Project Report

Title: - AI – Enhanced Threat Intelligence Platform

Submitted By

NAME OF THE CANDIDATE

Durga Sai Vardhan Reddy Meka (21BCE7399)
Mohan Vemula (21BCE8626)
V Sathvik (21BCE8690)
Gadey Sathwik (21BCE8137)

Abstract

Introduction

In the digital age, cybersecurity is of paramount importance due to the rising sophistication of cyber threats. This abstract explores the emergence of AI-based Threat Intelligence Platforms, which harness the power of artificial intelligence to enhance cybersecurity measures significantly.

The Role of AI in Cybersecurity

Artificial intelligence has revolutionized cybersecurity by enabling the processing of vast data streams in real-time. AI systems excel at detecting patterns and anomalies, providing an advantage in identifying potential threats and vulnerabilities.

Components of an AI-Based Threat Intelligence Platform

An AI-Based Threat Intelligence Platform comprises three primary components:

1. **Data Collection**: These platforms aggregate data from various sources, including network logs, endpoint data, and external threat feeds. The data collected can be both structured and unstructured, offering a comprehensive view of the threat landscape.

2. **Data Analysis:** AI algorithms process this data, applying machine learning techniques to detect patterns, anomalies, and potential threats. They can categorize threats and prioritize them based on their severity.

3. **Threat Assessment:** The platform's output is a real-time threat assessment, which helps security professionals respond swiftly and efficiently to emerging threats.

Benefits of AI-Based Threat Intelligence

The adoption of AI-based threat intelligence platforms brings several advantages:

Faster Threat Detection: AI's ability to process data in real-time leads to quicker threat identification.

Reduced False Positives: Machine learning algorithms reduce false alarms, enabling security teams to focus on genuine threats.

Proactive Threat Mitigation: AI can predict and proactively address potential threats, thus bolstering overall security.

Challenges and Ethical Considerations

Developing AI-based threat intelligence platforms is not without challenges:

Data Privacy: The collection of extensive data raises concerns about privacy and compliance with data protection regulations. **AI Bias**: Ensuring that AI models are trained without bias is crucial to prevent discrimination in threat assessments.

Use Cases and Case Studies

Several organizations have successfully implemented AI-based threat intelligence platforms. For example:

Company X: By implementing an AI-driven threat intelligence platform, Company X managed to prevent a significant cyberattack. The platform's ability to analyze network traffic patterns in real-time helped them thwart the attack. **Organization Y**: Organization Y leveraged machine learning algorithms to reduce false positives, streamlining their incident response process.

Conclusion

AI-Based Threat Intelligence Platforms are integral in today's cybersecurity landscape. They provide an innovative approach to tackling the ever-evolving threat landscape, offering faster detection, reduced false positives, and proactive threat mitigation. Nevertheless, ethical considerations and data privacy concerns must be addressed as these platforms continue to evolve.

The significance of AI in threat intelligence is only expected to grow, emphasizing the need for continued research and development in this field.

Future Scope

The future of AI-enhanced Threat Intelligence Platforms is promising. With the advent of a new era of autonomous threat detection and response, AI is expected to play a pivotal role in collecting, processing, and synthesizing threats, thereby transforming the way organizations combat cyber risks1.

In the next half-decade, the threat intelligence industry is positioned to turn into a high-speed, machine-driven operation1. Autonomous systems are already capable of gathering and processing massive quantities of data from a multitude of sources—from network traffic and log files to dark web forums1. They can churn through this data at speeds and scales that humans could never match, identifying patterns, correlations, and anomalies that hint at potential threats1.

The integration of AI in threat intelligence will drive significant changes across the industry. Analysts' workload will be significantly reduced as AI empowers analysts to focus their expertise on complex threats that require human intervention1. The productivity gains brought about by AI in threat intelligence and security operations are expected to be substantial1.

Analysts will be able to dedicate more time to strategic planning, proactive threat hunting, and developing targeted mitigation strategies1. This shift from reactive to proactive security practices will enable organizations to stay ahead of rapidly evolving cyber threats1. Furthermore, the advent of AI in threat intelligence will redefine the roles and responsibilities of the security operations center (SOC) Level 1 team1.

TITTLE :
AI ENHANCED THREAT INTELLIGENCE PLATFORM

OVERVIEW:

An AI-enhanced threat intelligence platform is a cybersecurity solution that uses artificial intelligence (AI) to automate and augment the process of collecting, analyzing, and disseminating threat intelligence. This type of platform can help organizations to improve their security posture by providing them with a more comprehensive and timely understanding of the threats they face.

AI-enhanced threat intelligence platforms typically include the following key features:
Automated data collection and analysis: The platform can automatically collect threat intelligence data from a variety of sources, including public and private feeds, social media, and the dark web. It can then use AI to analyze this data to identify patterns and trends, and to correlate it with existing threat intelligence data.
Threat prioritization: The platform can use AI to prioritize threats based on their severity, likelihood, and potential impact to the organization. This helps organizations to focus their resources on the most important threats.
Actionable insights: The platform can provide organizations with actionable insights into how to mitigate the threats they face. This may include recommendations on how to patch vulnerabilities, block malicious IP addresses, or educate employees about phishing attacks.

AI-enhanced threat intelligence platforms can provide organizations with a number of benefits, including:

Improved security posture: By providing organizations with a more comprehensive and timely understanding of the threats they face, AI-enhanced threat intelligence platforms can help them to improve their security posture and reduce the risk of being compromised.

Reduced workload for security teams: AI-enhanced threat intelligence platforms can automate many of the tasks involved in threat intelligence, freeing up security teams to focus on more strategic initiatives.

Improved collaboration: AI-enhanced threat intelligence platforms can help organizations to collaborate more effectively with other organizations and security vendors. This can be done by sharing threat intelligence data and insights.

TEAMMATES:

SNO	NAME	COLLAGE	CONTACT
1.	M.DURGA SAI VARDHAN REDDY	VELLORE INSTITUTE OF TECHNOLOGY (VITAP)	vardhan.21bce7399 @vitapstudent.ac.in
2.	GADEY SATHWIK	VELLORE INSTITUTE OF TECHNOLOGY (VITAP)	sathwik.21bce8137 @vitapstudent.ac.in
3.	V.V.RAM MOHAN	VELLORE INSTITUTE OF TECHNOLOGY (VITAP)	ram.21bce8626@vitapstudent.ac.in
4.	V.SATHVIK	VELLORE INSTITUTE OF TECHNOLOGY (VITAP)	sathvik.21bce8690 @vitapstudent.ac.in

List of Vulnerabilities:

SNO	VULNERABILITY NAME	CWE NO
1.	TLS Version 1.0 Protocol Detection	Cwe 326
2.	TLS Version 1.1 Protocol Deprecated	Cwe 326
3.	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Cwe 327
4.	ICMP Timestamp Request Remote Date Disclosure	Cwe 200
5.	Additional DNS Hostnames	Cwe 350
6.	Apache Tomcat Detection	Cwe 200
7.	HSTS Missing From HTTPS Server	Cwe 523
8.	SSL Cipher Suites Supported	Cwe 326
9.	OS Identification	Cwe 209
10.	SSL Root Certification Authority Certificate Information	Cwe 295

REPORT

1. Vulnerability Name:- TLS Version 1.0 Protocol Detection

   CWE : - Cwe 326

   OWASP Category:- TLS 1.0 protocol detection can be attributed to two categories from OWASP Top Ten 2017:
   A3: Sensitive Data Exposure
   A6: Security Misconfiguration

   Description:- TLS Version 1.0 Protocol Detection is the process of identifying whether or not a server or client is supporting TLS Version 1.0.
   This can be done using a variety of methods, such as:
   - Sending a TLS handshake request
   - Analyzing network traffic
   - Checking server configuration

   Business Impact:- Organizations that continue to use TLS Version 1.0 are at risk of a number of security incidents, including:
   - Data breaches
   - Malware infections
   - Denial-of-service attacks

2.

Vulnerability Name:- TLS Version 1.1 Protocol Deprecated

CWE : - Cwe 326

OWASP Category:- TLS Version 1.1 is deprecated and is included in the OWASP Top 10 under

- A5 Security Misconfiguration category.

Description:- TLS Version 1.1 Protocol Deprecated means that TLS Version 1.1 is no longer considered secure and should not be used. It is vulnerable to a number of security vulnerabilities, including:

- POODLE (Padding Oracle On Downgraded Legacy Encryption).
- FREAK (Factoring RSA Export Keys)
- DROWN (Decrypting RSA with Obsolete and Weakened Encryption)

Business Impact:- The business impact of TLS Version 1.1 protocol deprecation can be significant. Organizations that continue to use TLS Version 1.1 are at risk of a number of security incidents, compliance violations, and business disruptions.

- Intercept and decrypt
- traffic Impersonate legitimate servers
- Inject malware into applications

3.

Vulnerability Name:- SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

CWE : - Cwe 327

OWASP Category:- SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) is a vulnerability in cryptography that affects infrastructure. It is categorized as CWE-327: Use of a Broken or Risky Cryptographic Algorithm and is identified

- A8 Insecure Cryptographic Storage

Description:- The LOGJAM attack is a SSL/TLS vulnerability that allows attackers to intercept HTTPS connections between vulnerable clients and servers and force them to use 'export-grade' cryptography, which can then be decrypted or altered.

Business Impact:- This vulnerability occurs when an organization uses a Diffie-Hellman key exchange with a modulus less than or equal to 1024 bits. It can be exploited by an attacker to downgrade the security of TLS connections and enable man-in-the-middle (MITM) attacks. Allows an attacker to weaken the encryption complexity, consequently decrypting data easily without the user's knowledge

4.

Vulnerability Name:- ICMP Timestamp Request Remote Date Disclosure

CWE : - Cwe 200

OWASP Category:- ICMP Timestamp Request Remote Date Disclosure is not included in the OWASP Top 10. It is a vulnerability that allows an attacker to determine the date and time of a remote system by sending an ICMP Timestamp Request packet.

Description:- The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Business Impact:- Organizations that are vulnerable to this attack could experience a number of negative consequences, including:

- Data breaches
- Disruptions to operations
- Damage to reputation
- Regulatory compliance violations

5.

Vulnerability Name:- Additional DNS Hostnames

CWE : - Cwe 350

OWASP Category:- Additional DNS Hostnames is not included in the OWASP Top 10. It is a vulnerability that allows an attacker to discover additional DNS hostnames associated with a target system.

Description:- Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server. Different web servers may be hosted on name-based virtual hosts.

Business Impact:- Organizations that are vulnerable to this attack could experience a number of negative consequences, including:

- Phishing attacks
- Denial-of-service attack
- Data breaches
- Loss of customer trust
- Regulatory compliance violations

6.

Vulnerability Name:- Apache Tomcat Detection

CWE : - Cwe 200

OWASP Category:- OWASP includes Apache Tomcat Detection in its

- A5 Security Misconfiguration category.

Description:- Apache Tomcat Detection is the process of identifying and tracking Apache Tomcat instances on a network. This can be done using a variety of methods, including:

- Network scanning
- Log analysis
- Web application firewall (WAF) inspection

Business Impact:- The business impact of not detecting Apache Tomcat instances:

- Increased risk of cyberattacks
- Reduced security posture
- Increased compliance risk
- Reduced visibility into the network
- Difficulty in managing and securing Apache Tomcat instances

7.

Vulnerability Name:- HSTS Missing From HTTPS Server

CWE : - Cwe 523

OWASP Category:- HSTS Missing From HTTPS Server is included in the OWASP Top 10 under the

- A5 Security Misconfiguration category.

Description:- HSTS Missing From HTTPS Server describes a security vulnerability that occurs when an HTTPS server does not have the HSTS (HTTP Strict Transport Security) header set. This means that browsers will not be forced to use a secure HTTPS connection when communicating with the server, which could leave users vulnerable to man-in-the-middle attacks.Man-in-the-middle attacks occur when an attacker intercepts traffic between two parties and impersonates one of the parties.

Business Impact:- Organizations that do not configure HSTS are at risk of a number of negative consequences, including:

- Security breaches
- Compliance violations
- Damage to reputation
- Loss of customer trust

8.

Vulnerability Name:- SSL Cipher Suites Supported

CWE : - Cwe 326

OWASP Category:- SSL Cipher Suites Supported is included in the OWASP Top 10 under

- A6 Sensitive Data Exposure category.

Description:- SSL Cipher Suites Supported is a security vulnerability that occurs when an organization supports insecure cipher suites for its SSL/TLS connections. SSL/TLS is a cryptographic protocol that provides secure communication over a computer network. It is used to protect data in transit between two applications, such as a web browser and a web server. SSL/TLS uses a variety of cryptographic algorithms to encrypt and decrypt data. The algorithms that are used are specified in a cipher suite. A cipher suite is a set of algorithms that are used together to provide a certain level of security.

Business Impact:- Organizations that support insecure cipher suites are at risk of a number of negative consequences, including:

- Data breaches
- Compliance violations
- Damage to reputation
- Loss of customer trust

9.

Vulnerability Name:- OS Identification

CWE : - Cwe 209

OWASP Category:- OS Identification is included in the OWASP Top 10 under

- A5 Security Misconfiguration category.

Description:- OS Identification is a security vulnerability that allows an attacker to determine the operating system (OS) that a web application is running on. This information can then be used to launch targeted attacks against the web application. Attackers can exploit the OS Identification vulnerability in a number of ways, including:

- Exploiting known vulnerabilities in specific OS versions
- Launching denial-of-service (DoS) attacks
- Social engineering attacks

Business Impact:- Organizations that are vulnerable to this attack could experience a number of negative consequences, including:

- Data Breaches
- Disruptions to Operations
- Compliance Violations
- Loss of Customer Trust

10.

Vulnerability Name:- SSL Root Certification Authority Certificate Information

CWE : - Cwe 295

OWASP Category:- SSL Root Certification Authority Certificate Information is included in the OWASP Top 10 under

- A7: Identification and Authentication Failures

Description:- SSL Root Certification Authority Certificate Information is a security vulnerability that allows attackers to obtain the root certification authority (CA) certificate of a web application. This certificate can then be used to create fraudulent certificates that can be used to impersonate the web application. Root CA certificates are trusted by all major browsers and operating systems. When a browser visits a website, it checks the website's certificate against its list of trusted root CA certificates.

Business Impact:- Organizations that are vulnerable to this attack could experience a number of negative consequences, including:

- Data Breaches
- Disruptions to Operations
- Compliance Violations
- Loss of Customer Trust

This is stage 1 where we understand web application testing in

testfire.net

we took help from OWASP top 10 understand them.

STAGE 2

ABOUT NESSUS

Nessus is a vulnerability scanner that helps organizations identify and assess security vulnerabilities in their networks and systems. It is one of the most popular vulnerability scanners in the world, and is used by a wide range of organizations, including government agencies, Fortune 500 companies, and small businesses.

Nessus works by scanning networks and systems for known vulnerabilities. It uses a variety of techniques to do this, including:

- Network scanning: Nessus scans networks to identify all of the devices that are connected to the network. It then collects information about each device, such as its operating system, version, and open ports.
- Vulnerability assessment: Nessus uses a variety of methods to assess vulnerabilities on the devices that it scans. It uses a database of known vulnerabilities to identify potential vulnerabilities, and then performs tests to confirm whether or not the vulnerabilities are present.
- Risk assessment: Nessus assesses the risk of each vulnerability that it finds. It takes into account factors such as the exploitability of the vulnerability, the potential impact of the vulnerability, and the likelihood that the vulnerability will be exploited.

Nessus provides a variety of reports that can be used to assess the security of networks and systems. These reports include:

- Vulnerability report: The vulnerability report lists all of the vulnerabilities that have been found, along with their severity and risk.
- Executive summary: The executive summary provides a high-level overview of the security of the network or system, and highlights the most critical vulnerabilities.
- Remediation report: The remediation report provides recommendations on how to fix the vulnerabilities that have been found.

Nessus is a powerful tool that can help organizations to improve the security of their networks and systems. It is easy to use and provides a variety of features that make it a valuable tool for security professionals.

Here are some of the benefits of using Nessus:

- Comprehensive vulnerability coverage: Nessus scans for a wide range of vulnerabilities, including network vulnerabilities, application vulnerabilities, and configuration vulnerabilities.
- Accurate results: Nessus uses a variety of techniques to assess vulnerabilities, and its results are highly accurate.
- Easy to use: Nessus is easy to set up and use, even for users with no prior experience with vulnerability scanning.

- Powerful reporting: Nessus provides a variety of reports that can be used to assess the security of networks and systems, and to identify and prioritize remediation activities.

Nessus is a valuable tool for any organization that is serious about improving the security of its networks and systems.

TARGET WEBSITE :

https://yugenanime.tv

TARGET IP ADDRESS :

172.67.219.135

LIST OF VULNERABILITIES

SNO	VULNERABILITY NAME	SEVERITY	PLUGINS
1.	Nessus Scan Information	none	Published:2005/08/26, Modified: 2023/07/31
2.	Common Platform Enumeration (CPE)	none	Published:2010/04/21, Modified: 2023/10/16
3.	Device Type	none	Published:2011/05/23, Modified: 2022/09/09
4.	HTTP Server Type and Version	none	Published:2000/01/04, Modified: 2020/10/30
5.	HyperText Transfer Protocol (HTTP) Information	none	Published:2007/01/30, Modified: 2019/11/22
6.	Nessus SYN scanner	none	Published:2009/02/04, Modified: 2023/09/25
7.	OS Identification	none	Published:2003/12/09, Modified: 2022/03/09
8.	Service Detection	none	Published:2007/08/19, Modified: 2023/07/10
9.	TCP/IP Timestamps Supported	none	Published:2007/05/16, Modified: 2019/03/06
10.	Traceroute Information	none	Published:1999/11/27, Modified: 2023/06/26

1.

Vulnerability Name:- Nessus Scan Information

Severity : - none

Synopsis :- This plugin displays information about the Nessus scan.

Plugin:- Published: 2005/08/26, Modified: 2023/07/31
tcp/0

Port :- TCP 8834

Description:- This plugin displays, for each tested host, information about the scan itself

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.

solution:- n/a

Business Impact:- Applications may crash because of the service detection that is performed on open ports

2.

Vulnerability Name:- Common Platform Enumeration (CPE)

severity : - none

Synopsis :- It was possible to enumerate CPE names that matched on the remote system.

Plugin:- Published: 2010/04/21, Modified: 2023/10/16
tcp/0

Port :- 3307

Description:- By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

solution:- n/a

Business Impact:- CPE is a standardized way for enterprises to describe and identify classes of applications, operating systems, and hardware. CPE also helps in Making Security Measurable.

3.

Vulnerability Name:- Device Type

severity : - none

Synopsis :- It is possible to guess the remote device type

Plugin:- Published: 2011/05/23, Modified: 2022/09/09
tcp/0

Port :- 3306

Description:- Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

solution:- n/a

Business Impact:- Organizations that do not have this information may be at risk of a number of negative consequences, including:

- Security breaches
- Compliance violations
- Performance issues

4.

Vulnerability Name:- HTTP Server Type and Version

severity : - none

Synopsis :- A web server is running on the remote host.

Plugin:- Published: 2000/01/04, Modified: 2020/10/30
tcp/80/www

Port :- 80

Description:- This plugin attempts to determine the type and the version of the remote web server.

solution:- n/a

Business Impact:- Organizations that do not have this information may be at risk of a number of negative consequences, including:

- Security breaches
- Compliance violations
- Performance issues

5.

Vulnerability Name:- HyperText Transfer Protocol (HTTP) Information

severity : - none

Synopsis :- Some information about the remote HTTP configuration can be extracted.

Plugin:- Published: 2007/01/30, Modified: 2019/11/22
tcp/443/www

Port :- 80

Description:- This test gives some information about the remote HTTP protocol - the version used, whether HTTP KeepAlive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem.

solution:- n/a

Business Impact:- Organizations that do not have this information may be at risk of a number of negative consequences, including:

- Security breaches
- Compliance violations
- Performance issues
- Business disruption

6.

Vulnerability Name:- Nessus SYN scanner

severity : - none

Synopsis :- It is possible to determine which TCP ports are open.

Plugin:- Published: 2009/02/04, Modified: 2023/09/25
tcp/2052/www

Port :- 443

Description:- This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

solution:- n/a

Business Impact:- Organizations that do not have this information may be at risk of a number of negative consequences, including:

- Security breaches
- Compliance violations
- Financial losses

7.
Vulnerability Name:- OS Identification

severity : - none

Synopsis :- It is possible to guess the remote operating system.

Plugin:- Published: 2003/12/09, Modified: 2022/03/09
tcp/0

Port :- 22

Description:- Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

solution:- n/a

Business Impact:- Organizations that do not have this information may be at risk of a number of negative consequences, including:

- Security breaches
- Compliance violations
- Performance issues
- Business disruption

8.

Vulnerability Name:- Service Detection

severity : - none

Synopsis :- The remote service could be identified.

Plugin:- Published: 2007/08/19, Modified: 2023/07/10
tcp/2082/www

Port :- 21

Description:- Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

solution:- n/a

Business Impact:- Organizations that do not have this information may be at risk of a number of negative consequences, including:

- Security breaches
- Compliance violations
- Financial losses
- Damage to reputation

9.

Vulnerability Name:- TCP/IP Timestamps Supported

severity : - none

Synopsis :- The remote service implements TCP timestamps.

Plugin:- Published: 2007/05/16, Modified: 2019/03/06
tcp/0

Port :- 53

Description:- The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

solution:- n/a

Business Impact:- A successful attack can result in a variety of negative consequences, including:

- Data breaches
- Financial losses
- Damage to reputation
- Loss of customer trust

10.

Vulnerability Name:- Traceroute Information

severity : - none

Synopsis :- It was possible to obtain traceroute information.

Plugin:- Published: 1999/11/27, Modified: 2023/06/26
udp/0

Port :- UDP port 33434, TCP port 80 ,ICMP port 7

Description:- Makes a traceroute to the remote host.

solution:- n/a

Business Impact:- Organizations that cannot use Traceroute may be at risk of a number of negative consequences, including:

- Difficulty troubleshooting network problems
- Inability to investigate security incidents
- Compliance violations

Stage3

Report Title: AI-Based Threat Intelligence Platforms

Introduction

Threat intelligence is a critical component of any cybersecurity program. It helps organizations to identify, understand, and mitigate threats. Traditional threat intelligence platforms rely on human analysts to collect and analyze data. However, the volume and complexity of threats is growing rapidly, making it difficult for human analysts to keep up.

AI-based threat intelligence platforms use artificial intelligence (AI) to automate the collection and analysis of threat data. This allows them to provide more comprehensive and up-to-date threat intelligence than traditional platforms.

Benefits of AI-Based Threat Intelligence Platforms

There are a number of benefits to using an AI-based threat intelligence platform, including:

Increased efficiency: AI-based threat intelligence platforms can automate the collection and analysis of threat data, freeing up human analysts to focus on other tasks.
Improved accuracy: AI-based threat intelligence platforms can use machine learning to identify threats that would be missed by human analysts.
Reduced costs:AI-based threat intelligence platforms can be more cost-effective than traditional platforms, as they do not require as much human input.

Use Cases for AI-Based Threat Intelligence Platforms

AI-based threat intelligence platforms can be used for a variety of purposes, including:

Identifying new threats: AI-based threat intelligence platforms can use machine learning to identify new threats that are not yet known to human analysts.
Tracking threat activity: AI-based threat intelligence platforms can track the activity of known threats, helping organizations to understand how they are evolving and spreading.
* **Mitigating threats:** AI-based threat intelligence platforms can help organizations to mitigate threats by providing them with actionable intelligence.

Conclusion

AI-based threat intelligence platforms are a valuable tool for organizations that want to improve their cybersecurity posture. They can provide more comprehensive, up-to-date, and accurate threat intelligence than traditional platforms. This can help organizations to identify, understand, and mitigate threats more effectively.

Stage 1: What is Web Application Testing?

Web application testing is a type of security testing that focuses on identifying vulnerabilities in web applications. These vulnerabilities can be exploited by attackers to gain unauthorized access to data, steal sensitive information, or disrupt the operation of the application.

Web application testing can be performed manually or with the help of automated tools. Manual testing involves a security tester manually testing the application for vulnerabilities. Automated testing involves using a tool to scan the application for vulnerabilities.

Stage 2: What is a Nessus Report?

A Nessus report is a report generated by the Nessus vulnerability scanner. The report lists the vulnerabilities that the scanner has found in the target system. The report can be used to identify and prioritize vulnerabilities that need to be addressed.

Stage 3: What is a SOC/SEIM/QRadar Dashboard?

A SOC/SEIM/QRadar dashboard is a graphical user interface (GUI) that provides a centralized view of security information and events. The dashboard can be used to monitor the security of an organization's network and systems.

Future Scope of AI-Based Threat Intelligence Platforms

The future scope of AI-based threat intelligence platforms is bright. As the volume and complexity of threats continues to grow, AI-based platforms will become increasingly important for organizations that want to stay ahead of the curve.

Some of the future trends in AI-based threat intelligence platforms include:

Increased use of machine learning: Machine learning will be used to identify new threats, track threat activity, and mitigate threats.

Improved integration with other security tools:AI-based threat intelligence platforms will be integrated with other security tools, such as firewalls and intrusion detection systems, to provide a more comprehensive view of the security landscape.
Increased use of cloud-based platforms: AI-based threat intelligence platforms will be increasingly deployed in the cloud, making them more accessible and affordable for organizations of all sizes.

Conclusion

AI-based threat intelligence platforms are a valuable tool for organizations that want to improve their cybersecurity posture. They can provide more comprehensive, up-to-date, and accurate threat intelligence than traditional platforms. This can help organizations to identify, understand, and mitigate threats more effectively.