# Post-Incident SOC Analysis

## Incident Summary

During my Azure Security Lab, I simulated two common cloud threats:

- **Malware Upload (EICAR Test File)**: A known test file was uploaded to an Azure Storage account to test real-world malware detection.

- **Brute Force RDP Attack**: Multiple failed login attempts were made against a public VM to simulate an RDP brute-force attack.

## Detection & Monitoring

- **Azure Defender for Cloud** immediately flagged the uploaded EICAR test file as malicious, generating a high-severity alert on the storage resource.

- **Azure Sentinel** SIEM integrated with Defender for Cloud correlated and surfaced the incident, providing real-time visibility into security threats.

- The brute-force attack was monitored, and custom analytics rules/playbooks were prepared to detect and respond to suspicious login patterns.

## Response & Remediation

- **Automated Response:**
  A Logic App playbook was triggered by Sentinel to send an email notification to the SOC team when a high-severity incident was detected.

- **Manual Remediation:**
  After reviewing Defender's recommendations, I remediated network security group rules to restrict RDP access and further hardened VM exposure to the Internet.
  The malicious EICAR file was deleted from storage, and security controls were re-scanned to verify no further compromise.

### Results & Security Improvement

- **Alerts and Incidents:**
    - All simulated threats were detected and surfaced in Defender and Sentinel.
    - Incidents were triaged, investigated, and resolved within minutes.
- **Secure Score:**
    - After remediation, Secure Score increased, reflecting improved security posture and reduction in attack surface.
- **Dashboard Visualization:**
    - Built a custom Sentinel Workbook dashboard to visualize incident response metrics and SOC efficiency.

### Lessons Learned & Next Steps

- **Real-time threat detection and automated response are critical for cloud environments.**
- Integrating Defender for Cloud with Sentinel provides end-to-end detection, investigation, and automation capabilities.
- Proactive remediation and secure configuration can prevent common attack vectors like malware uploads and RDP brute force.
- Future enhancements: Integrate with Microsoft Teams for SOC notifications, automate incident closure, and implement Just-In-Time (JIT) access.

## What I'd Improve Next

- **Automate brute-force blocking and alerting via Sentinel analytics rules.**
- **Expand playbooks to trigger on additional incident types.**
- **Simulate additional attack vectors for deeper threat hunting and forensics practice.**