

AI-DRIVEN SECURITY AND THREAT DETECTION USING SENTINEL

-Bhavya Agarwal



What is the problem?



- Organizations are bombarded with cyber threats daily.
- Traditional security tools struggle to keep up with the scale and sophistication of modern attacks. They work in silos, making it hard to detect coordinated attacks.
- Organizations need an AI-powered solution that provides a holistic security view.

Microsoft Sentinel



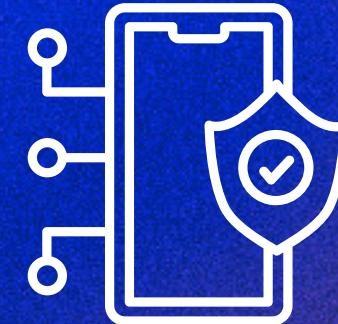
SIEM (Security Information and Event Management) & **SOAR** (Security Orchestration, Automation, and Response) solution.



One-stop security solution for all your resources: VMs, databases, cloud applications, networks, and more.



MITRE ATT&CK framework to visualize the nature and coverage of your organization's security status based on the tactics and techniques.



Microsoft's threat intelligence stream to detect malicious activity in your environment and provide context to security investigators for informed response decisions.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

bhavyagarwa@umass...
EFFECTIVE AZURE DIRECTORY

Home > Microsoft Sentinel

Microsoft Sentinel | MITRE ATT&CK (Preview) ...

Selected workspace: 'effaz-global-log'

Search Search by technique ID... Matrices type view : 13 selected Coverage level : All Active rules 3 selected Simulated rules Select options

> General

<< Legend None Low Medium High

<<

> Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)**
- SOC optimization

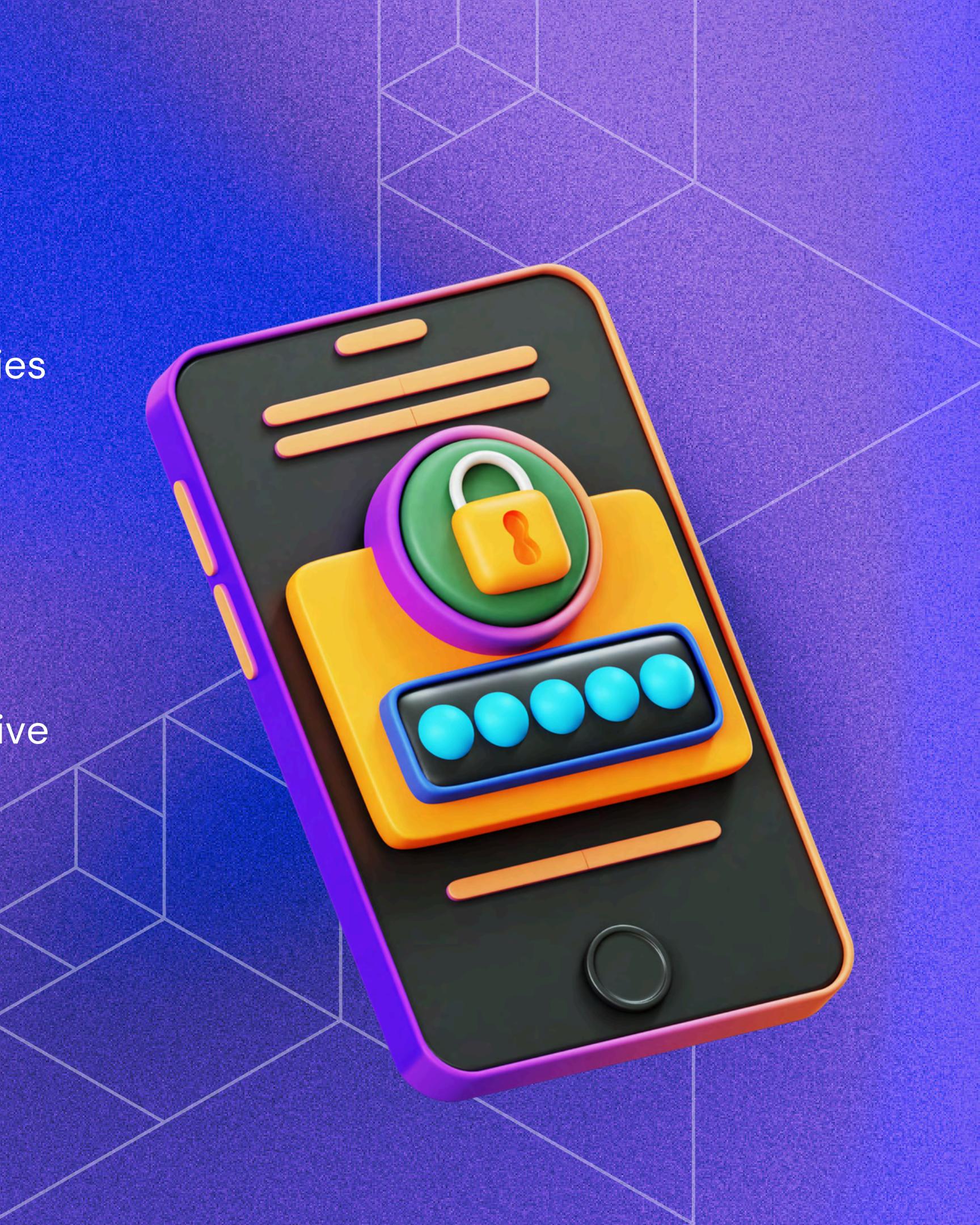
> Content management

> Configuration

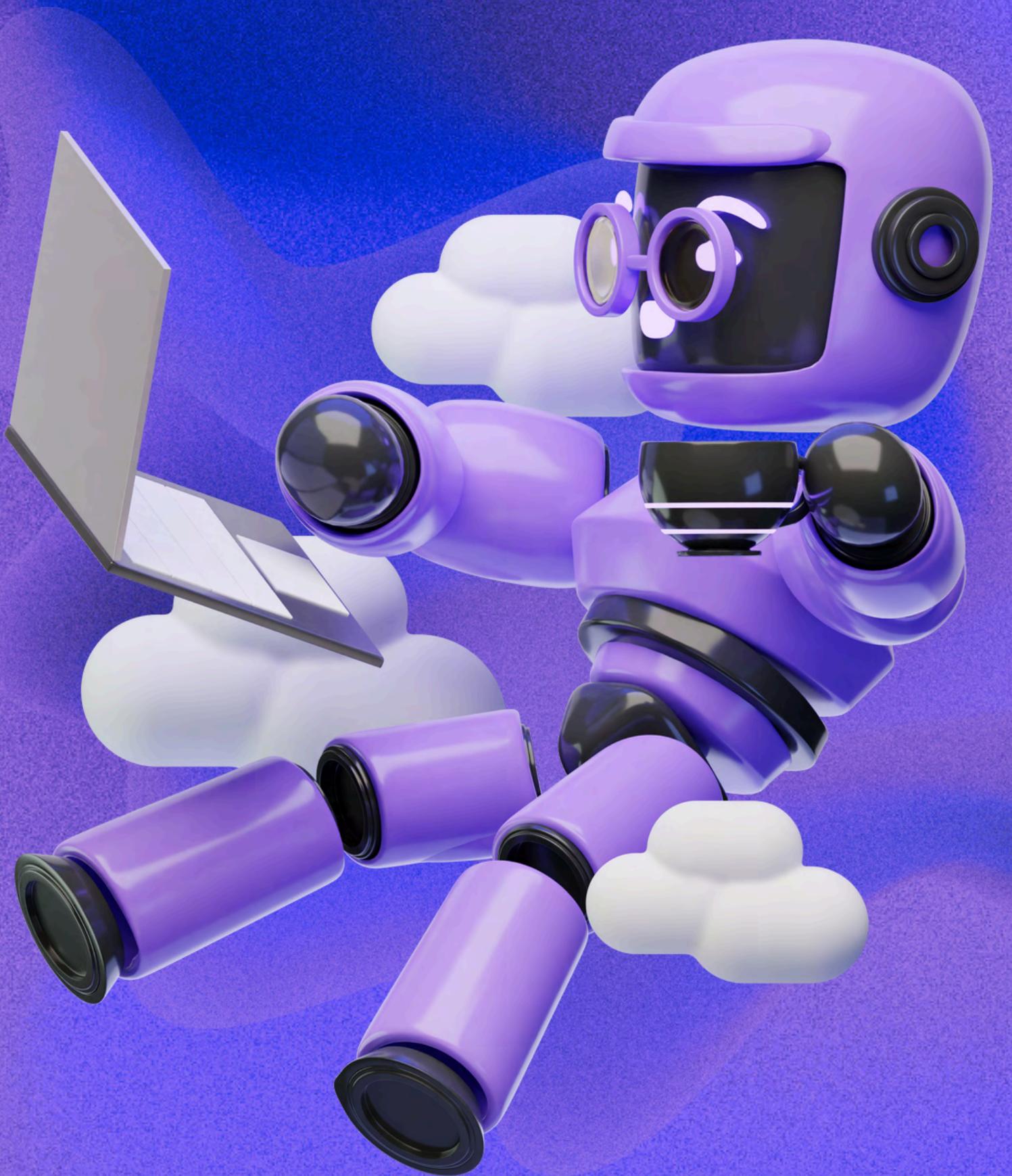
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques
Active Scanning	Acquire Access	Drive-by Compromise	1 Command and Scripting...	3 Account Manipulation	Abuse Elevation Control...	Abuse Elevation Control...	Man-in-the-Middle	1 Account Discovery	Exploitation of Remote Services	Man-in-the-Middle
Gather Victim Host...	Acquire Infrastructure	3 Exploit Public-Facing...	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	11 Brute Force	Application Window...	Internal Spearphishing	Archive Collected Data
Gather Victim Identity...	Compromise Accounts	External Remote Services	Inter-Process Communication	Boot or Logon Autostart...	Boot or Logon Autostart...	BITS Jobs	Credentials from Password Stores	Browser Bookmark...	Lateral Tool Transfer	Audio Capture
Gather Victim Network...	Compromise Infrastructure	Hardware Additions	Native API	Boot or Logon Initialization...	Boot or Logon Initialization...	Debugger Evasion	Exploitation for Credential...	Debugger Evasion	Remote Service Session...	Automated Collection
Gather Victim Org Information	Develop Capabilities	Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System...	Deobfuscate/Decode Files or...	Forced Authentication	Device Driver Discovery	Remote Services	Man in the Browser

UEBA

- **User and Entity Behavior Analytics** (UEBA) detects anomalies in user and machine behavior.
- Instead of relying on predefined rules, UEBA learns patterns over time using **machine learning** and flags suspicious activities.
- Identifies insider threats (e.g., an employee accessing sensitive data at odd hours), detects compromised accounts (e.g., a legitimate account suddenly logging in from a different country), analyzes peer behavior (e.g., comparing a user's actions to their typical patterns).



How UEBA Works in Sentinel



- Sentinel leverages UEBA to enhance security analytics by identifying anomalies that traditional rule-based systems might miss.
- It correlates activity across users, devices, and applications to detect sophisticated attack patterns.
- Provides risk-based alerts, and works alongside threat intelligence and machine learning models to improve detection accuracy and response time.
- Article- <https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics>

Scenario #1 – Threat Simulation (TOR & Failed Login Attempt)

- **Scenario:** A hacker tries to brute-force their way into a VM using TOR.
- **What Happens in Sentinel?**
 - Sentinel detects multiple failed login attempts from a suspicious IP.
 - AI identifies the attacker's behavior as anomalous.
 - Sentinel raises an alert, linking it with other attack signals.



Scenario #2 – Threat Simulation (Password Theft & Mimikatz Attack)



- **Scenario:** An attacker steals the VM password using Tor and Microsoft Key Vault and downloads Mimikatz on it.
- **What Happens in Sentinel?**
 - Detects unusual authentication activity (e.g., logging in from an unfamiliar device).
 - Flags the download of Mimikatz, a known hacking tool.
 - It classifies the risk (high risk) based on severity, confidence, and correlation with other threats.



Compose

Mail



Inbox

6,196



Starred



Snoozed



Sent



Drafts

More

Labels

**From:** Microsoft Azure <azure-noreply@microsoft.com>**Sent:** Thursday, March 20, 2025 9:51:50 AM**To:** Bill Wilder <bill@semantickernel.dev>**Subject:** User at risk detected

User at risk detected

We detected a new user with at least high risk in your Effective Azure Directory directory. This might be because we noticed suspicious account activity or we found their emails and passwords posted in a public location.

[View detailed report >](#)[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



3 of many





Compose



2 of many < >

Subject: Fw: Microsoft Defender for Cloud has detected suspicious activity in your environment **Inbox** 6,196 **Starred** **Snoozed** **Sent** **Drafts** **More****Labels****From:** Microsoft Defender for Cloud <DefenderCloudnoreply@microsoft.com>**Sent:** Thursday, March 20, 2025 10:14:42 PM**To:** Bill Wilder <bill@semantickernel.dev>**Subject:** Microsoft Defender for Cloud has detected suspicious activity in your environment**HIGH SEVERITY**

Microsoft Defender for Cloud has detected suspicious activity in your resource



Mimikatz credential theft tool was detected (Agentless)

The Mimikatz hacktool was detected on this device. Mimikatz is a credential theft tool that can harvest plaintext passwords, password hashes, smartcard PINs, and Kerberos tickets. An attacker might be trying to harvest credentials to log into this or other devices on the network, by impersonating a valid user.

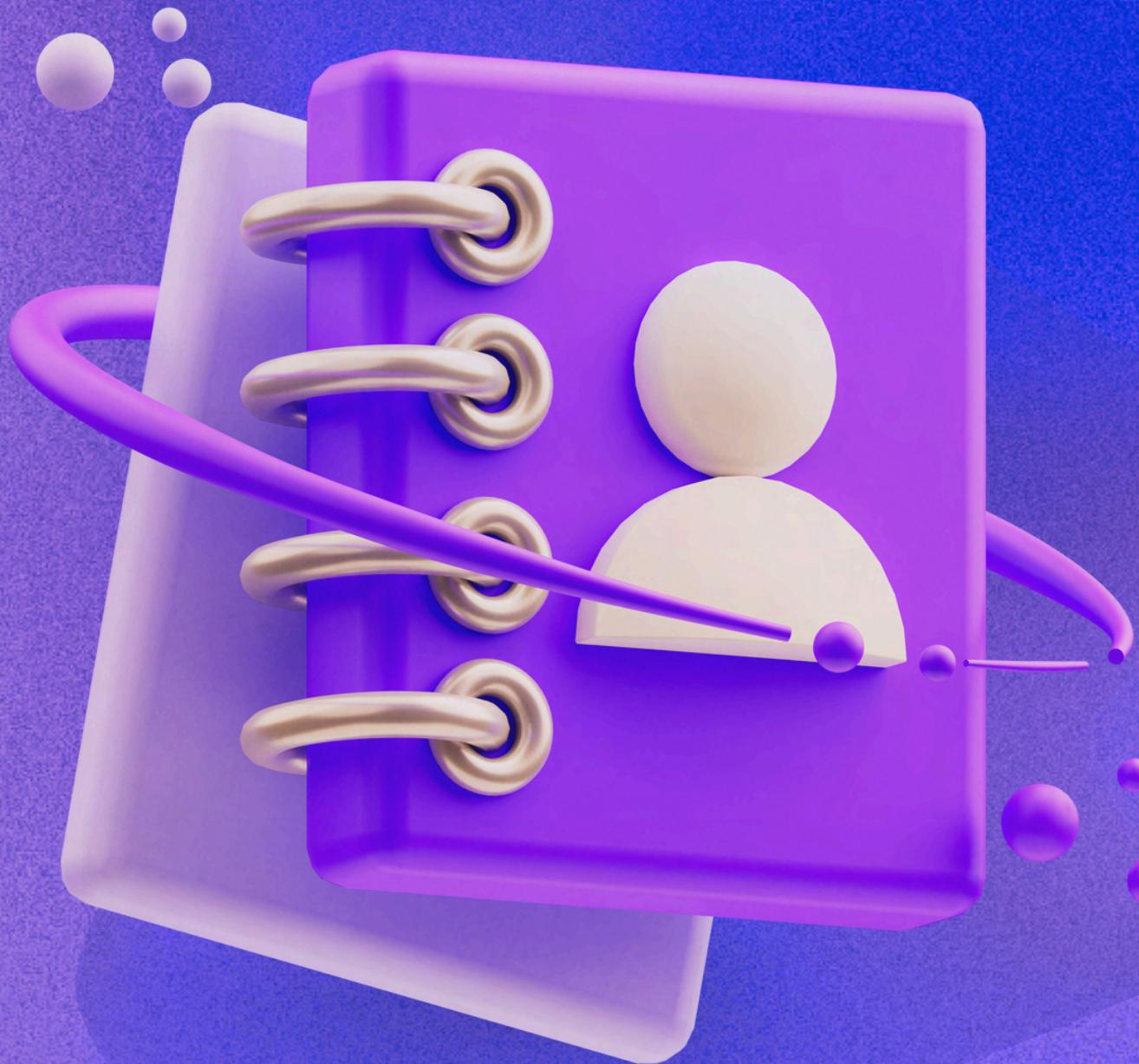
March 21, 2025 2:14 UTC

Affected Virtual Machine:
AggieDetected by
Microsoft[View the full alert >](#)

AI in Cybersecurity

- AI enhances cybersecurity by automating complex threat detection and reducing human workload.
- It analyzes vast amounts of security data to identify patterns that humans might miss.
- AI-driven security solutions can adapt to new attack methods without requiring manual rule updates.

Major Takeaways



- Most people think of AI as chatbots, but it's so much more! Just because its not a chatbot does not mean it does not have any AI elements to it!
- AI-driven solutions for AI-driven problems!
- Cybersecurity is a never-ending battle, but with AI, we can stay one step ahead of attackers.

Thank You!