



# Threat Intelligence

Threat intelligence is crucial in today's constantly evolving cyber landscape. In this presentation, we'll explore the different sources, tools, and challenges of threat intelligence.

# Sources of Threat Intelligence



## Open Source Intelligence

OSINT provides public information that can be analyzed to detect vulnerabilities and threats



## Internal Data

Internal data can include network traffic, logs, and transactions that provide valuable information for threat threat hunting.



## Human Intelligence

Human intelligence involves gathering gathering information from people or people or communities that are susceptible to cyber threats.



# Analyzing Threat Intelligence

## Data Visualization

Data visualization tools can help help make sense of large, complex data sets.

## Contextual Analysis

Contextual analysis involves examining threat data within the the context of your company's company's unique environment. environment.

## Collaborative Analysis

Threat intelligence analysis shouldn't be done in isolation. isolation. Collaborative analysis analysis can lead to deeper insights and a better understanding of threats.

# Threat Intelligence Tools

## SIEM Tools

Security Information and Event Management (SIEM)  
(SIEM) tools provide real-time analysis of security  
security alerts.

1

## Vulnerability Scanners

Help identify weaknesses in your system before they  
can be exploited.

2

3

## Threat Data Feeds

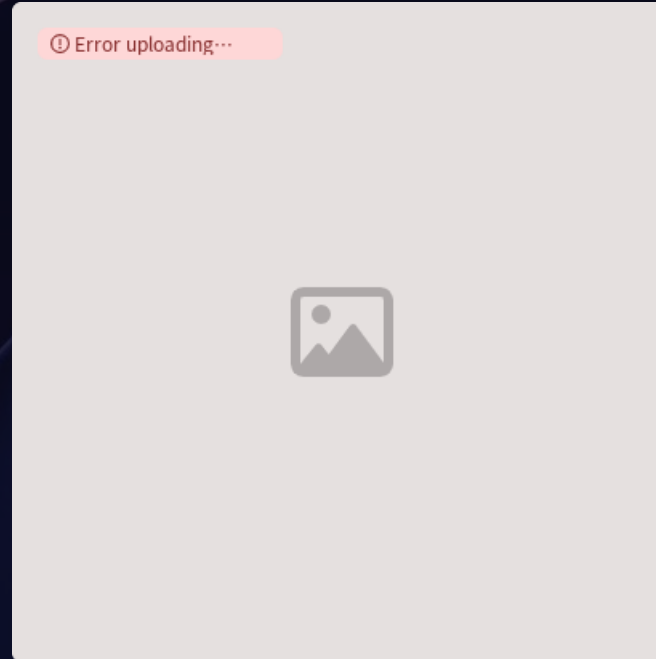
Threat data feeds deliver timely intelligence on active  
active threats and malware.

# Challenges of Threat Intelligence



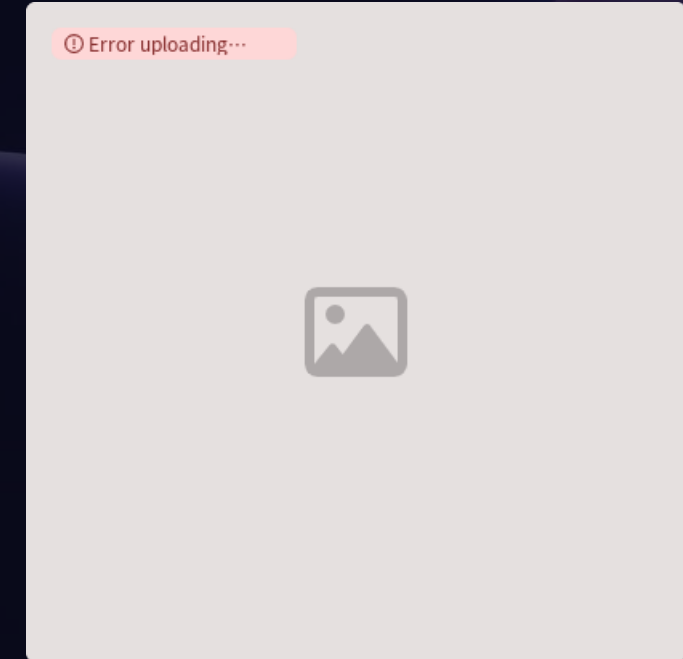
## Quality of Data

Intelligence sources can be unreliable and provide inconsistent information.



## Complexity

The sheer volume of data generated can be overwhelming to analysts and make it difficult to identify critical threats.



## Culture and Management

Effective threat intelligence requires a culture of security and cross-functional communication within an organization, which can be a challenge to establish.

# Benefits of Threat Intelligence

## Early Threat Detection

Threat intelligence can help identify and mitigate security risks before they cause significant damage.

## Enhanced Incident Response

Effective threat intelligence can provide faster and more efficient incident response.

## Better Risk Management

By providing insights into potential threats, threat intelligence can help companies better understand and manage risks.

# Conclusion



## Vigilance

Threat intelligence goes beyond just being reactive to potential threats. By adopting a proactive and vigilant mindset, companies can stay ahead of cyber threats.



## Protection

Threat intelligence can help safeguard company assets and reputation by providing valuable insights that can inform and improve security strategy.



## Preparedness

The right mindset and tools can help organizations be better prepared for any type of cyber attack.