Technical Presentation on

Enhancing Cyber Resilience: The Role of Threat Intelligence in Risk Management

By

Tharunaditya Anuganti 20P61A6206

Cyber Security Department

Abstract

This technical research paper investigates the role of threat intelligence in risk management in cyberspace. The study analyzes current practices in threat intelligence and risk management, identifying gaps and challenges, and proposing solutions for improving cyber resilience. The findings contribute to the development of best practices for threat intelligence and risk management, helping organizations proactively identify and mitigate cyber threats. The research includes a review of prestigious research papers and surveys conducted both in and out of the college. The study provides technical and practical insights valuable to cybersecurity professionals, IT managers, and risk management experts, aiming to create a more secure and resilient cyber landscape.

Contents

Introduction

Enhancing cyber resilience through threat intelligence involves leveraging actionable insights to proactively detect and respond to cyber threats, fortifying organizations' defenses and minimizing the impact of potential attacks.

Understanding Cyber Resilience

Understanding cyber resilience involves the ability of individuals and organizations to anticipate, withstand, and recover from cyber threats, ensuring the continuity and security of their systems and data.

The Evolving Threat Landscape

- Evolving threat landscape: ever-changing cyber threats and risks.
- Constant development and adaptation of techniques, tactics, and tools.
- Exploitation of vulnerabilities and malicious activities.

Introduction to Threat Intelligence

Threat intelligence is the knowledge and information about potential and existing cyber threats. It helps organizations understand and proactively defend against threats, enhancing their overall cybersecurity posture.

Integrating Threat Intelligence into Risk Management

- Integrating threat intelligence into risk management.
- Utilizing information about potential cyber threats.
- Informing and enhancing risk assessment and mitigation processes.
- Better prioritization and resource allocation.
- Protection against relevant and imminent threats.

Threat Intelligence Sharing and Collaboration

Trust relationships
Define rules of engagement with sharing partners
Verification credibility and reliability of information

- Collect
- Analyze
- Categorize

From various sources such as

- Internal security tools
- Open source feeds and industry specific sharing platforms

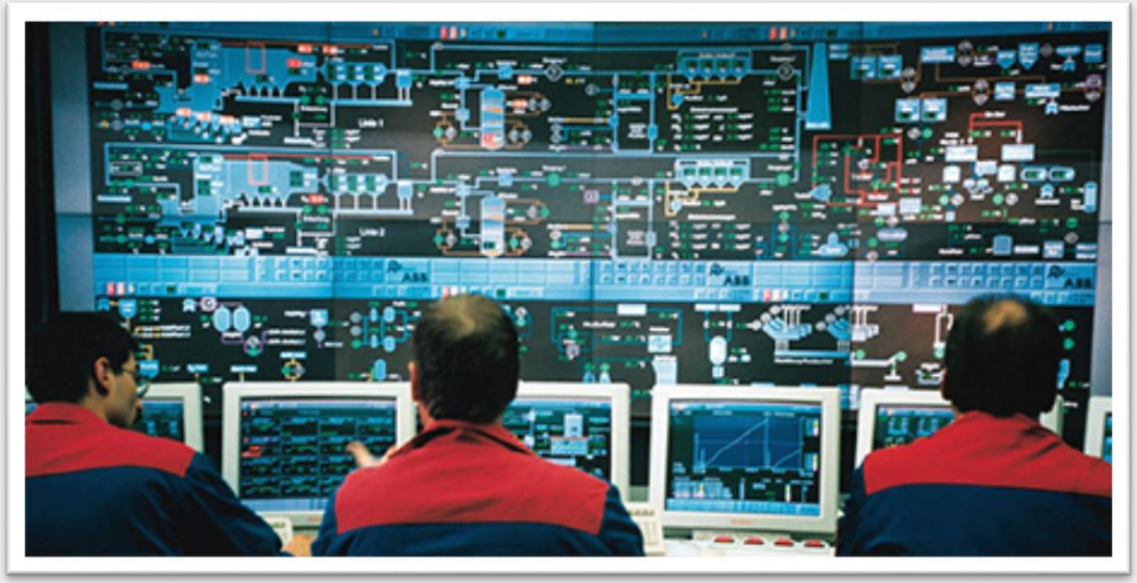
(Structured Threat Information eXpression)

https://oasis-open.github.io/cti-documentation/stix/examples.html

Automated mechanisms like TAXII (Trusted Automated eXchange of Indicator Information).

https://oasis-open.github.io/cti-documentation/taxii/intro.html

Sharing can occur within closed communities, such as Information Sharing and Analysis Centers (ISACs), or through broader industry collaborations.

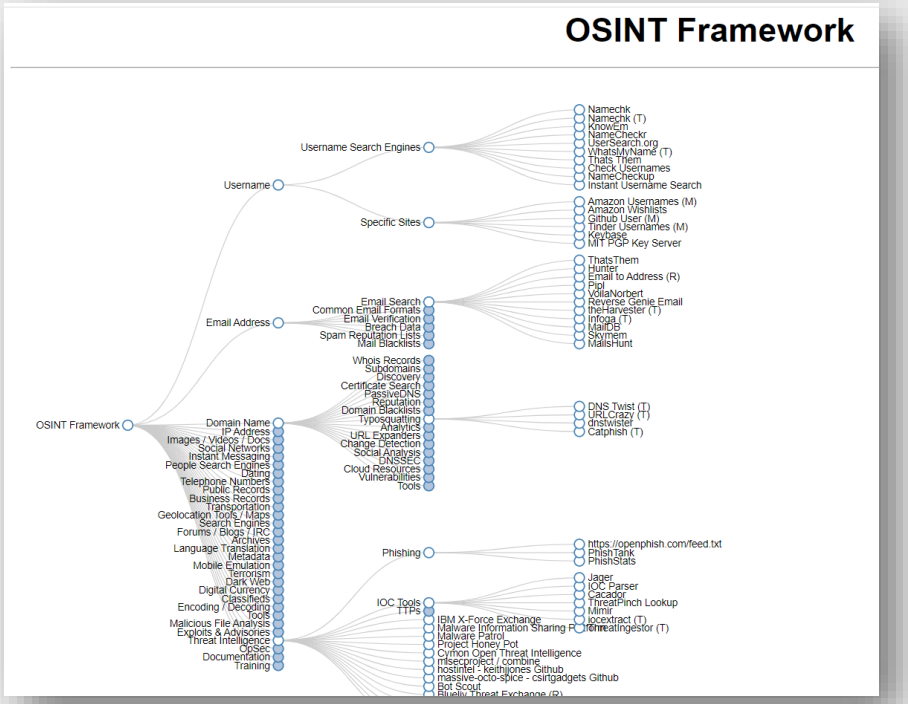


Cyber Security of UK Infrastructure

Microsoft joins Space ISAC as founding member to further space cybersecurity intelligence

Sharing Models and Frameworks

Ensuring that the information is relevant, actionable, and can be effectively utilized by the recipients. Here, we will discuss some commonly used sharing models and frameworks:



1. Trusted Third-Party Sharing:

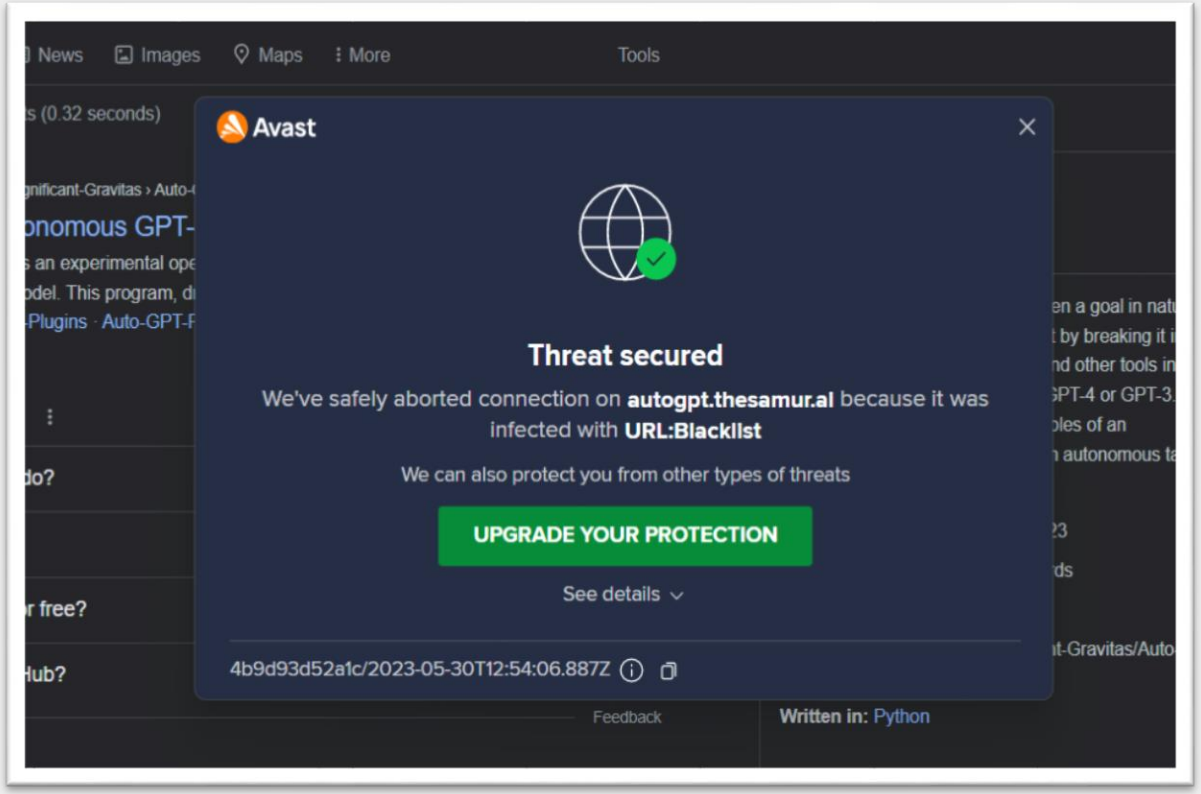
2. Open-Source Intelligence (OSINT) Sharing:

1.Peer-to-Peer Sharing:

- No intermediator involvement
- Quick and direct communication
- Trusted peers
- Critical threat information

https://cti-league.com/services/

Volunteers
COVID 19 pandemic
Saved health records



Anti virus pop ups when it encounters any blacklisted URLs

https://www.recordedfuture.com/

https://www.anomali.com/

https://threatconnect.com/

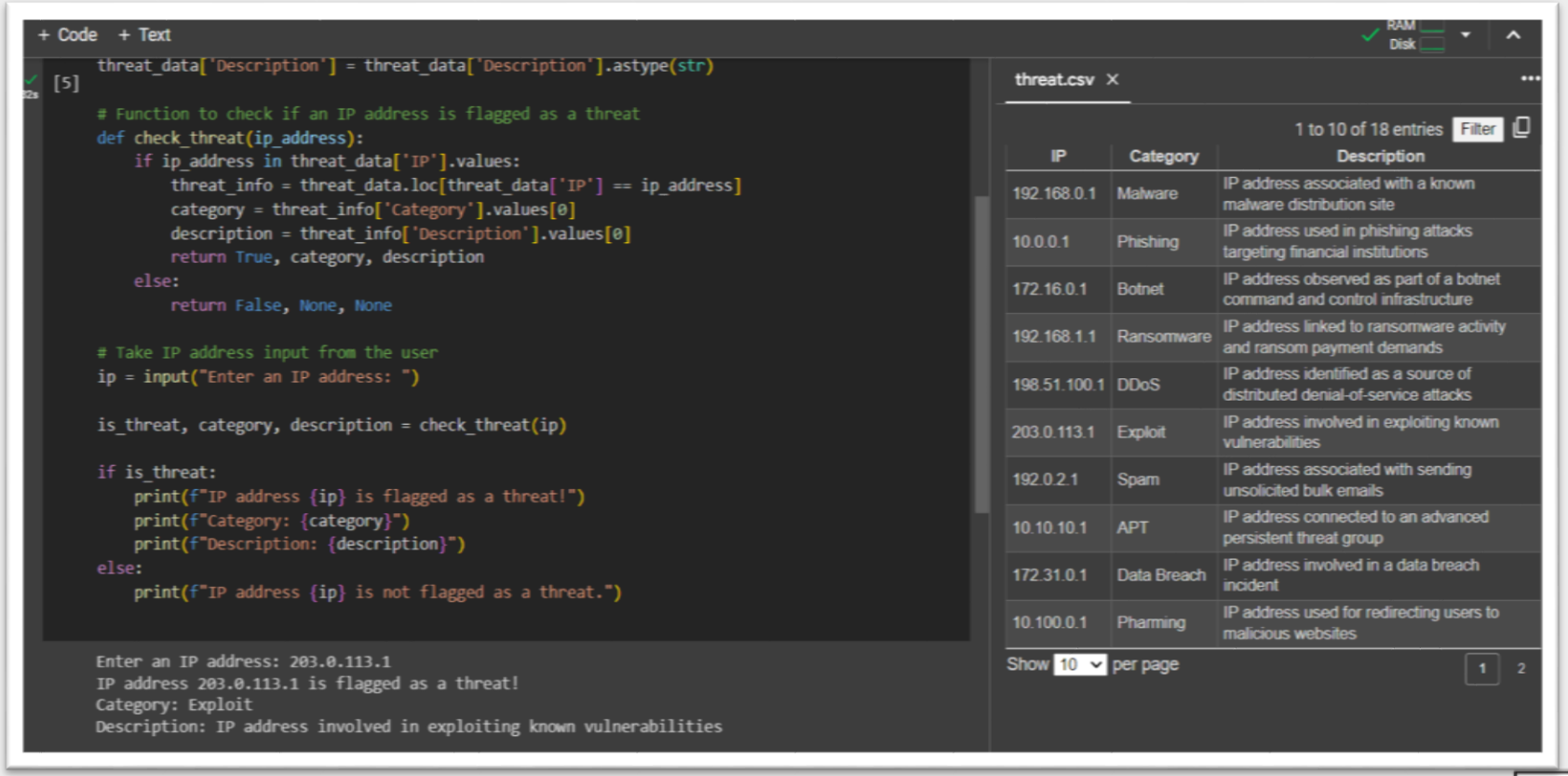
https://otx.alienvault.com/

The World's First Truly Open Threat Intelligence Community

free online service that analyzes files and URLs for potential malware threats. It aggregates data from multiple antivirus engines and other sources to provide comprehensive threat intelligence.

Threat intelligence model using Numpy and pandas

By Tharunaditya Anuganti



```
+ Code  + Text

[5]
threat_data['Description'] = threat_data['Description'].astype(str)

# Function to check if an IP address is flagged as a threat
def check_threat(ip_address):
    if ip_address in threat_data['IP'].values:
        threat_info = threat_data.loc[threat_data['IP'] == ip_address]
        category = threat_info['Category'].values[0]
        description = threat_info['Description'].values[0]
        return True, category, description
    else:
        return False, None, None

# Take IP address input from the user
ip = input("Enter an IP address: ")

is_threat, category, description = check_threat(ip)

if is_threat:
    print(f"IP address {ip} is flagged as a threat!")
    print(f"Category: {category}")
    print(f"Description: {description}")
else:
    print(f"IP address {ip} is not flagged as a threat.")

Enter an IP address: 203.0.113.1
IP address 203.0.113.1 is flagged as a threat!
Category: Exploit
Description: IP address involved in exploiting known vulnerabilities
```

threat.csv

1 to 10 of 18 entries Filter

IP	Category	Description
192.168.0.1	Malware	IP address associated with a known malware distribution site
10.0.0.1	Phishing	IP address used in phishing attacks targeting financial institutions
172.16.0.1	Botnet	IP address observed as part of a botnet command and control infrastructure
192.168.1.1	Ransomware	IP address linked to ransomware activity and ransom payment demands
198.51.100.1	DDoS	IP address identified as a source of distributed denial-of-service attacks
203.0.113.1	Exploit	IP address involved in exploiting known vulnerabilities
192.0.2.1	Spam	IP address associated with sending unsolicited bulk emails
10.10.10.1	APT	IP address connected to an advanced persistent threat group
172.31.0.1	Data Breach	IP address involved in a data breach incident
10.100.0.1	Pharming	IP address used for redirecting users to malicious websites

Show 10 per page 1 2

Executional source code at :

https://colab.research.google.com/drive/1Mn2fwYTEFC2h8zTgv6mTVivtVq3fNmGR?usp=share_link

Threat Intelligence Sharing in a global context

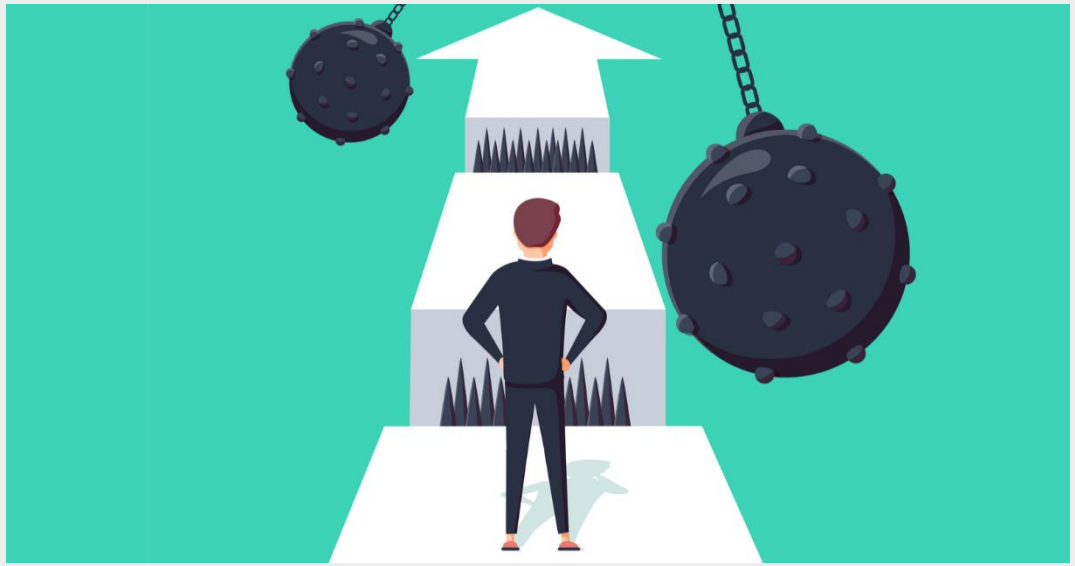
- Exchange: Sharing
- Actionable: Useful, practical
- Information: Insights, intelligence
- Organizations: Companies, entities
- Governments: Public authorities, ruling bodies
- Security communities: Networks, groups
- Early threat detection: Early warning, proactive identification
- Strengthening defenses: Enhancing protection
- Cyber threats: Online risks, malicious activities
- Global scale: Worldwide scope
- Secure: Safe, protected

Best Practices for Effective Threat Intelligence Programs

1. Comprehensive Data Collection
2. Timely and Accurate Analysis
3. Collaboration and Information Sharing
4. Contextualization
5. Automation and Machine Learning
6. Continuous Monitoring and Updating
7. Integration with Security Operations
8. Tailored Reporting and Communication

Addressing Challenges in Threat Intelligence Implementation

1.Data Overload
2.Lack of Context
3.Data Quality and Accuracy
4.Resource Constraints
5.Information Sharing Barriers
6.Skill and Knowledge Gap
7.Continuous Adaptation



Conclusion

In conclusion, threat intelligence plays a vital role in enhancing cyber resilience and mitigating risks in today's evolving threat landscape. By leveraging comprehensive threat intelligence programs, organizations can proactively detect, respond to, and mitigate potential threats. Collaborative sharing, effective implementation, and adherence to best practices are key to achieving a robust and resilient cybersecurity posture in an increasingly interconnected world.

References

R. D. Covey, "Cyber Resilience: The New Paradigm for Managing Cyber Risk," Security Journal, vol. 33, no. 3, pp. 449-464, 2020.

M. B. Cohen, "Threat Intelligence: What It Is, and Why You Need It," RSA Conference, 2018. [Online]. Available:

https://www.rsaconference.com/library/presentation/threat-intelligence-what-it-is-and-why-you-need-it

A. Sharma, "The Role of Threat Intelligence in Risk Management," Cyber Defense Magazine, 2021. [Online]. Available:

https://www.cyberdefensemagazine.com/the-role-of-threat-intelligence-in-risk-management/

Summary of Cyber Threat Intelligence
Adeyemo Oladele David

Huzhou University

https://www.researchgate.net/publication/368281489_Summary_of_Cyber_Threat_Intelligence

Cyber Threat Intelligence in Risk Management

https://thesai.org/Publications/ViewPaper?Volume=12&Issue=10&Code=IJACSA&SerialNo=18

Cyber Threat Intelligence for Improving Cybersecurity and Risk Management Critical Infrastructure

https://repository.uel.ac.uk/item/877y3