George Mason University
AIT-670- Cloud Computing Security
College of Engineering and Computing

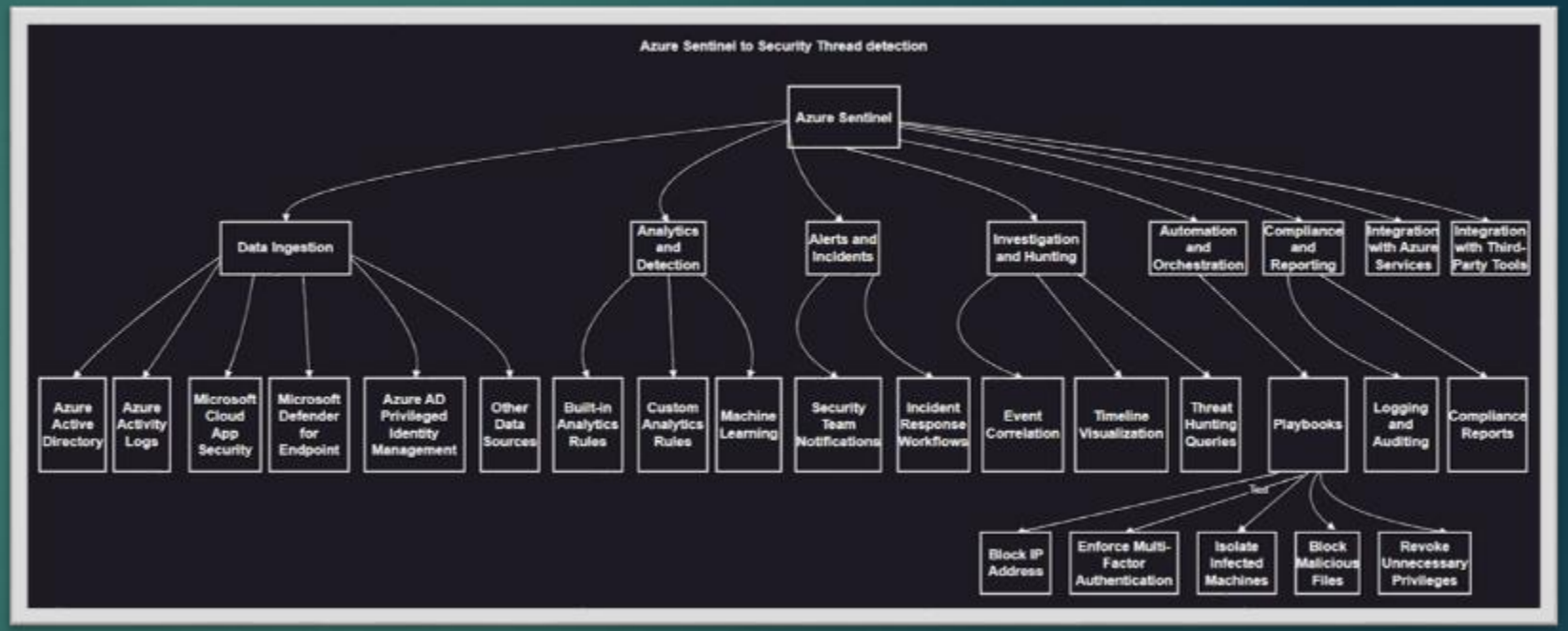
Improving Cloud Security Posture With Azure Sentinel: A Real Time Threat Detection Solution

GROUP 6

PROJECT MEMBERS: MUTHYALA TUSHAAR REDDY, ASHRITH BHOOKA RAVINANDAN, BOJJA SATHWIK REDDY, SAI CHARAN THALLAPELLI, SRI ROHIT YADLAPALLI, MANI KUMAR EDUKOJU, SAI AMARTYA MARUTH MANDEDI

Outline

- Problem Statement: How Azure Sentinel will work to resolve key threats in real time scenarios?
- Research Questions
- List of Tools used in Project
- Process Workflow
- Results
- Lessons Learned & Conclusion
- References



How Azure Sentinel Will Work To Resolve Key Threats In Real Time Scenarios

Problem Statement: In the present cloud security ecosystem, clients face various challenges regarding real-time detection, analysis, and incident response for any suspected incidents that left them vulnerable to subsequent attacks against them, relenting them to cyber threats. With many current setups, manual monitoring of fragmented security systems do not allow for timely and effective protection. The goal is to build an automated Cloud Solution using Azure Sentinel to specially tackle this problem.

How Azure Sentinel Solves the Problem:

- **Early Threat Detection:** Azure Sentinel applies data analytics to real-time suspicious activity detection which diminishes the intended attacks potentially hiding in the attack surface which could affect critical systems.
- **Centralizes Security Data:** Sentinel aggregates the logs and security data of many sources grouped by type into that summarized view that shall commence easily identifying security incidents.
- **Automates Threat Responses:** Automates responses to the known threats, such as quarantining the infected machines or blocking malicious items, therefore reducing the response time and damage through a concept known as Security Orchestration, Automation, and Response, **SOAR**.
- **Proactive Threat Hunting:** Sentinel Threat hunt features enhance to search for hidden threats that may be typically lost by automated systems to improve the triaging strategies for a team-based approach toward a live threat hunt.
- **Future Compliance & Reporting:** Up to date in keeping the compliance report of the latest cyber-attack strategies that will ensure that security measures get very fast up-to-date updates.

Research Questions

- What cost implications and scalability challenges does Azure Sentinel present for organizations of different sizes?
- What are the current strategies that could be implemented to facilitate collaboration among cyber teams, integrated with Azure Sentinel's dashboard and reporting features?
- How does Azure Sentinel handle false positives, and what methods can be taken to prevent them?

List of Tools Used In Project

- **GitHub Link** for all Excel Sheets for Power BI dashboards, PowerShell Scripts, Kusto Queries (KQL), and all other important information: Click Here
- **PowerShell:** To load log data into Azure sentinel tables and convert CSV data to JSON format for Sentinel to recognize
- **KQL Querying:** Usage of Kusto Query Language to query log data for ingestion and analysis in Azure Sentinel
- **Microsoft Power BI:** Visualizing KQL Sentinel Security Use Cases Dashboards
- **Microsoft Excel:** Data holder for logs data in CSV Format
- **Microsoft Azure:** Cloud Platform of Choice for Project Using mainly the Services of Microsoft Sentinel, Log Analytics Workspace, Cloud Shell, and Action Group Alerts

Process Workflow

Log Data Ingestion and Intergration

We are sampling Six Different Security uses cases of data to ingest: Blocked Malicious IP Addresses, Blocking User Privileges, Infected Virtual Machine Logs, Blocking Non-Legitimate Users, and Analysis of Multifactor Authentication and MSFT Entra ID Logs.

To Ingest the above data into Sentinel we use an internally developed PowerShell script where load these logs into a table for sentinel to ingest **[Please Refer to Personal GitHub].** The Data from the six use cases will be converted from CSV format to a JSON format for sentinel to recognize them.

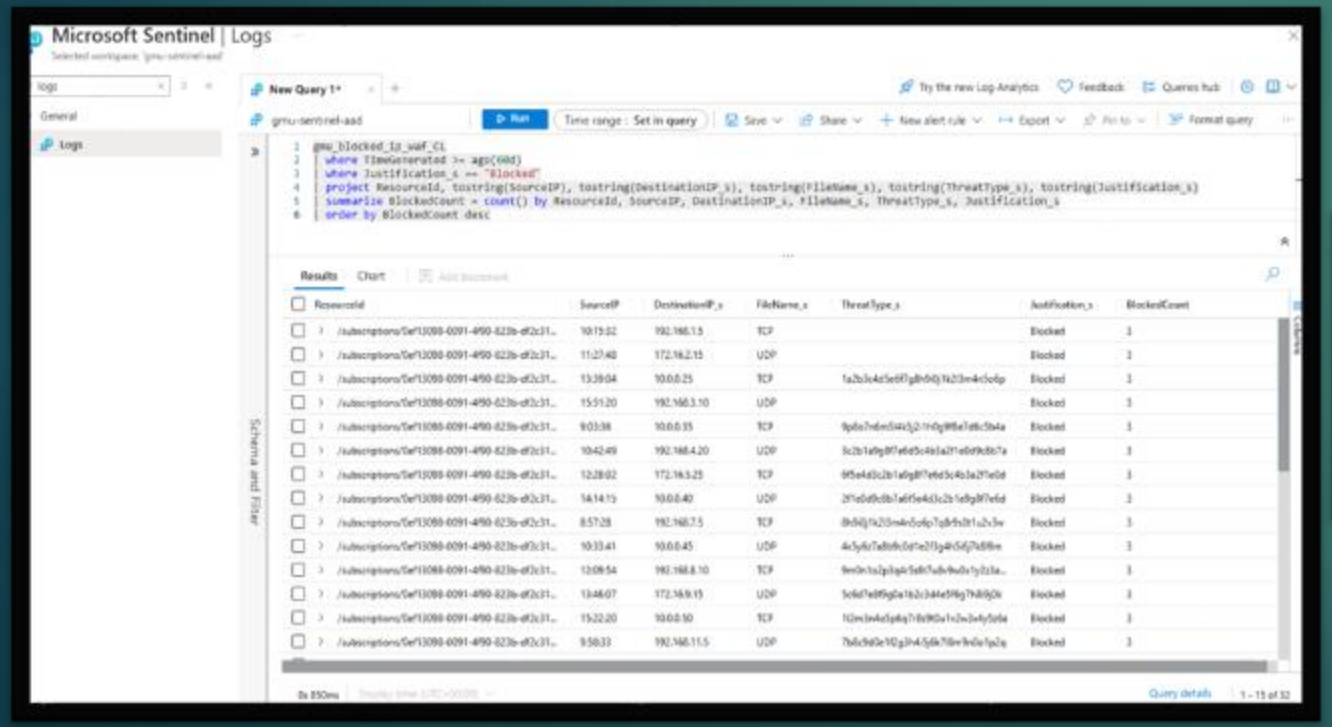
For Step 2 to work correctly, we need to hook up an Azure Log Analytics alongside the created Sentinel workspace ID and the Share Key generated.

Data Ingestion and Intergration

```
# Replace with your Workspace ID
CustomerId = "22a5cfdc-4d0b-4d05-
# Replace with your Primary Key
SharedKey = "PoFviItOCGs8o
# Specify the name of the record type that you'll be creating
LogType = "gmu_blocked_ip_waf"
# Optional name of a field that includes the timestamp for the data. If the time field is not specified, Azure Monitor assumes the time is the message ingestion time
```

```
PS /home/manimozhi> vi gmu_ip.ps1
PS /home/manimozhi> ./gmu_ip.ps1
200
PS /home/manimozhi>
```

PowerShell Execution on Azure Portal



KQL Query Running from Sentinel

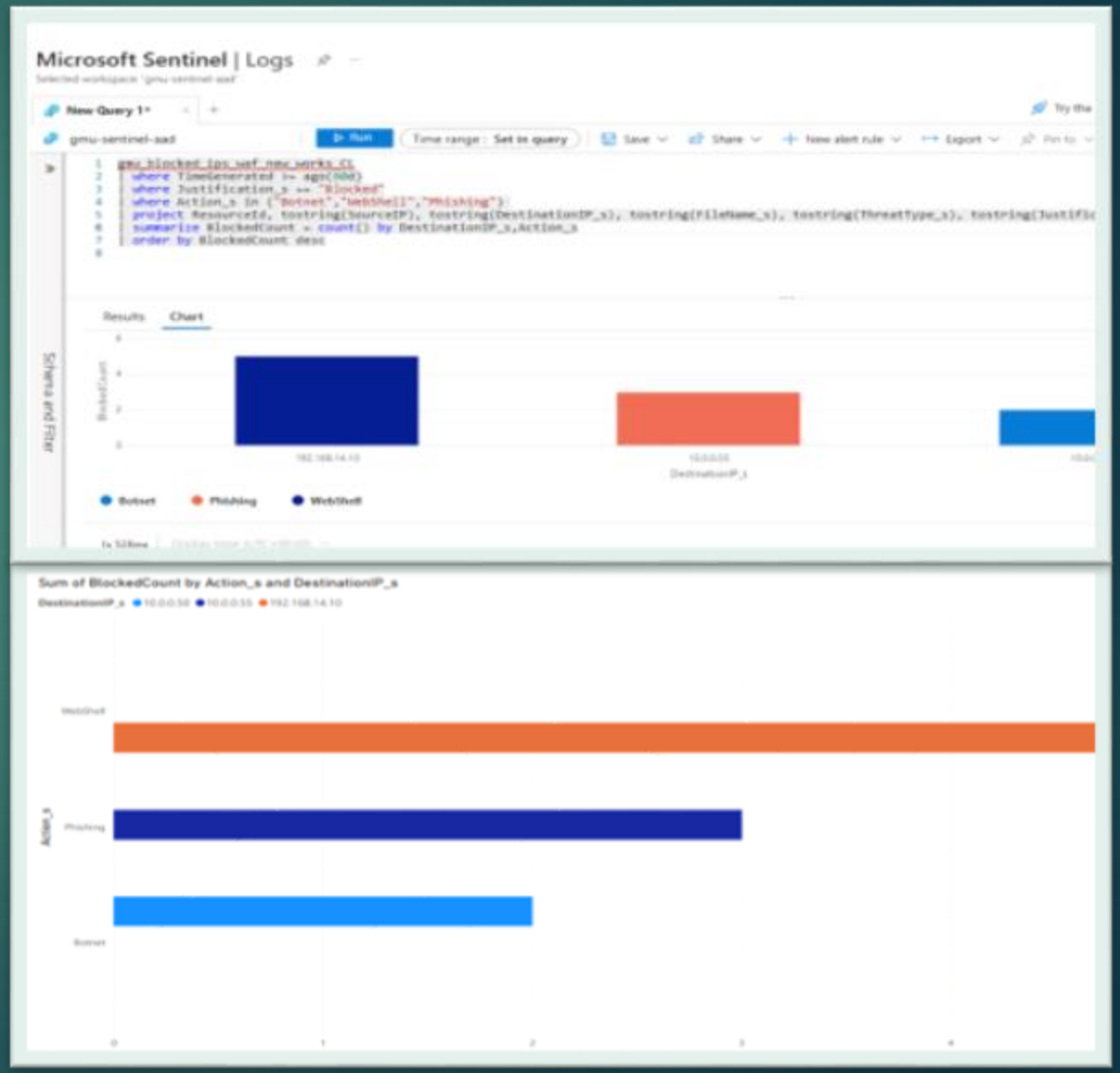
Log Analytics Workspace Table Showing the Loaded Data

Analytics and Threat Detection

- Azure Sentinel Logs can be queried via KQL (Kusto Query Language) after the log ingestion. Each six use security cases have a different KQL query to pull depending on the scenario.**[Also Refer to Personal GitHub for all Six KQL Queries used]**
- After KQL Query is executed, we can generate different type of dashboards to Analyze via the Charts option. In this Project we exported the created Azure chart to Excel and then to Microsoft Power BI to visualize each scenario in a clean format.
- Parallelly after the KQL Query is executed, we can create an alert rule using an action group via Azure monitor to send to our GMU Email for any suspicious activity found from the sentinel incidents.
- Similar Procedure as well to create alert rules to forward to the Sentinel main dashboard which we can triage into categories of Informational, Low, Medium, and High.

Security Use Case #1: Blocked IP's

- The team will create a Microsoft Sentinel security dashboard to monitor botnet, phishing, and web shell activities.
- We'll start in the "Workbooks" section, adding KQL queries for each type of attack.
- Custom dashboard visuals and alert rules provide real-time insights for quick threat response.
- Alerts will send email notifications to the security team upon detecting suspicious activities using actions groups.
- Source IPs tracked per attack: Botnet - 10.0.0.50, Phishing - 10.0.0.55, Web Shell - 192.168.14.10.
- IP tracking reveals repeated threat sources, aiding in proactive security.
- Attack frequency displayed: Botnet - 2 blocks, Phishing - 3 blocks, Web Shell - 3+ blocks.
- Insights support data-driven defenses and targeted responses for our given uses case



Security Use Case #2: Revoked Users

- The team shall make a Microsoft Sentinel security dashboard to monitor revoked users based on azure resource justification aligned with their role + name
- High-Access Activity in Data-Driven Roles: Data Analyst and Developer roles also show frequent access changes; the changes may be justified through "Role change" and "Project completion" that may lead towards typical project-driven task-specific access needs.
- Elevated Privilege Actions by SysAdmins: Which involve sensitive actions like "Employee termination", "Infrastructure change", and "Security audit" require close monitoring due to their high impact on security?
- Potential Insider Threat Risk in Termination Events: Involvement of SysAdmins in "Employee termination" activities could represent high-risk scenarios; post-termination monitoring for unauthorized access becomes paramount in these scenarios.
- Infrastructure Change and Security Audit Justifications: The frequency of SysAdmin activity on "Infrastructure change" and in "Security audit" gives an impression of proactive system maintenance efforts- unexpected spikes warrant further investigation for unauthorized configuration attempts.
- Concentration of Users with High Role Changes: A small pool of users changing roles frequently across multiple projects/departments may indicate possible over-privileging, thereby calling for periodic access review to prune privilege creep

Security Use Case #3: Infected VM Logs

Affected Systems:

▸VMs such as vm42 (IP: 10.0.0.42) and vm48 (IP: 10.0.0.48) are among those showing suspicious activities, such as unauthorized SSH key additions and malware-related events.

Threat Types:

▸Possible malware distribution was flagged due to suspicious file uploads on vm42.

▸Unauthorized access was detected on vm48 via the addition of an unknown SSH key, raising concerns about insider threats.

Event Patterns:

▸vm46 (IP: 10.0.0.46) exhibited critical log tampering, indicating an attacker attempting to erase traces of activity.

▸vm44 (IP: 10.0.0.44) recorded unusual connections to the Tor network, suggesting attempts to anonymize malicious actions.

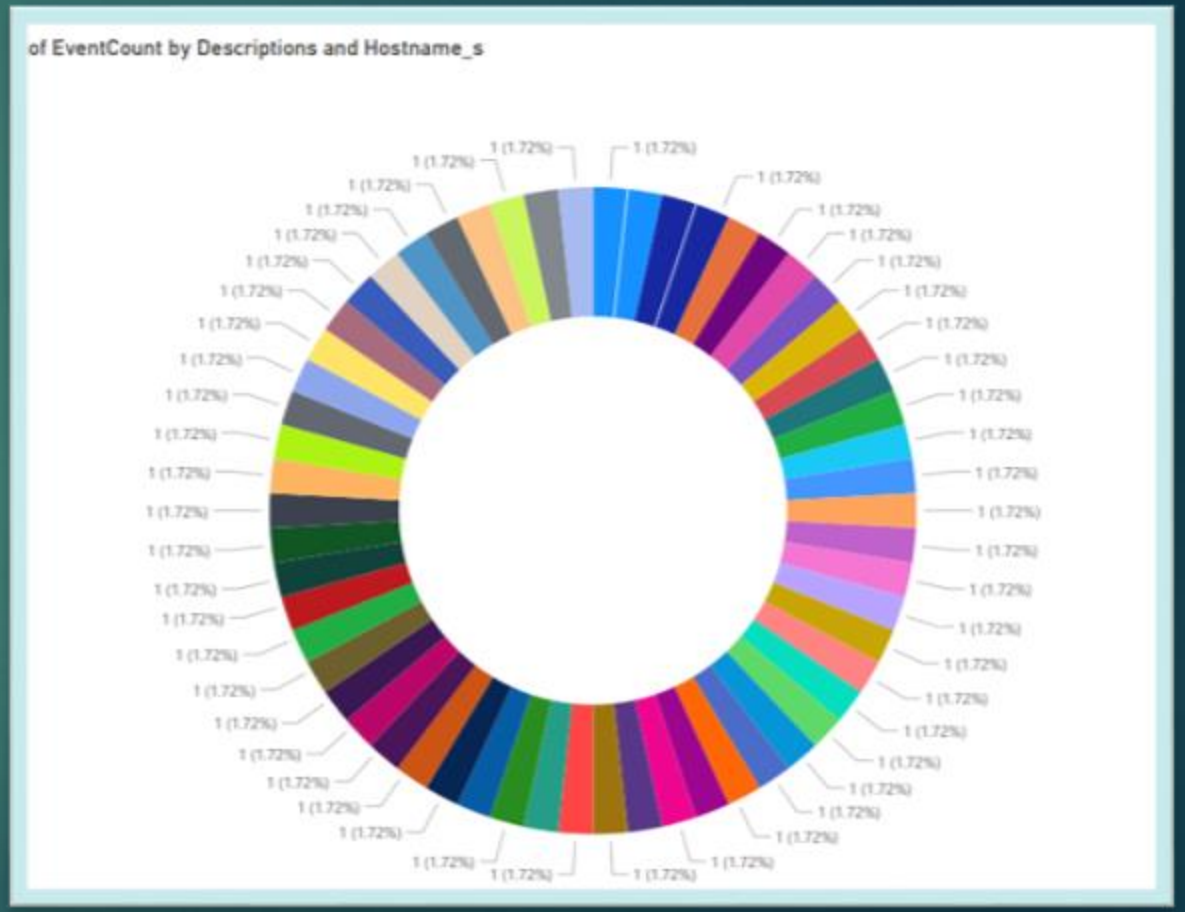
Impact Metrics Threshold:

▸VMs with critical threat levels, such as vm46 and vm52 (IP: 10.0.0.52), require immediate investigation due to activities like high CPU usage, potentially pointing to system compromise.

Potential Security Recommendations:

▸Isolate vm46 to secure logs and prevent further tampering.

▸For vm42 and vm44, review uploaded files and monitor network connections for anomalous traffic patterns to prevent potential malware delivery and anonymized attacks.



Security Use Case #4/#5: MFA Non-Legit and Legit Users Analysis

- **Multiple Authentication Methods Failure**: Failed MFA attempts across SMS, Mobile App, and Phone Call suggest user errors or potential automated attacks trying to bypass MFA.
- **Global Geopolitical Variations**: High-risk locations like the US, AU, and IN indicate potential cyberattack regions, but could also reflect legitimate users facing connectivity issues.
- **Repeated Failures from Same User**: Several consecutive MFA failures within short timeframes may point to credential stuffing or brute force attempts.
- **Device-Specific Issues**: Different devices (iPhone, Android, Windows, macOS) failing MFA indicate potential synchronization problems or targeted attacks on device vulnerabilities.
- **High Risk from Multiple Locations**: Authentication attempts from different regions, especially in quick succession, may suggest account compromise or testing by unauthorized users.
- **High Frequency of Authentication Failures**: The consistent frequency of failed MFA attempts throughout the day (from 12:30 to 16:41) may indicate a sustained attack or misconfigured authentication systems, requiring closer monitoring to identify and mitigate potential threats.

Security Use Case #6: Entra ID Logs

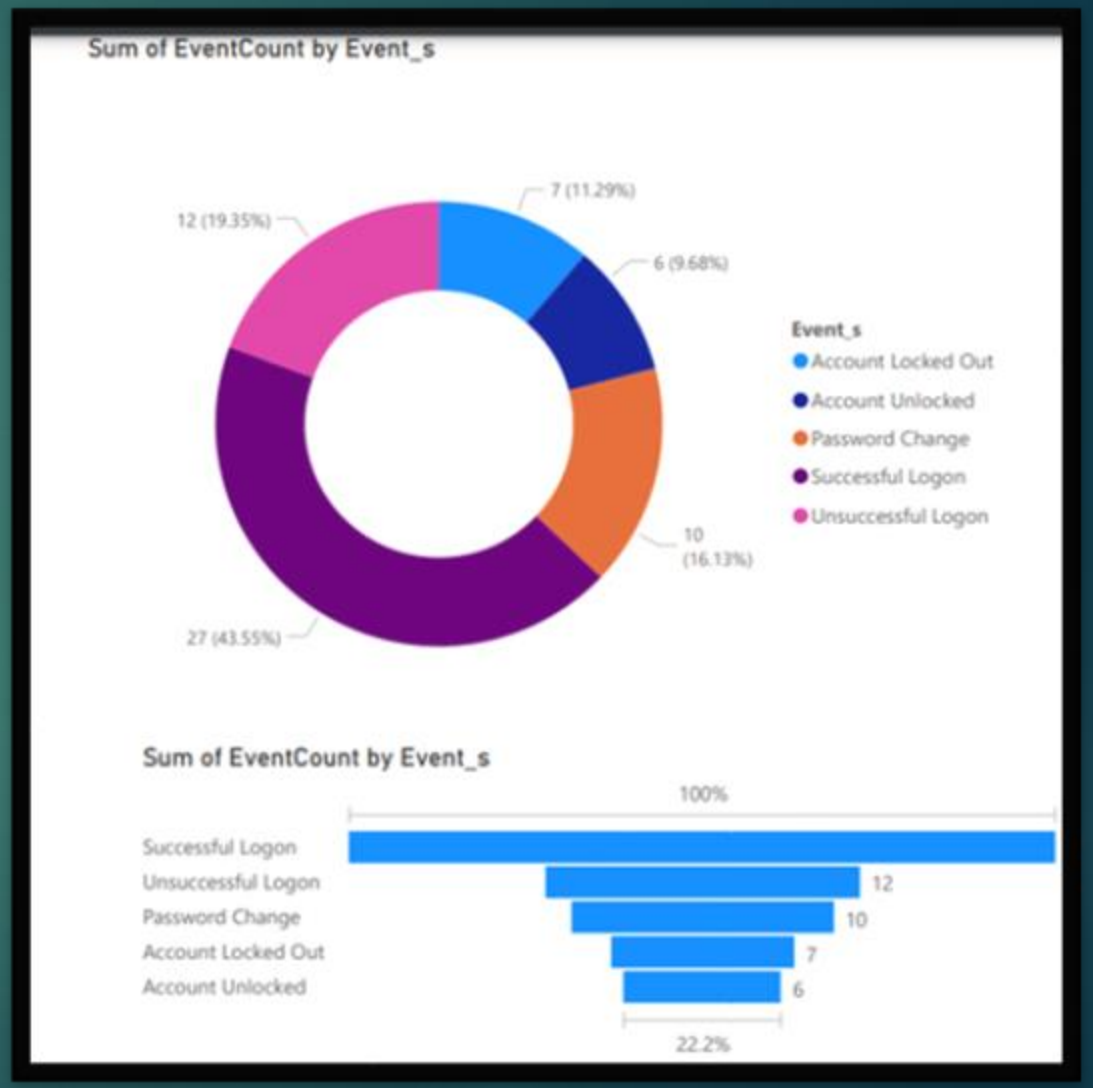
•**Multiple Failed Login Attempts**: User2, User5, User7, and User10 experienced unsuccessful logins, indicating either user errors or potential attack attempts on their accounts. This could be a sign of unauthorized access attempts or simple user misconfigurations.

•**Account Lockouts and Unlocked Events**: User4, User6, User8 experienced account lockouts, followed by account unlock events. This may indicate security measures triggered by multiple failed login attempts, suggesting potential brute-force or unauthorized access attempts.

•**Successful Logins Post-Lockout**: Despite previous lockouts, users such as User4 and User6 were able to successfully log in afterward, which could indicate that either their accounts were properly unlocked, or access was granted after successful recovery procedures.

•**Password Changes Indications**: User1, User8 underwent password changes, potentially for security reasons or in response to account issues. Password changes could also indicate an ongoing effort to improve account security or resolve access issues.

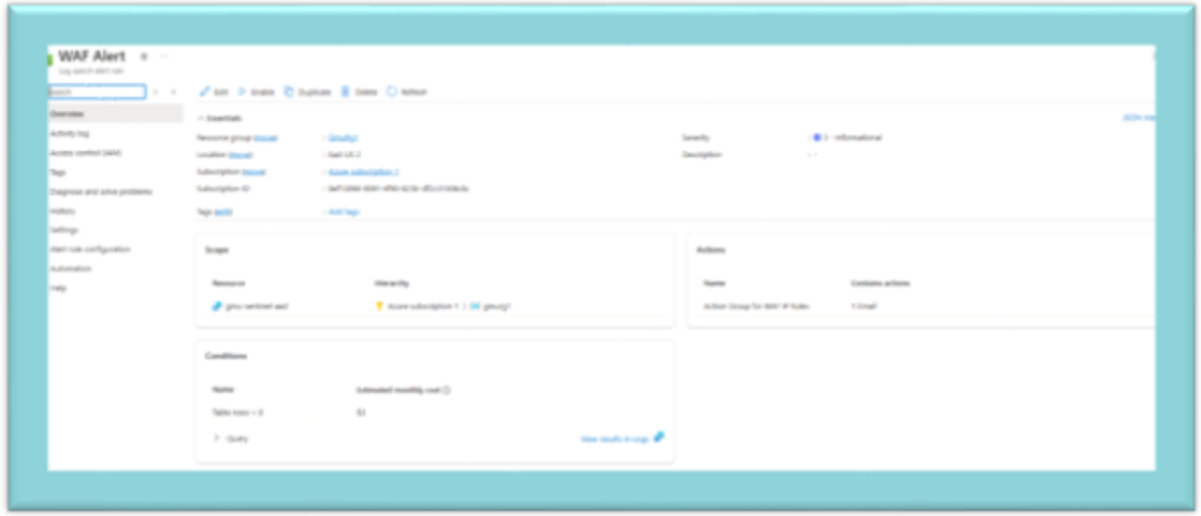
•**IP Address Analysis**: The data reveals multiple logons from various IP addresses (e.g., 10.0.0.1, 10.0.0.2, etc.). A high number of failed logins from a particular IP or unusual IP patterns could indicate suspicious behavior, warranting closer inspection for potential malicious activity.

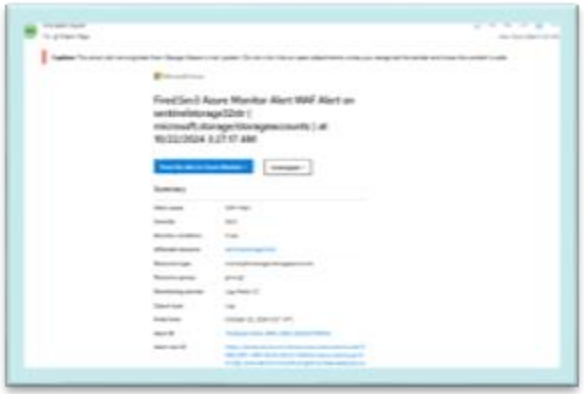


Alerts and Incident Management

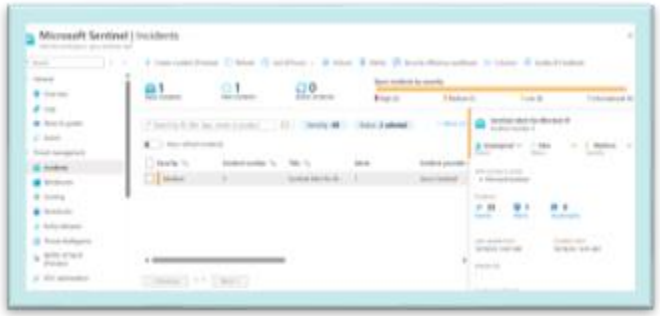
- We can create Incident Using KQL. Ex. Create a High Priority Incident for reoccurring Blocked IP attack logs in the last 5 minutes.
- Like Threat Detection we can also alert these incidents to our email via Action groups
- From the email or from the live Sentinel Incident Management dashboard we can review the live incident and assign to a user to review and hopefully mitigate live incident to closure.

WAF Azure Alert << Action Group Azure





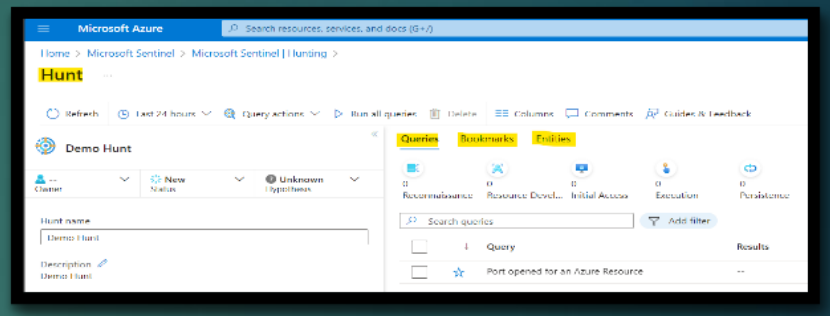
GMU Azure Email Alert From Action Groups



Sentinel Dashboard/Incident Tracker

Investigation and Threat Hunting

- In a Live Threat hunt, we need categorize our threats in a method of triaging. Ex. Would an IP Blocked due to a rootkit from an unknown location pose a higher threat and require more attention compared to a threat where a Virtual Machine got infected with Malware needs to be cleaned up.
- Comparing this to our Security six use cases there will be various threats spun up from them and we need to categorize them and clean them up based on threat hunt triage priority



"Leverage MITRE ATT&CK in Sentinel to map threat hunting strategies with precise adversary techniques. Enhance detection by aligning KQL queries and analytics rules to known tactics and indicators of compromise (IOCs)."

Investigation and Threat Hunting

1. Blocked Malicious IP Addresses

- **Scenario:** This is viewed as a suspected botnet because multiple login attempts originated from this previously unknown IP from different geographical locations.

Hunt Questions:

- Was this IP address flagged by multiple sources? **Yes**
- What other activity has this IP engaged in on the network? **Rootkits**
- Are there any associated IP's that show anomalous behavior? **Yes**

Conclusion: If the IP has recently been tied to attacks, it may shed light on a larger campaign targeting your environment that deserves attention right away.

Investigation and Threat Hunting

2. Blocking User Privileges

- **Scenario:** After an unexplained surge in access requests for sensitive data (which the user would usually not access), a user's privileges were blocked.

Hunt Questions:

- What were the reasons for the privilege escalation requests? **Role Change**
- Has this user account shown signs of compromise (e.g., unusual login times or locations)? **Yes**
- Are there any signs of collaboration with other accounts (e.g., shared sessions)? **Yes**

Conclusion: If the observed user behavior aligns itself with the attempts at data exfiltration, that may imply insider threat or an account compromise scenario.

Investigation and Threat Hunting

3. Infected Virtual Machine Logs

- **Scenario:** Logs show this VM was infected by some form of malware and was trying to contact a known C2 server under the greatest suspicion.

Hunt Questions:

- How did the malware initially infiltrate the VM? **Unauthorized Access and File Sharing**
- What actions were performed by the malware before detection? **Unusual Connection Attempts**
- Are there other VMs on the same host showing similar signs of infection? **Yes**

Conclusion: If this is an infection carried across multiple VMs, it may warrant widespread containment and remediation.

Investigation and Threat Hunting

4. **Blocking Non-legitimate Users**

- **Scenario:** Blocking an account or group of accounts is often the result of situational audit checks by the proper authorities to review non-legitimate users created without proper verification processes.

Hunt Questions:

- Where did these accounts originate (i.e., their IP addresses or email domains)? **Outside and Inside the USA**
- Do they follow any patterns that suggest they might have been created by some sort of automated script? **Possibly**
- Have these accounts done anything that interacted with any sensitive systems? **Yes**

Conclusion: If non-legitimate accounts are suspect for provoking credential stuffing or phishing campaigns, it warrants further investigation towards their account creation processes.

Investigation and Threat Hunting

5. Analysis of Multifactor Authentication (MFA)

- **Scenario:** Conspicuous circumstances within the MFA logs display a string of failed attempts of authentication, before which a relevant user logged in a location previously unassociated.

Hunt Questions:

- Was there a successful MFA attack, and if so, how did it occur? **Yes, Via Permission Change via SMS Swap**
- Were there any indications of a hack of the package? **Yes, But not detailed enough to predict from these limited logs**
- Has this user reported anything suspicious over the past couple of weeks? **Not Clear**

Conclusion: If MFA was circumvented, then it raises questions regarding the usability of the current authentication systems and the possible exploitable weaknesses in the system.

Investigation and Threat Hunting

6. Analysis of MSFT Entra ID Logs

- **Scenario:** The alteration of Entra ID logs indicates that a service principal has been vested with rights greater than operational requirements; perhaps this is indicative of a misconfiguration or misuse.

Hunt Questions:

- What actions triggered the permission changes, and by whom? **Account Lock out by user #26**
- Are there any audit trails indicating legitimate use of these permissions? **Potentially by studying the previous history of users**
- Are there any incidents connected that indicate a service account has been compromised?

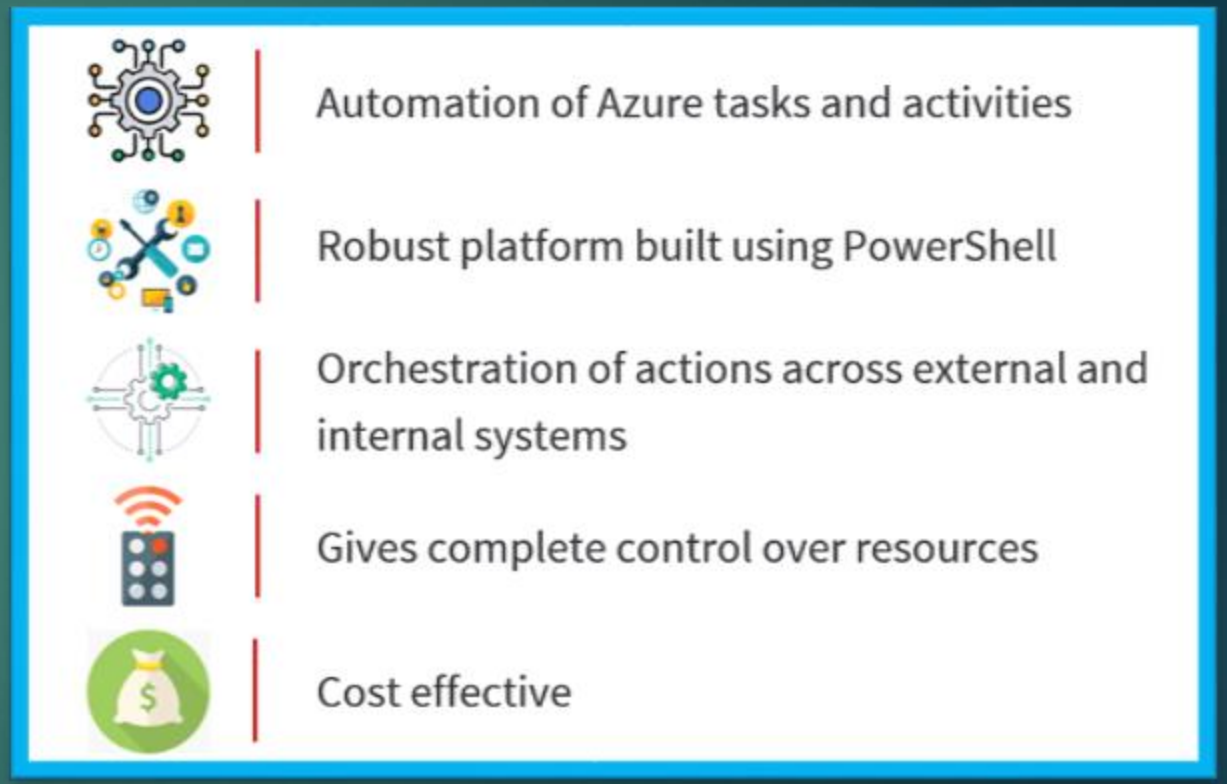
Conclusion: If the permission escalation seems unwarranted, it may very well evidence possible privilege abuse or exploitation that requires immediate attention.

Investigation and Threat Hunting

- **Azure Sentinel** provides the triage categories or incident severity levels to assist in prioritizing security incidents while focusing attention on the most critical threats. These categories generally include:
- **Informational:** events that are of low risk and are logged for monitoring purposes but that are not necessarily indicative of a threat and do not necessarily warrant immediate attention are audited for benign activities most of the time.
- **Low:** incidents in the system are incidents not likely to become a significant threat; should they be unattended to propagate their nuisance over time, they may result in significant problems. These include minor anomalies or policy violations.
- **Medium:** incidents that warrant attention with a moderate degree of risk that could have larger security implications if not mitigated. Often, they are indicators of attempted but failed attacks or suspicious activity.
- **High:** incidents that are serious in nature, demanding intensified and immediate attention and response mainly when a successful attack or breach has taken place that might compromise the most critical systems or data.
- **Critical:** the most serious category, involving any act that constitutes a threat to the systems and infrastructures of the various organizations and requires prompt action to minimize or mitigate heavy losses to their data or social infrastructures.

Automation and Orchestration

- **Automated Response with Playbooks**: We can Create Sentinel playbooks triggered by alerts from non-legit MFA activity (e.g., multiple failures or suspicious IPs). Playbooks can automate actions such as disabling compromised accounts, notifying administrators, or blocking malicious IPs in real-time.
- **Integration with SOAR for Enhanced Hunting**: We can Leverage Sentinel's SOAR capabilities to enrich MFA failure data with external threat intelligence (e.g., IP reputation or geolocation). Automated orchestration workflows can correlate this data with other logs (e.g., sign-in logs, VPN activity) to identify broader attack patterns and provide proactive threat-hunting insights.



Compliance and Reporting: EX. MFA Analysis Study

▶Recommended Actions for Compliance Study With Sentinel

▶User Education: Train users on MFA best practices to reduce suspicious login attempts.

▶Policy Review: Update access control policies to block high-risk IP ranges and enforce stricter geolocation restrictions.

▶Alert Rules: Configure Sentinel to trigger alerts when specific compliance thresholds (e.g., more than 5 failed MFA attempts per user) are crossed.

▶This report could be expanded into a comprehensive workbook or exported to share with auditors to fulfill compliance documentation requirements.

Metric	Value	Compliance Measure
Total Non-Legit MFA Attempts	25	Ensure policy for frequent failures
Users Impacted	10	Flag accounts for review and remediation
High-Risk Locations	3 countries	Review access policies and geo-restrictions

Results

Seamless Data Integration:

- Successfully ingested logs from six security use cases into Azure Sentinel using the PowerShell script. The script effectively converted CSV data into JSON format, enabling compatibility with Sentinel.

Enhanced Threat Monitoring:

- The Azure Log Analytics workspace, integrated with the Sentinel workspace ID and shared key, allowed real-time ingestion and analysis of security events like malicious IP blocking, user privilege violations, and infected VM logs.

Improved Security Insights:

- The ingested data facilitated the creation of actionable dashboards and alert rules in Sentinel using action groups, providing comprehensive coverage across use cases, including MFA anomalies and unauthorized access detection.

Enhanced Threat Hunting and Compliance Auditing:

- The ingested log data supported proactive threat hunting by identifying suspicious activities and patterns across use cases, while ensuring compliance through detailed auditing of user access, privilege blocks, and MFA enforcement logs.

Lessons Learned & Conclusion

Based on our research questions:

- **Cost Implications**: Smaller organizations may face financial constraints due to Azure Sentinel's pay-as-you-go model for data ingestion and retention, while larger organizations benefit from its ability to scale with increased log volume but may encounter higher operational costs for extensive use.
- **Scalability Challenges**: As log sources grow, scaling Sentinel requires optimization strategies like selecting specific data types for ingestion or implementing tiered data storage to balance cost with performance as we saw with our use cases.
- **Collaboration Strategies Among Cyber Teams**
- **Integrated Workspaces**: Enable multiple cyber teams to collaborate by creating shared workspaces within Azure Sentinel and standardizing KQL queries, dashboards, and reporting templates for unified analysis.
- **Enhanced Reporting**: Implement automated workflows and scheduled reports that compile findings across integrated threat-hunting and incident-response activities, fostering cross-team situational awareness.
- **Handling and Preventing False Positives**
- **Custom Alert Thresholds**: Set specific thresholds and conditions tailored to your typical normal behavior patterns to reduce the likelihood of generating false positives. For example, fine-tune rules to ignore low-severity events or establish baseline activity profiles for known systems and users.
- **Whitelist Known Entities**: Create and maintain dynamic whitelists of trusted IP addresses, devices, and users to exclude them from alert triggers, ensuring focus on anomalous or genuinely suspicious activities.

References (MLA)

- Microsoft. "Data Collector API." *Azure Monitor Logs*, Microsoft, https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-collector-api?tabs=powershell#alternatives-and-considerations. Accessed 16 Nov. 2024.
- Tutorials Dojo. "How to Set Up Alerts Rules and Action Groups in Azure Monitor." *Tutorials Dojo*, https://tutorialsdojo.com/how-to-set-up-alerts-rules-and-action-groups-in-azure-monitor/. Accessed 16 Nov. 2024
- Trull, Jonathan, et al. *Microsoft Azure Sentinel: Planning and Implementing Microsoft's Cloud-Native SIEM Solution*. Microsoft Press, 2020.
- Falode, Elijah. *Microsoft Power BI Demystified: Step by Step Guide on How to Create Interactive Dashboard and Reports Using Power BI.* M-POWER CORPORATE, 2021.
- "Use KQL to Master Sentinel Data." *Practical 365*, https://practical365.com/use-kql-to-master-sentinel-data/. Accessed 16 Nov. 2024.
- "Conditional Access Policies for Entra Joined Devices." *Scalefusion Help Center*, https://help.scalefusion.com/docs/conditional-access-policies-for-entra-joined-devices. Accessed 16 Nov. 2024.
- Van der Woude, Derk. "Web Attacks Prevented by Azure WAF and Detected by Azure Sentinel." *Medium*, 19 Aug. 2021, https://derkvanderwoude.medium.com/web-attacks-prevented-by-azure-waf-and-detected-by-azure-sentinel-a4d78f46100b. Accessed 16 Nov. 2024.
- University of New Mexico. "What Is Azure Multi-Factor Authentication (MFA) and How Does It Work at UNM?" *UNM IT Services*, University of New Mexico, 2023, https://unm.custhelp.com/app/answers/detail/a_id/7823/~/what-is-azure-multi-factor-authentication-%28mfa%29-and-how-does-it-work-at-unm%3F.
- "How to Check Azure Firewall Logs." *MS Codes*, 2024, ms.codes/blogs/internet-security/how-to-check-azure-firewall-logs?srsltid=AfmBOooGHu1z94ydTJpl7zxNl9en68lb4nJqvO5D4daVYM_wsid8sH0w. Accessed 14 Nov. 2024.


THANK YOU