Microsoft Azure

Azure Developer Community

Journey  Cyber Security with Linux | Open Source| Microsoft Sentinel

https://github.com/sivolko/rvce-session

This link contains all this session details.

Shubhendu
Cyber Security Engineer

Agenda

- Other sides of Cyber Security
- Why Linux ?
- Role Play of Open Source
- Linux Hands on
- Microsoft Sentinel Hands on
- Quiz

https://github.com/sivolko/rvce-session

This link contains all this session details.

Prerequisite

- Laptop /Mobile with stable Internet
- Duplex Communication
- **Zero Trust Model**

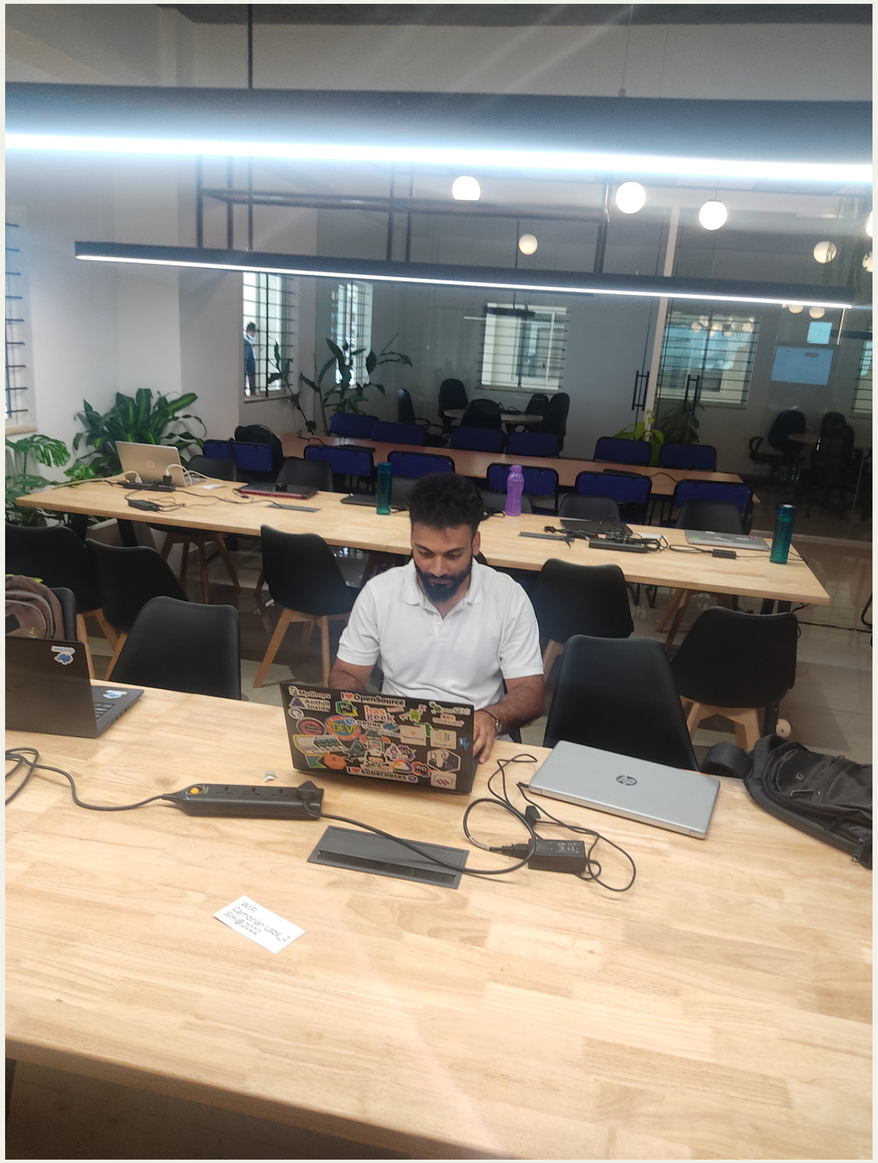
== Never Trust , Always verify

https://github.com/sivolko/rvce-session

This link contains all this session details.

Microsoft Azure

Azure Developer Community



whoami

sudo rm -rf / problems

- Cloud Security Eng @ TCS (Red Team)
- Former SOC L3 (Blue Team)
- Former Product Mentor @ SIH -2022
- Worked with Ministry of Edu & myGov.in
- Open Source Contributor in Docker , Soda foundation
- Meetup-Organiser

hugs4bugs.me

Social Life


Winner
Team Name
Rupees
One Lakh Only
₹ 1,00,000/-


outsystems


Winner
One Lakh Only
₹ 1,00,000/-


Winner
One Lakh Only
₹ 1,00,000/-


14:34

Other sides of Cyber Security

We don't wear black hoodies

we don't hack Insta/Twitter Passwords

we don't use black over green Terminal

Other sides of Cyber Security

We don't wear black hoodies

we don't hack Insta/Twitter Passwords

we don't use black over green Terminal

SOC : Front Liner Defender

Security Operations Center (SOC) analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

Responsibilities

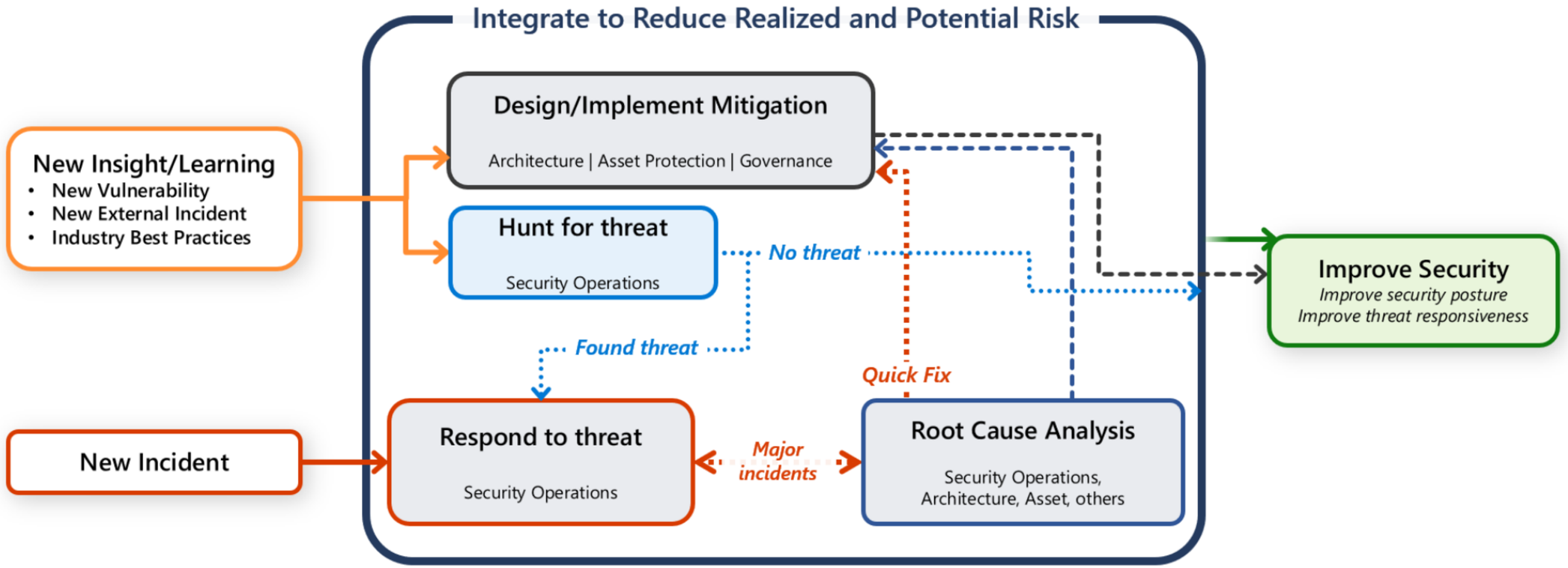
threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats .

SOC : Services

Service	Description
Quick response to detected events	Respond to alerts received from Microsoft Managed Desktop devicesAnalyze event to identify the impactAssess the overall risk to a device or Microsoft Managed Desktop environmentDetermine if a security incident occurred
Drive the security incident response	Protect the Microsoft Managed Desktop environment from known or suspected compromisesReduce the compromise risk by preventing spreadEnsure timely and accurate communication with your security teamProvide analysis and recommendations based on events and risks
Advanced hunting	Provide analysis and recommendations based on events and risksCustomized detections and alert suppression, across managed devices, are part of on-demand indicators and entities for both known and potential threats

source : Microsoft

SOC: Azure



source : Microsoft

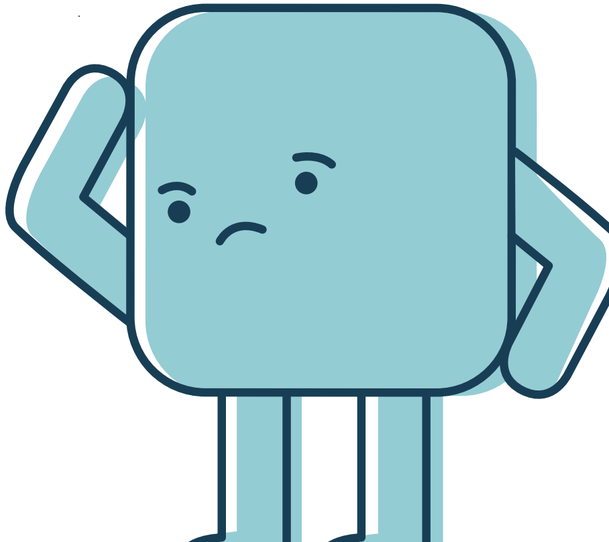
Azure Tools: SOC

Tool	Purpose
Microsoft Sentinel	Centralized Security Information and Event Management (SIEM) to get enterprise-wide visibility into logs.
Microsoft Defender for Cloud	Alert generation. Use security playbook in response to an alert.
Azure Monitor	Event logs from application and Azure services.
Azure Network Security Group (NSG)	Visibility into network activities.
Azure Information Protection	Secure email, documents, and sensitive data that you share outside your company.

source : Microsoft

Why Open Source ?

- is that safe ?
- what if someone steals our code?
- How to contribute ?



Why Linux ?