CWL
CyberWarFare Labs

Detecting Threats in Real Time: A Deep Dive into Defensive Stack Strategies

About CyberWarFare Labs :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform

About Speaker :

Aayush Poojary

Security-Intern

AGENDA

1. Introduction
2. Defensive Stack as a Glance
3. Real-Time Threat Detection
4. Deep Dive: Detection Across Layers

1] Introduction

a) Threat Definition & Impact

- Cyber threats are attempts to steal, damage, or disrupt digital systems.
- Impact- Service Disruptions, Data breach, Financial loss, Compliance Violations, Brand Damage etc

b) Why Real-Time Detection Matters

- Traditional detection = too late.
- Real-time → stops lateral movement & reduces response time.
- Faster incident response → less damage.

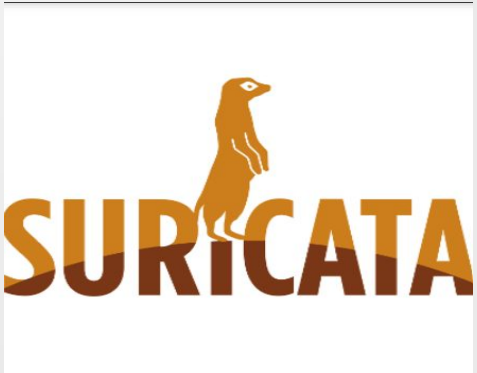
2] Defensive Stack at a Glance

Wazuh (SIEM, EDR, XDR)

- Collects and correlates logs.
- Real-time alerts.
- Integrates with agents for file integrity, rootkit detection.

Suricata (NIDS/IPS)

- Packet-based detection.
- Works with rules to detect threats
- (e.g., malware, exploit attempts).



b) Key Capabilities and Benefits

Tool	Key Capabilities	Benefits
Wazuh	Agent-based monitoring, event analysis, alert correlation	Enhances endpoint visibility, supports compliance, improves threat detection
Suricata	Network- based monitoring, traffic inspection, threat detection	Improves network visibility, detects attacks in real time, complements endpoint tools

3] Real-Time Threat Detection

Structure of Threat Detections:

Components	Description
Data Sources	Where the data comes from
Logs	Records of system activities
Events	Actions or things that happen
Correlation and Rules	Connecting events to find threats
Alerts	Warnings about possible issues
Visualization	Visual representation of data

4] Deep Dive: Detection Across Layers

a) Exploiting Access Mechanisms: SSH Brute-force & Unauthorized SMB Access-

- **SSH Brute-force**: Attackers attempt many username/password combinations to gain unauthorized access to remote systems via SSH.
- **Unauthorized SMB Access**: Attackers exploit weak or default credentials in SMB (file sharing protocol) to access shared files or systems without permission.

b) File & Integrity-Based Attacks- Attackers target critical files and their integrity, modifying or deleting them to disrupt system operations or cover their tracks.

Example: Malicious changes to system files, configuration files, or sensitive data files.

c) Process & Execution Monitoring- Monitoring the execution of processes and applications on a system to detect suspicious or malicious activity.

d) Network-Level Alerts with Suricata- Suricata analyzes network traffic and generates alerts for suspicious activities or potential intrusions at the network level.

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings please contact

support@cyberwarfare.live

To know more about our offerings, please visit: **https://cyberwarfare.live**