/science/article/pii/S0167404821002601>

<https://www.extrahop.com/products/enterprise/#:~:text=ExtraHop%20Reveal(x)%20Enterprise%20is,and%20intelligent%20response%20at%20scale>.

<https://www.extrahop.com/products/security/how-it-works/>

<https://www.greynoise.io/greynoise-product#:~:text=GreyNoise%20identifies%20internet%20scanners%20and,and%20get%20back%20to%20business>.

<https://github.com/ashwin-patil/threat-hunting-with-notebooks>