

Microsoft Sentinel Hackathon - Spring 2022

TWILIGHT MALWARE THREAT DETECTION

POWERED BY



MICROSOFT



DEVPOST

TEAM-TWILIGHT

DEEPAN

KAVYA

Major Security Problems

- 01 Backdoor– malware that gives malicious hackers remote access

- 02 Password stealer–malware that gathers usernames and passwords

- 03 Ransomware– malware that encrypts your files

- 04 Trojan–malware that attempts to appear harmless

- 05 Worm–malware that spreads to other devices file sharing

MICROSOFT AZURE SENTINEL

Limitless cloud speed and scale

Bring your **Office 365** data for Free

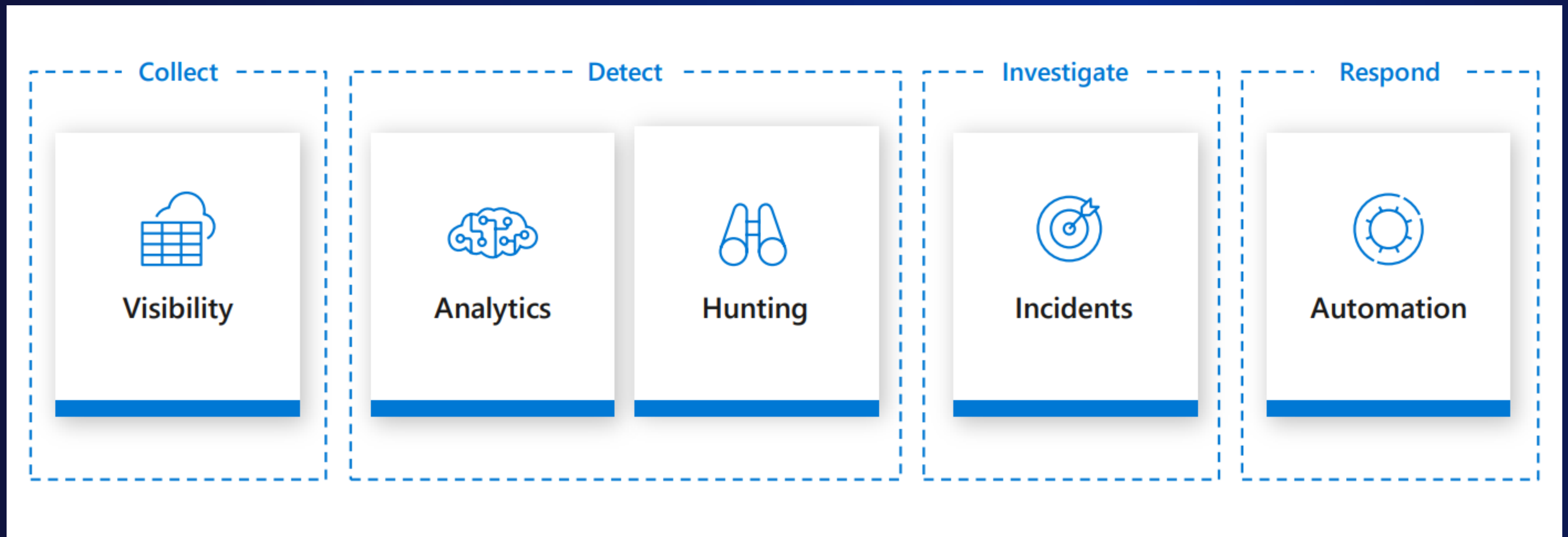
Easy integration with your **existing tools**

Faster threat protection with **AI by your side**



SOLUTION

AZURE SENTINEL END TO END SOLUTION



Architecture

AZURE



SUBSCRIPTION



RESOURCE GROUP



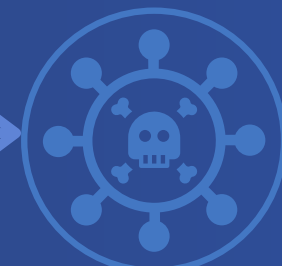
VM



SENTINEL



LOG ANALYTICS
WORKSPACE



THREAT INTELLIGENCE



AUTOMATION

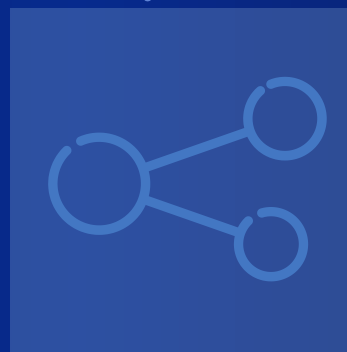


WORKBOOK



ANALYTICS

CONNECTOR



Communication

servicenow

Ticket Analysis



Channel



mail

How it Works

Communication

ANALYTICS

WORKBOOK

AUTOMATION
Logic Apps

THREAT
INTELLIGENCE

SENTINEL

WEB
SERVER

VM

Machine which
has malware exe
installed

Azure Sentinel with log
analytics workspace enables to
detect threat intelligence of
malware exe

Threat Intelligence detects
malware files,exe,tools by
value type such as URLs,
file hashes, or IP addresses
with known threat activity
such as phishing, botnets,
or malware

Automation Rule
playbook creation
using logic apps
which connects to
external services like
servicenow for ticket,
teams channels, mail
communication for
high severity issues

workbooks to visualize
and monitor your data
Using flow connector n.

Microsoft Sentinel allows you
to create custom workbooks
across your data, and also
comes with built-in workbook
templates to allow you to
quickly gain insights across
your data as soon as you
connect a data source.

Analytics rules search for
specific events or sets of
events across your
environment, alert you
when certain event
thresholds or conditions
are reached, generate
incidents for your SOC to
triage and investigate, and
respond to threats with
automated tracking and
remediation processes

servicenow

Visibility

Detection

Automation

*Data
Visualization*

Rule

Demonstration

Git hub link

<https://github.com/TWILIGHTCLOUDCODERZ/TWILIGHTSENTINEL>

Video Link

https://youtu.be/b_Rkvzue_Vg

Thanks for the opportunity to learn and explore new technology

Team - Twilight

POWERED BY



MICROSOFT



DEVPOST

TEAM-TWILIGHT

DEEPAN

KAVYA