Hybrid Microsoft Sentinel Lab
Blue Team Project

Custom Detection Rules | Azure Arc | AMA | SIEM | Incident Response

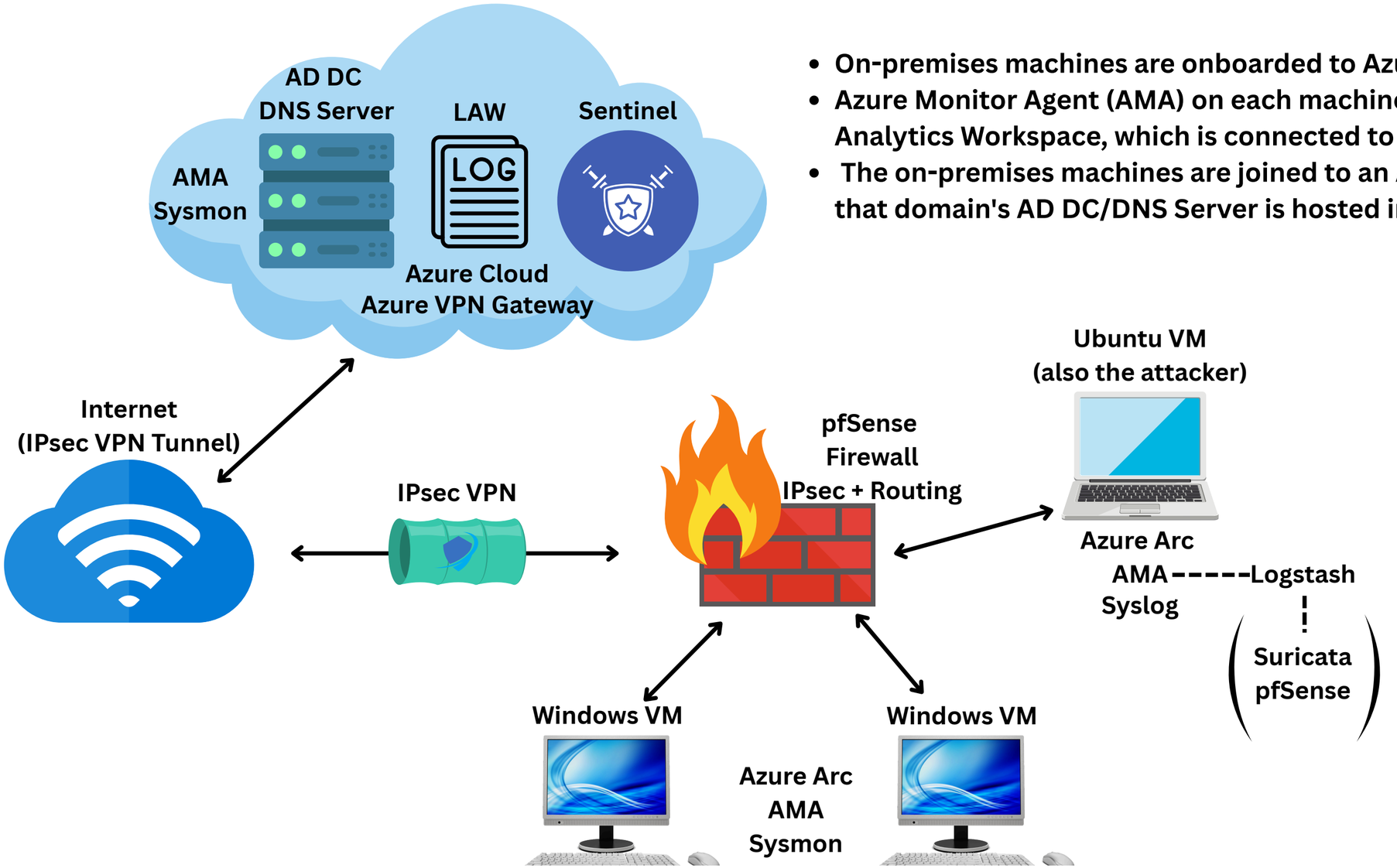
This lab simulates a hybrid enterprise environment with SIEM logging,
AD domain joining, and simulated attacks.

Nikola Marković

Goals

- Simulate a hybrid enterprise setup with cloud-hosted AD and VPN-connected on-premises devices
- Build detection rules for key TTPs (persistence, reverse shell, etc.)
- Visualize attack paths and alerting in Microsoft Sentinel
- Practice KQL, playbooks, and log ingestion
- Simulate attacker behavior to test detection capabilities

Infrastructure



- On-premises machines are onboarded to Azure via Azure Arc.
- Azure Monitor Agent (AMA) on each machine sends logs to Log Analytics Workspace, which is connected to Microsoft Sentinel.
- The on-premises machines are joined to an AD domain, and that domain's AD DC/DNS Server is hosted in the Azure cloud.

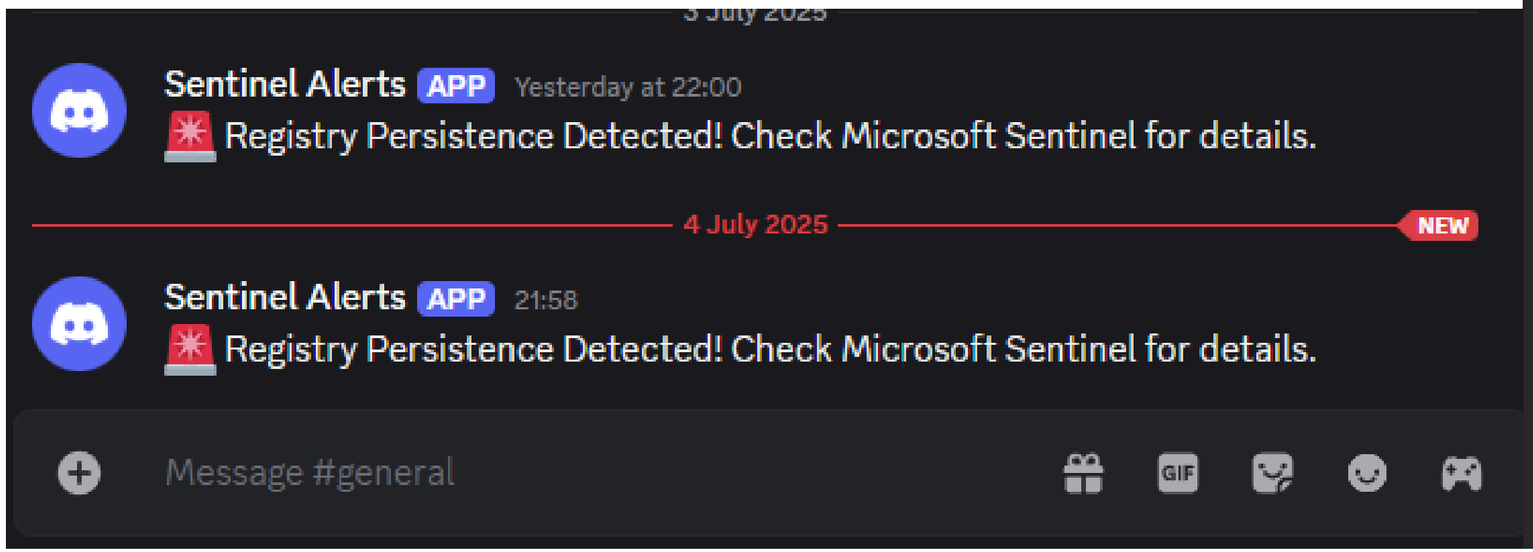
Detection Rules

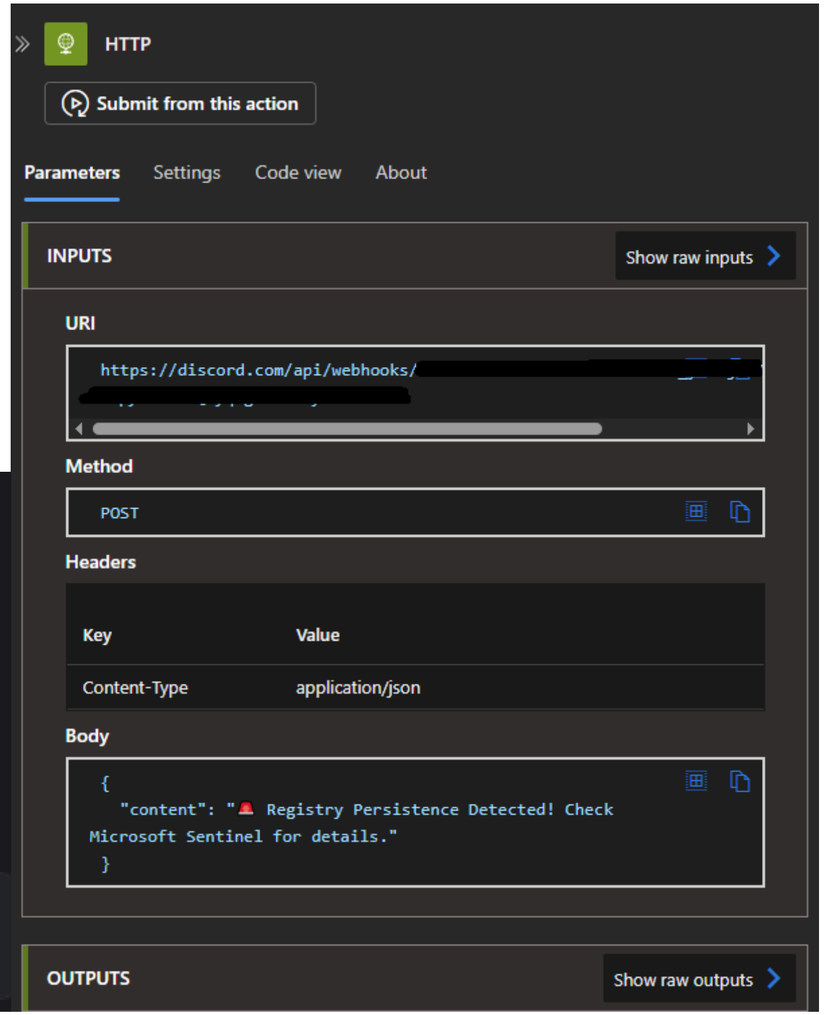
- Suspicious File Creation in Downloads Folder
- Suspicious Download Activity via PowerShell or CMD
- Persistence - Registry Run Key to Suspicious Script or Executable
- Persistence - Suspicious Script or Executable Launched at User Login
- Execution - Suspicious Reverse Shell Activity
- Execution - Reconnaissance Commands Detected
- Network - Suspicious Outbound Connection to C2 Port
- Exfiltration - Sensitive File Access via Command Line
- Brute Force - Multiple Failed Logon Attempts
- Privilege Escalation - User Added to Administrator Group

Severity	Incident number	Title
High	35	Added to Domain Admins, User BLUE\shawnspencer, on CloudWinLab.blue.lab
High	28	Suspicious Outbound Connection to C2 Port 4444, IP 10.10.10.101, on Sentinel-Win10.blue.lab
High	26	Suspicious Reverse Shell or Payload Execution on Sentinel-Win10.blue.lab
High	25	Persistence - Registry Run Key Modified on Sentinel-Win10.blue.lab
High	24	Suspicious Script or Executable Launched at Login on Sentinel-Win10.blue.lab by user BLUE\shawnspencer
Medium	34	Brute Force Attack Detected - Unknown Account on CloudWinLab.blue.lab
Medium	33	Suspicious File Created in Downloads - Sentinel-Win10.blue.lab
Medium	32	Sensitive File Access via Command Line on Sentinel-Win10.blue.lab by BLUE\shawnspencer
Medium	30	Reconnaissance Commands Detected on Sentinel-Win10.blue.lab by BLUE\shawnspencer
Medium	27	Suspicious Download Command Detected on Sentinel-Win10.blue.lab by BLUE\shawnspencer

Automated Playbook: Discord Alert

- **Trigger: Registry persistence detection**
- Action: HTTP POST to Discord via webhook
- Payload: Alert notification sent to Discord
- Purpose: Immediate analyst notification

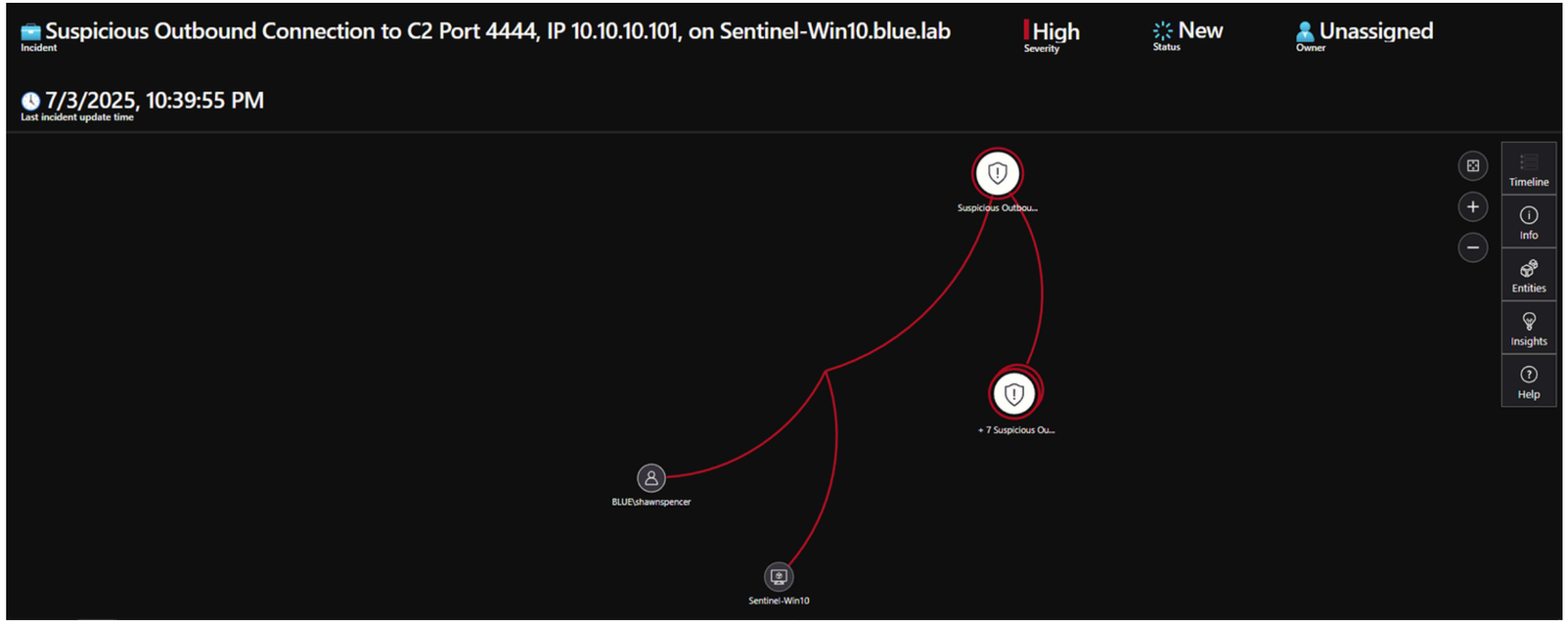




Simulated Attack Flow

Attacker (Ubuntu VM) compromised a Windows 10 user using a fake PDF lure.
Upon execution, the payload downloaded a reverse shell and set persistence via the Windows Run registry key.
The attacker:

- **Achieved persistence via registry run key modification**
- **Established a reverse shell using Netcat**
- **Exfiltrated files over the same channel**
- **Brute-forced credentials and escalated privileges on the domain controller**



Sentinel Investigation Graph – Reverse Shell Detection

Final Notes

- Built a hybrid SOC lab using Azure Arc, Microsoft Sentinel, and on-premises VMs
- Simulated a full attack chain: initial access, persistence, C2, brute-force, privilege escalation
- Created custom detection rules and automated alerts with Logic Apps
- Reviewed and analyzed incidents using Sentinel’s built-in tools (alerts, graphs, KQL)

Contact Info

nikola.z.markovic@pm.me

linkedin.com/in/nikolazmarkovic