Security Operation Center Project

Presented by :
Omar Ayesh & Ahmad Hassouneh
Supervised by:
Dr. Oraib AbuAlganam

What is SOC?

Centralized Unit

Continuous monitoring and analysis of organizational risks.

Detection

Identifying suspicious activity across endpoints and networks.

Response

Rapid action to neutralize cyber threats and attacks.

The Need for Monitoring

- Monitor Attackers **Tactics, Techniques, and Procedures (TTPs)**
- Indicators of Compromise (IOCs) appear across multiple systems
- Continuous monitoring enables early detection and response

Attackers often bypass traditional security controls, requiring continuous monitoring.

Core Tools & Technologies

Splunk SIEM

Central platform for log indexing and visualization.

Sysmon

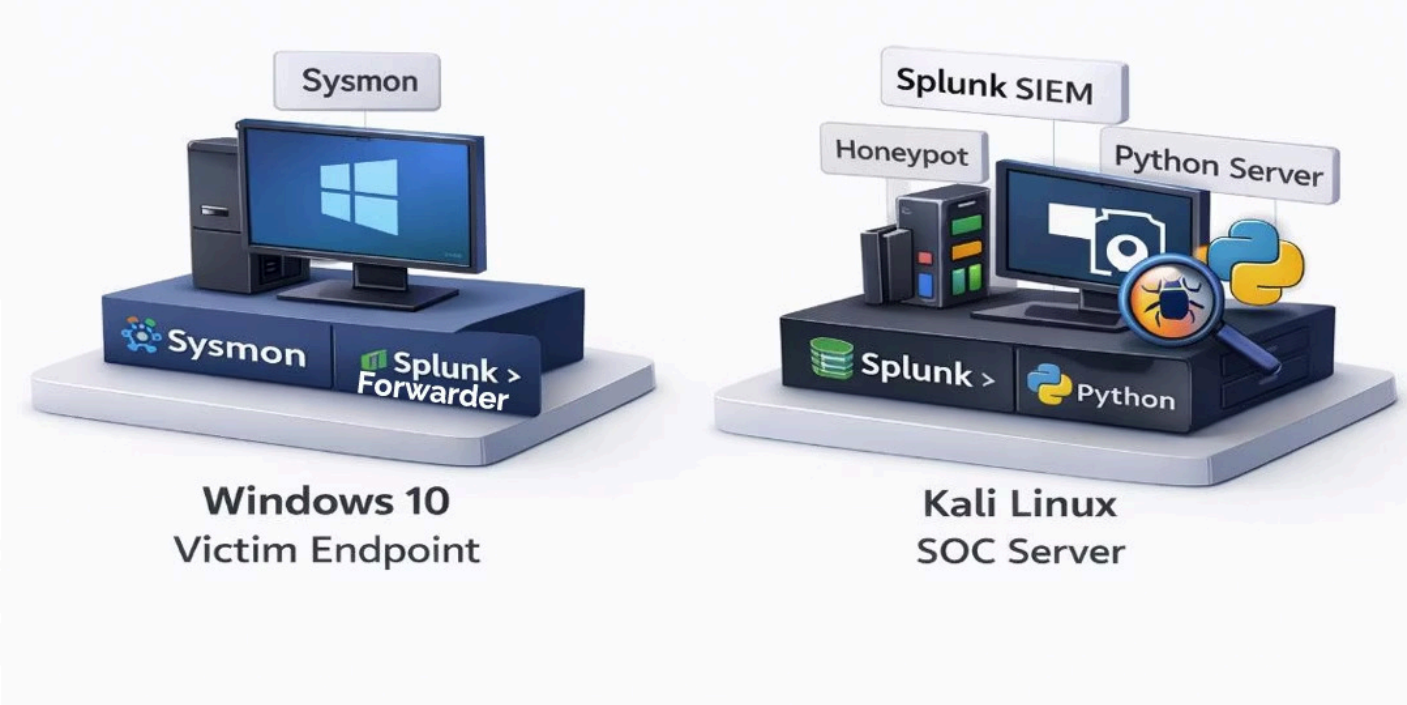
Detailed visibility into Windows endpoint activities.

Pentbox Honeypot

Decoy system to trap and detect lateral movement.

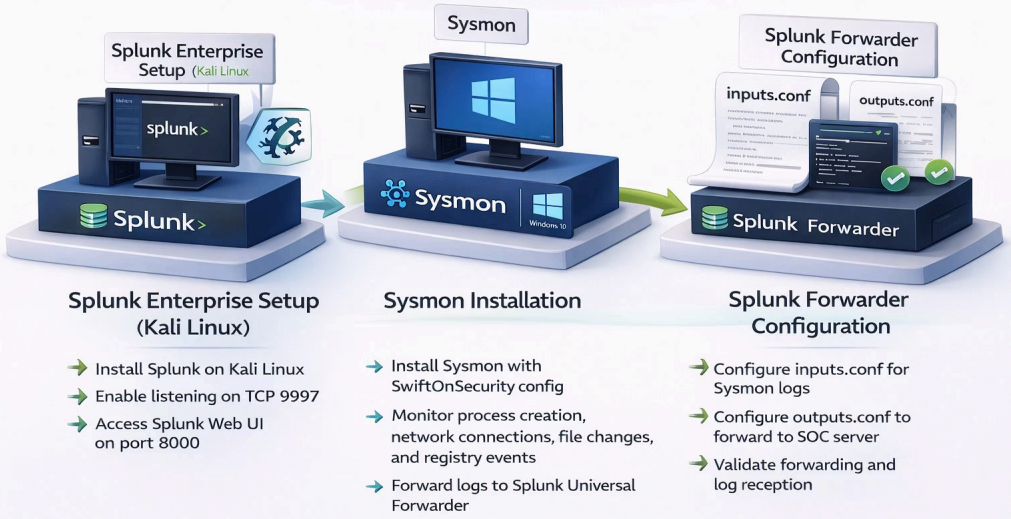
Lab Environment Architecture

Virtual Machine	OS	Role
VM 1	Windows 10	Victim Endpoint (Sysmon + Forwarder)
VM 2	Kali Linux	SOC Server (Splunk + Honeypot)



Lab setup

System Setup & Configuration



Splunk Enterprise Setup (Kali Linux)

- Install Splunk on Kali Linux
- Enable listening on TCP 9997
- Access Splunk Web UI on port 8000

Sysmon Installation

- Install Sysmon with SwiftOnSecurity config
- Monitor process creation, network connections, file changes, and registry events
- Forward logs to Splunk Universal Forwarder

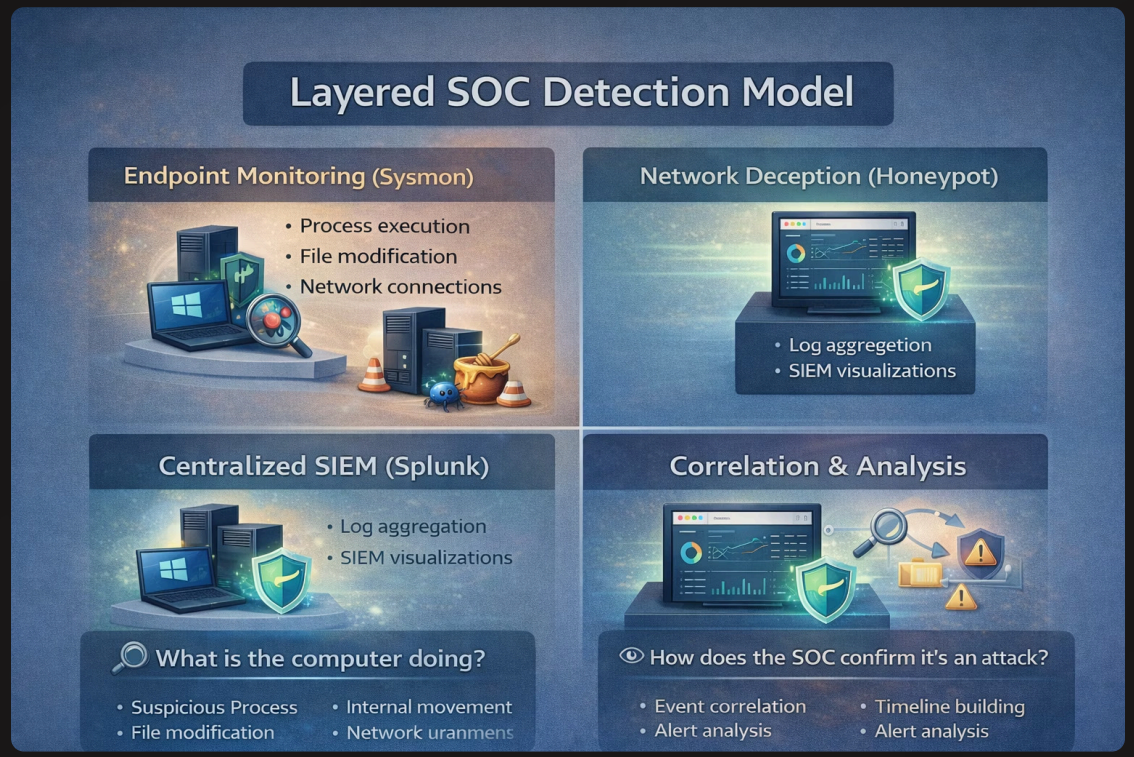
Splunk Forwarder Configuration

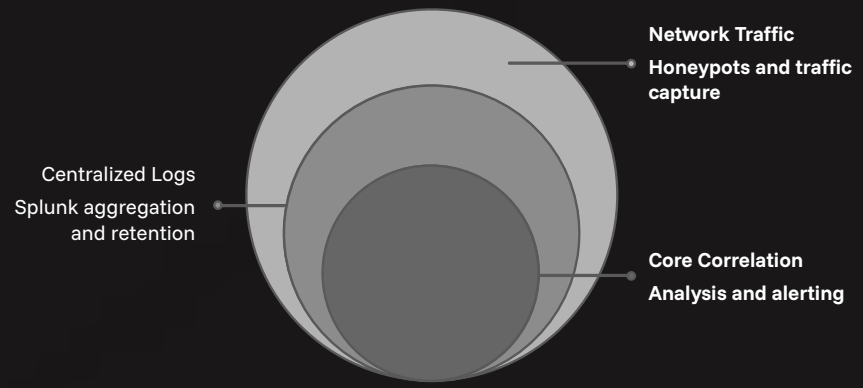
- Configure inputs.conf for Sysmon logs
- Configure outputs.conf to forward to SOC server
- Validate forwarding and log reception

Honeypot Setup

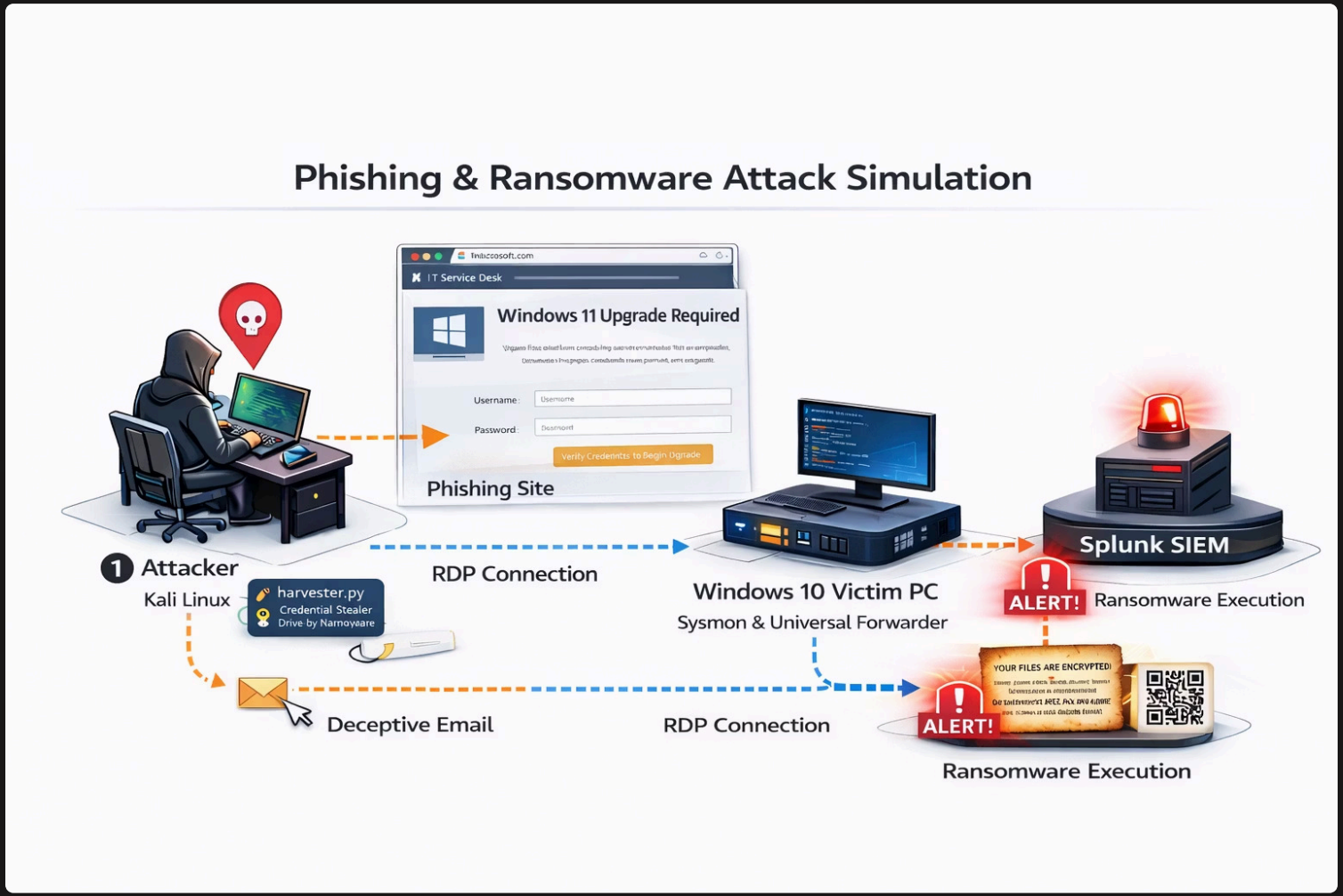
Phishing Website

Layered Detection Model

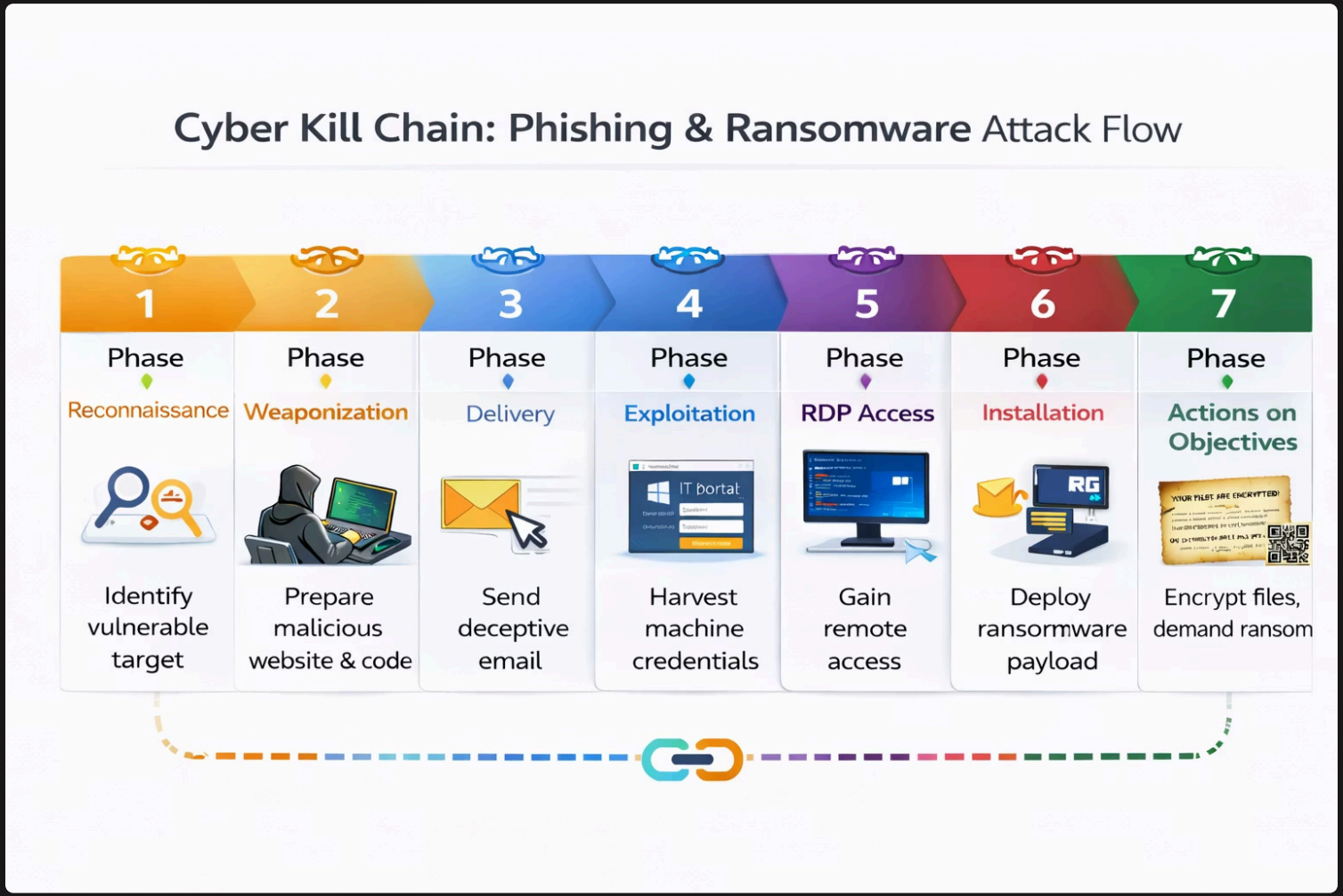




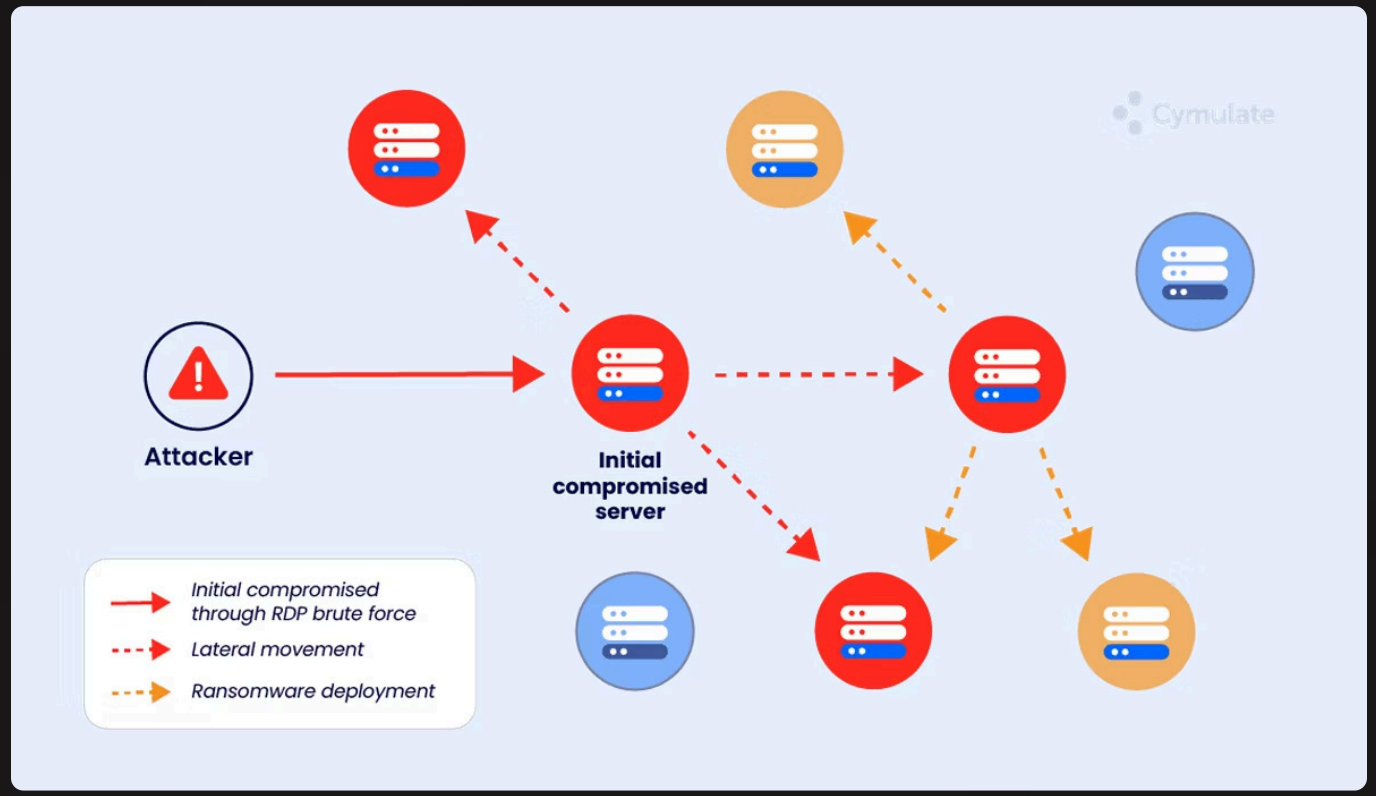
Attack 1: Phishing & Ransomware



Cyber kill chain

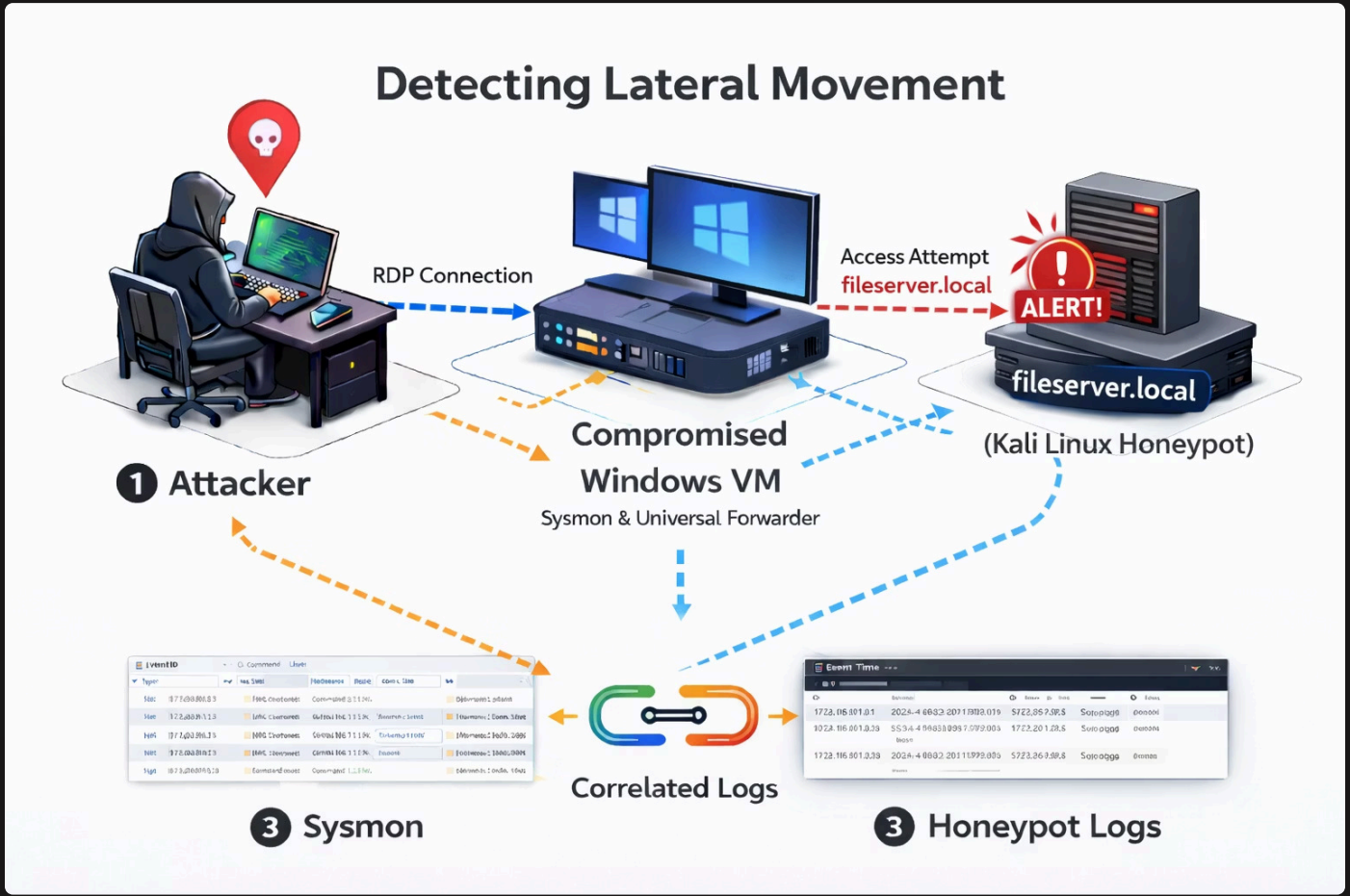


Attack 2: Lateral Movement



- Attacker gains access to one internal system
- Uses legitimate credentials or tools (RDP)
- trying to compromise other internal servers and services
- Attempts to expand access within the network

Attack 2: Lateral Movement



Future Work

AI Integration

Automated alerts and correlation rules.

Threat Intelligence

Enriching analysis with global feeds.

Scaling

Simulating complex multi-endpoint environments.

THE END