24 Use Cases

Microsoft Sentinel

SIEM

for Threat detection

Rajneesh Gupta
@rajneeshcyber

WHAT IS MICROSOFT SENTINEL SIEM?

Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) solution that helps detect, respond to, and manage security threats in real time across hybrid environments.
It leverages AI and automation to enhance threat detection and streamline incident response, integrating with both Azure services and third-party tools.

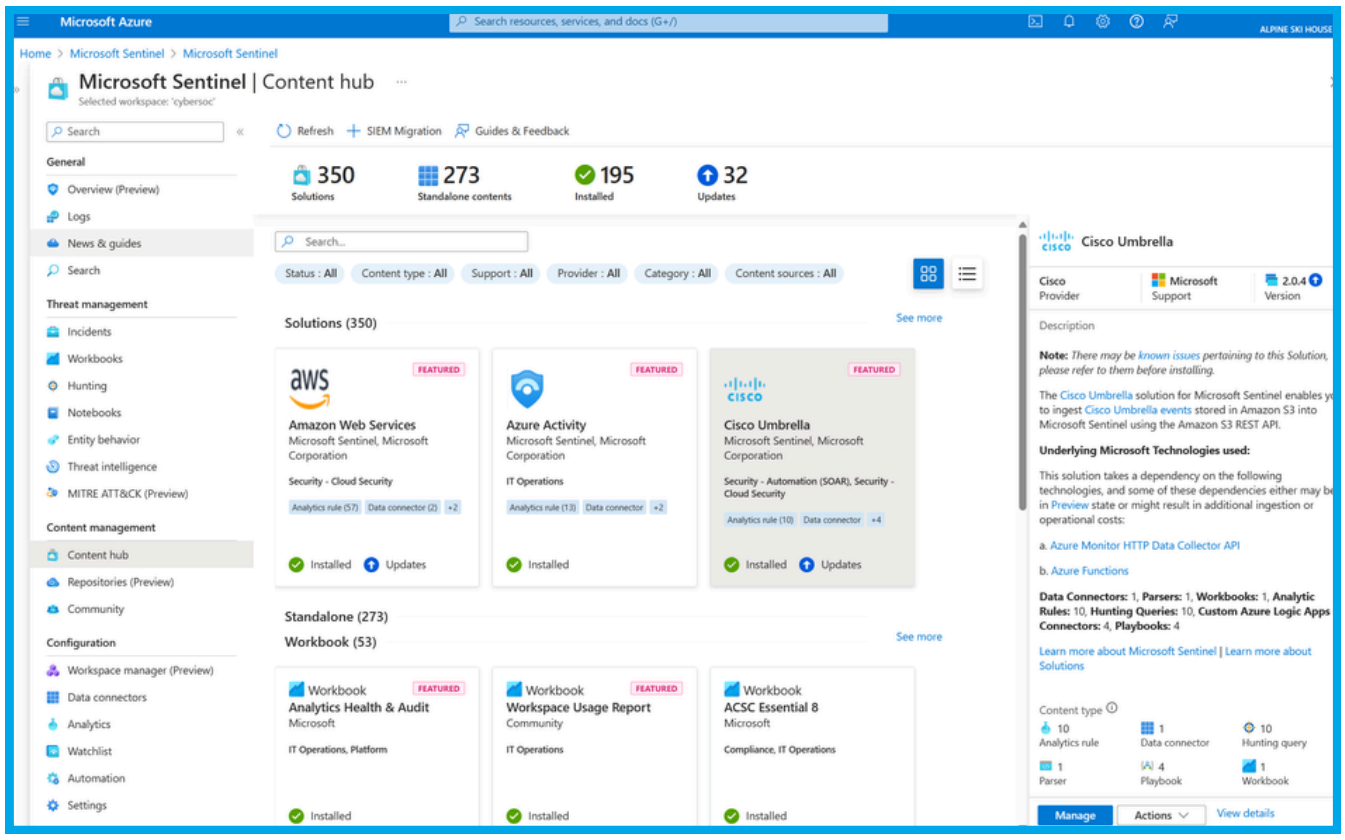
Key Features:

- Centralized security management across cloud and on-premises
- AI-powered incident detection and automation
- Built-in integrations with Azure services and third-party tools

WHY USE MICROSOFT SENTINEL SIEM?

Benefits

- Rapid deployment with cloud-native architecture
- Efficient automation for repetitive tasks
- Comprehensive visibility across systems



WHY USE MICROSOFT SENTINEL SIEM?

Benefits

- Rapid deployment with cloud-native architecture
- Efficient automation for repetitive tasks
- Comprehensive visibility across systems

SUPPORTED INTEGRATION

Azure Services

Integrates seamlessly with Azure Active Directory, Azure Security Center, and Azure Monitor for enhanced security management.

Third-Party Tools

Supports popular security solutions like Palo Alto, Cisco, Fortinet, and AWS, allowing for comprehensive monitoring across diverse environments.

SIEM and SOAR

Works with various SIEM tools like Splunk and security orchestration solutions like ServiceNow for streamlined incident response.

Custom Data Connectors

Allows custom connectors to ingest data from virtually any source using REST APIs or Logstash.

MICROSOFT SENTINEL QUERY (KQL EXAMPLE)

- Microsoft Sentinel uses Kusto Query Language (KQL) for searching and analyzing security logs.
- Powerful query capabilities allow you to filter, aggregate, and visualize security data.

Example Query: Detect Suspicious Login Attempts

```
SigninLogs
| where ResultType != 0
| summarize Count = count() by UserPrincipalName,
IPAddress
| order by Count desc
```

Explanation:

- Filters failed logins (ResultType != 0)
- Aggregates the count of failed logins by user and IP address
- Lists the most frequent failed login attempts to detect potential threats

24 USE CASES

MICROSOFT SENTINEL SIEM

NEXT

1

BRUTE FORCE ATTACK DETECTION

Goal

Identify brute force login attempts on Windows systems through repeated failed login attempts.

Example query

```
SecurityEvent
| where EventID == 4625
| summarize count() by Account, bin(TimeGenerated, 5m)
```

Outcome

Alerts when multiple failed login attempts from the same account are detected within 5 minutes.

2

PRIVILEGE ESCALATION DETECTION (SYSMON)

Goal

Detect unauthorized privilege escalation by monitoring process creation events with admin-level access.

Example query

```
Sysmon
| where EventID == 1 and ElevatedToken == "True"
```

Outcome

Detects processes that are started with elevated privileges, indicating potential privilege escalation attempts.

3

PALO ALTO SUSPICIOUS DNS QUERIES

Goal

Detect unusual DNS queries, which may indicate malware or exfiltration attempts via DNS tunneling.

Example query

```
PaloAltoNetwork_CL
| where action == "dns-query"
| where query contains "suspicious-domain"
```

Outcome

Flags suspicious DNS queries, detecting potential data exfiltration or command-and-control activity.

4

CROWDSTRIKE MALWARE DETECTION

Goal

Detect active malware identified by CrowdStrike agents across the endpoint environment.

Example query

```
CrowdStrikeEvent_CL
| where EventType == "malware-detected"
```

Outcome

Detects and alerts on any malware detected by CrowdStrike, allowing quick containment of infected endpoints.

5

UNAUTHORIZED FIREWALL CONFIGURATION CHANGES

Goal

Identify unauthorized changes to Palo Alto firewall configurations, which may weaken security controls.

Example query

```
PaloAltoNetwork_CL
| where action == "configuration-change"
```

Outcome

Detects and flags unauthorized changes in firewall settings, preventing accidental or malicious configuration tampering.

6

SUSPICIOUS LATERAL MOVEMENT

Goal

Detect unusual lateral movement attempts from one Windows machine to another using Sysmon event logs.

Example query

```
Sysmon
| where EventID == 3 and DestinationIP != "internal_IPs"
```

Outcome

Identifies lateral movement by alerting on unusual remote connections to unauthorized IP addresses.

7

REMOTE DESKTOP PROTOCOL (RDP) LOGIN MONITORING

Goal

Monitor and detect unusual RDP login activities from unfamiliar IP addresses on Windows servers.

Example query

```
SecurityEvent
| where EventID == 4624 and LogonType == 10
```

Outcome

Detects successful RDP logins, helping identify potentially unauthorized access via remote desktop.

8

MALICIOUS POWERSHELL ACTIVITY

Goal

Detect suspicious PowerShell commands execution that may indicate an attack or malicious script execution.

Example query

```
Sysmon
| where EventID == 4104 and CommandLine contains
"Invoke-Mimikatz"
```

Outcome

Identifies the use of known malicious PowerShell commands like Mimikatz, a common tool for credential theft.

9

UNAUTHORIZED FILE ACCESS

Goal

Detect unauthorized access to sensitive files and directories on Windows systems.

Example query

```
SecurityEvent
| where EventID == 4663 and ObjectName contains
"sensitive_file"
```

Outcome

Alerts on unauthorized file access attempts, highlighting potential insider threats or data theft activities.

10

SUSPICIOUS WEB TRAFFIC (PALO ALTO)

Goal

Monitor for outbound traffic to suspicious or blacklisted domains from the network using Palo Alto logs.

Example query

```
PaloAltoNetwork_CL
| where action == "web-browse" and URL in ("suspicious-URL")
```

Outcome

Detects outbound web traffic to suspicious domains, which could indicate malware communication or exfiltration.

11

CROWDSTRIKE HIGH SEVERITY THREATS

Goal

Detect high severity threats as flagged by CrowdStrike on endpoints for prioritized response.

Example query

```
CrowdStrikeEvent_CL
| where Severity == "High"
```

CrowdStrikeEvent_CL
| where Severity == "High"

Outcome

Provides alerts on high severity threats identified by CrowdStrike, ensuring prompt attention to critical incidents.

12

SUSPICIOUS REGISTRY CHANGES (SYSMON)

Goal

Detect unauthorized or suspicious changes to the Windows registry that may indicate persistence techniques.

Example query

```
CrowdStrikeEvent_CL
| where Severity == "High"
```

```
Sysmon
| where EventID == 13 and TargetObject contains "run\\"
```

Outcome

Detects modifications to auto-start registry keys, commonly used by attackers for persistence.

13

EXCESSIVE FAILED LOGIN ATTEMPTS (PALO ALTO)

Goal

Detect repeated failed login attempts across Palo Alto firewalls that may indicate brute force attacks.

Example query

```
PaloAltoNetwork_CL
| where action == "login-failed"
| summarize count() by UserName, bin(TimeGenerated, 5m)
```

Outcome

Flags multiple failed login attempts over a short period, signaling a potential brute force attack.

14

ABNORMAL PROCESS EXECUTION

Goal

Detect the execution of uncommon or suspicious processes that could indicate malware or insider threats.

Example query

```
Sysmon
| where EventID == 1 and ProcessName contains
"suspicious.exe"
```

Outcome

Identifies unusual process execution, helping detect malware or unauthorized software running on systems.

15

INTERNAL PHISHING DETECTION

Goal

Detect employees sending or receiving internal phishing emails using Windows event logs.

Example query

```
EmailEvents
| where Subject contains "urgent request"
```

Outcome

Detects potential phishing attempts by flagging emails with common phishing keywords or phrases.

16

CROWDSTRIKE THREAT INTELLIGENCE CORRELATION

Goal

Correlate CrowdStrike threat intelligence with current incidents to detect known malicious IPs or hashes.

Example query

```
CrowdStrikeEvent_CL
| where ThreatType == "KnownMalware"
```

Outcome

Matches endpoint data with CrowdStrike's threat intelligence, identifying systems infected by known malware.

17

UNAUTHORIZED APPLICATION INSTALLATION

Goal

Detect unauthorized installation of new software or applications on Windows systems

Example query

```
SecurityEvent
| where EventID == 4688 and ProcessName contains
"setup.exe"
```

Outcome

Alerts on any new application installations, identifying potential unauthorized software on the system.

18

FIREWALL PORT SCANNING DETECTION

Goal

Detect internal or external port scanning attempts using Palo Alto firewall logs.

Example query

```
PaloAltoNetwork_CL
| where action == "scan" and ApplicationProtocol ==
"TCP"
```

Outcome

Detects and alerts on port scanning activity, which could indicate reconnaissance efforts by an attacker.

19

CROWDSTRIKE LATERAL MOVEMENT DETECTION

Goal

Detect lateral movement attempts identified by CrowdStrike logs across the network.

Example query

```
CrowdStrikeEvent_CL
| where EventType == "lateral-movement"
```

Outcome

Alerts when CrowdStrike detects lateral movement behavior, allowing for swift investigation and containment.

20

SUSPICIOUS POWERSHELL EXECUTION (SYSMON)

Goal

Detect any suspicious PowerShell commands executed on a system via Sysmon logs.

Example query

```
Sysmon
| where EventID == 4104 and CommandLine contains "-nop"
```

Outcome

Identifies PowerShell commands that disable logging, commonly used in obfuscated or malicious scripts.

21

EXTERNAL ACCESS TO SENSITIVE DATA

Goal

Detect external access attempts to sensitive data using Windows security logs.

Example query

```
SecurityEvent
| where EventID == 4663 and ObjectType contains
"confidential"
```

Outcome

Detects access to sensitive files by external IPs or unauthorized accounts, signaling data exfiltration risks.

22

VPN LOGIN FROM UNUSUAL LOCATION (PALO ALTO)

Goal

Detect unusual VPN logins from suspicious or unknown geographic locations using Palo Alto VPN logs.

Example query

```
PaloAltoNetwork_CL
| where action == "vpn-login" and geo_location !=
"trusted_countries"
```

Outcome

Flags unusual VPN logins from unfamiliar regions, which could indicate compromised credentials.

23

CROWDSTRIKE DEVICE ISOLATION ALERTS

Goal

Detect any device isolation activity initiated by CrowdStrike as part of an incident response.

Example query

```
CrowdStrikeEvent_CL
| where EventType == "device-isolation"
```

Outcome

Provides alerts when CrowdStrike isolates a device, allowing SOC teams to investigate the root cause quickly.

24

SUSPICIOUS INBOUND CONNECTIONS (SYSMON)

Goal

Detect any device isolation activity initiated by CrowdStrike as part of an incident response.

Example query

```
Sysmon
| where EventID == 3 and DestinationPort == 3389
```

Outcome

Identifies inbound connections to RDP ports, commonly targeted for remote exploitation.

CONCLUSION

In conclusion, these queries provide robust detection capabilities across various attack vectors in Windows and network environments.

- Identify brute force attacks on Windows systems.
- Detect privilege escalation attempts using Sysmon logs.
- Flag suspicious DNS queries for potential exfiltration.
- Monitor unauthorized firewall configuration changes.
- Detect suspicious lateral movement in Windows environments.
- Alert on unusual VPN login attempts from unfamiliar regions.

Reach us at hi@haxsecurity.com

Security Consulting

- Risk assessment
- Security Architecture
- SOC Set up

Penetration testing

- Internal Pentest
- External Pentest
- Web App Pentest

Training and Courses

- SOC Training
- Certification Training
- Vendor-specific learning

Labs

- Hands-on Labs
- Career Path Labs
- Cyberrange for businesses