|  |  |
| --- | --- |
| [Document title]  [Document subtitle] | Abstract  [Draw your reader in with an engaging abstract. It is typically a short summary of the document. When you’re ready to add your content, just click here and start typing.]  [Author name]  [Course title] |

**Luis Irpum**

Contents

[1 Version History 2](#_Toc69736818)

[2 Background 2](#_Toc69736819)

[3 Approach 2](#_Toc69736820)

[4 In-Scope 3](#_Toc69736821)

[5 Out of Scope 3](#_Toc69736822)

[6 High-Level Architecture 3](#_Toc69736823)

[7 Data Sources 4](#_Toc69736824)

[8 Use-Cases 5](#_Toc69736825)

[9 Workbooks 7](#_Toc69736826)

[10 Implementation 8](#_Toc69736827)

[11 Prycing 8](#_Toc69736828)

[12 Appendix A – COMPANY Use-Cases 9](#_Toc69736829)

# Version History

This document has undergone the following iterations as listed in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Comments | Date |
| 0.1 | Luis Irpum | Document created | 07/11/2021 |

# Background

The Luis-Irpum\_AH Platform (COMPANY PLATFORM) consists of various applications and micro-services with a large amount of security data being generated in the form of events and logs. A security information event management (SIEM) and security orchestration automated response (SOAR) solution is required for alert detection, threat visibility and threat response.

Microsoft Azure Sentinel is a scalable, cloud native SIEM and SOAR solution that provides insight across the platform by collecting data, detecting threats, investigating threats using machine learning and responding to incidents in a reasonable timeframe.

This high-level design document forms part of the below Platform stories. These stories fall under the Azure Sentinel topic and detail the design elements of Azure Sentinel as a SIEM solution that are to be included in the PLATFORM :

# Approach

The following aspects of Sentinel will be covered in this design document:

**Data Sources:** To on-board Azure Sentinel, data sources need to be connected so that Sentinel can ingest the required security data for analysis. Azure Sentinel comes with several connectors available out-of-the-box that provide real-time integration. In addition to data connectors, diagnostic logs from Azure services can also be sent to Sentinel for analysis as well as third-party application logs via the syslog protocol.

**Analytics Rules (Use-Cases):** Analytics rules are the use-cases that create alerts indicating that a possible threat has occurred that needs to be investigated.

**Workbooks:** With the data sources connected to Sentinel, workbooks can be used to monitor data in the form of dashboards that provide an easy-to-use interface that a user can use to view an overall picture of specific topics.

# In-Scope

Sentinel will be deployed in two phases. Details of each phase along with the relevant owner can be found in ‘7 Data Sources’:

* **Phase 1 - Platform MVP**
  + Data sources: Out-of-the-box Azure-native only
  + Analytics Rules: Out-of-the-box Azure-native only
  + Workbooks: Out-of-the-box only where data sources have been connected as part of Phase 1
* **Phase 2 - (Date tbc)**
  + Data sources: non Azure-native services
  + Analytics Rules: Out-of-the-box rules for non Azure-native services

# Out of Scope

The following items are considered out of scope for Azure Sentinel under Epic AHBDB-2918:

* Custom Analytics Rules
* Playbooks
* Incident Response
* User and Entity Behaviour Analytics (UEBA)
* Hunting Queries

# High-Level Architecture

Architecture Image

# Data Sources

The following table lists how data will be ingested into Azure Sentinel along with who is responsible for connecting each data source and in what phase of the Sentinel deployment.

|  |
| --- |
| **Design Note** |
|  |
| Data sources labelled as ‘Preview’ are not backed by Microsoft SLA’s. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | Data Type | Data Source | Description | Owner | Phase | OOTB Use-Cases |
| 1 | Azure PaaS Services:   * Azure Kubernetes Service(AKS) * Azure Express Route * Azure Redis * Azure Container Registry * Azure Storage * Azure SQL Datawarehouse * Azure PostgreSQL * Azure Key Vault | Diagnostic Logs | Connection to all Azure PaaS services listed within the PLATFORM are achieved via diagnostic logs being sent to the underlying Log Analytics workspace.  This enables viewing log data in workbooks and using it to create custom alerts in order to improve investigations from within Sentinel. |  | Phase 1 | N/A |
| 2 | Azure Active Directory | Sentinel Connector | Ingests audit and sign-in data from Azure AD into Sentinel.   * Sign-in Logs collect information on user sign-in activities * Audit logs provide traceability of actions and changes performed within Azure AD. |  | Phase 1 | #009, #010, #011, #012,  #013, #014, #015, #016, #017, #018, #019, #021, #041, #042, #043 |
| 3 | Activity Log | Diagnostic Logs | Subscription log that provides insight into subscription-level events that occur in Azure including events from:     * Azure Resource Manager operational data * Service health events * Write operations taken on the resources in subscriptions * Status of activities performed in Azure |  | Phase 1 | #005, #006, #007 |
| 4 | Dynamics 365 **(Preview)** | Sentinel Connector | The Dynamics 365 Common Data Service (CDS) activities connector provides insight into admin, user, and support activities, as well as Microsoft Social Engagement logging events. |  | Phase 2 | N/A |
| 5 | Azure Defender (Security Centre) | Sentinel Connector | Alerts generated by Azure Security Centre are ingested into Azure Sentinel when it detects threats on resources. These threats originate from Azure Defender within Azure Security Centre. |  | Phase 1 | #001 |
| 6 | Azure Active Directory Identity Protection | Sentinel Connector | Provides a consolidated view of:   * At risk users * Risk events * Vulnerabilities      * Ability to remediate risk immediately and set policies to auto-remediate future events. |  | Phase 1 | #008, #020 |
| 7 | Security Events | Sentinel Connector | Streams all security events from Windows systems (servers and workstations, physical and virtual) to the Azure Sentinel workspace. |  | Phase 2 | #013, #022, #031, #032,  #033, #034,  #035, #036,  #037, #038 |
| 8 | Azure DDoS Protection | Diagnostic Logs | Connection to Azure DDoS Protection Standard logs is achieved via Public IP Address Diagnostic Logs.  This enables viewing log data in workbooks and using it to create custom alerts in order to improve investigations. |  | Phase 1 | N/A |
| 9 | Palo Alto | Sentinel Connector | Palo Alto Networks on Azure Sentinel provides more insights into Internet usage and will enhance its security operation capabilities. |  | Phase 2 | #039, #040 |
| 10 | Azure Web Application Firewall (WAF) / Application Gateway | Sentinel Connector | WAF protects applications from common web vulnerabilities such as SQL injection and cross-site scripting, and lets a user customize rules to reduce false positives.  This connector streams Microsoft Web application firewall logs into Azure Sentinel. |  | Phase 1 | #004 |
| 11 | Threat Intelligence Platforms **(Preview)** | * Sentinel Connectors (Threat Intelligence – TAXII & Threat intelligence Platforms. * Integration with existing COMPANY TI platforms | Sends threat indicators to Azure Sentinel from current Threat Intelligence Platforms (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, or other integrated applications. |  | Phase 2 | #022 |

# Use-Cases

The following table lists which out-of-the-box use-cases (analytics rules) will be enabled in Azure Sentinel. Please refer to ‘7 Data Sources’ as to when each use-case will be enabled based on the corresponding data source.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Category | Data Source | Sentinel Analytics Rule | Description |
| #001 | Defender | Sentinel Connector - Azure Defender | Create incidents based on Azure Security Center alerts | Create incidents based on all alerts generated in Azure Security Center |
| #002 | Syslog | Sentinel Connector - Syslog | New internet exposed SSH endpoints | Looks for SSH endpoints with a history of sign-ins only from private IP addresses are accessed from a public IP address. |
| #003 | Syslog | Sentinel Connector - Syslog | SSH - Potential Brute Force | Identifies an IP address that had 15 failed attempts to sign in via SSH in a 4-hour block over 24-hours. |
| #004 | WAF | Sentinel Connector - WAF | A potentially malicious web request was executed against a web server | Detects unobstructed Web Application Firewall (WAF) activity in sessions where the WAF blocked incoming requests by computing the ratio between blocked requests and unobstructed WAF requests in these sessions (BlockvsSuccessRatio metric). |
| #005 | Azure Activity | Diagnostic Logs – Azure Activity | Suspicious granting of permissions to an account | Identifies IPs from which users grant access to other users on azure resources and alerts when a previously unseen source IP address is used. |
| #006 | Azure Activity | Diagnostic Logs - Azure Activity | Suspicious number of resource creation or deployment activities | Indicates when an anomalous number of VM creations or deployment activities occur in Azure via the Azure Activity log. |
| #007 | Azure Activity | Diagnostic Logs - Azure Activity | Suspicious Resource deployment | Identifies when a rare Resource and Resource Group deployment occurs by a previously unseen Caller. |
| #008 | Active Directory | Sentinel Connector – Azure Active Directory Identity Protection | Create incidents based on Azure Active Directory Identity Protection alerts | Create incidents based on all alerts generated in Azure Active Directory Identity Protection |
| #009 | Active Directory | Sentinel Connector – Active Directory | Modified domain federation trust settings | This will alert when a user or application modifies the federation settings on the domain or Update domain authentication from Managed to Federated. |
| #010 | Active Directory | Sentinel Connector – Active Directory | Brute force attack against Azure Portal | Identifies evidence of brute force activity against Azure Portal by highlighting multiple authentication failures and by a successful authentication within a given time window |
| #011 | Active Directory | Sentinel Connector – Active Directory | Password spray attack against Azure AD application | Identifies evidence of password spray activity against Azure AD applications by looking for failures from multiple accounts from the same IP address within a time window |
| #012 | Active Directory | Sentinel Connector – Active Directory | Credential added after admin consented to Application | This query will identify instances where Service Principal credentials were added to an application by one user after the application was granted admin consent rights by another user. |
| #013 | Active Directory | Sentinel Connector – Active Directory  Sentinel Connector – Security Events | Failed Azure AD logons but success logon to host | Identifies a list of IP addresses with a minimum number (default of 5) of failed logon attempts to Azure Active Directory. Uses that list to identify any successful remote logons to hosts from these IPs within the same timeframe. |
| #014 | Active Directory | Sentinel Connector – Active Directory | Anomalous sign-in location by user account and authenticating application | An alert is generated for recent sign-ins that have location counts that are anomalous over last day but also over the last 7-day and 14-day periods. |
| #015 | Active Directory | Sentinel Connector – Active Directory | Attempts to sign in to disabled accounts | Identifies failed attempts to sign in to disabled accounts across multiple Azure Applications. Default threshold for Azure Applications attempted to sign in to is 3. |
| #016 | Active Directory | Sentinel Connector – Active Directory | Sign-ins from IPs that attempt sign-ins to disabled accounts | Identifies IPs with failed attempts to sign in to one or more disabled accounts signed in successfully to another account |
| #017 | Active Directory | Sentinel Connector – Active Directory | Distributed Password cracking attempts in Azure AD | Identifies distributed password cracking attempts from the Azure Active Directory Sign-in Logs. |
| #018 | Active Directory | Sentinel Connector – Active Directory | User added to Azure Active Directory Privileged Groups | This will alert when a user is added to any of the Privileged Groups |
| #019 | Active Directory | Sentinel Connector – Active Directory | First access credential added to Application or Service | This will alert when an admin or app owner account adds a new credential to an Application or Service Principal where there was no previous verify Key Credential associated. If a threat actor obtains access to an account with sufficient privileges and adds the alternate authentication material triggering this event, the threat actor can now authenticate as the Application or Service Principal using this credential. |
| #020 | Active Directory | Sentinel Connector – Azure Active Directory Identity Protection | Correlate Unfamiliar sign-in properties and atypical travel alerts | When a user has both an Unfamiliar sign-in properties alert and an Atypical travel alert within 20 minutes, the alert should be handled with a higher severity |
| #021 | Active Directory | Sentinel Connector – Active Directory | Successful logon from IP and failure from a different IP | Identifies when a user account successfully logs onto an Azure App from one IP and within 10 mins failed to logon to the same App via a different IP. This may indicate a malicious attempt at password guessing based on knowledge of the users account. |
| #022 | Threat Intelligence | Sentinel Connector – Threat Intelligence – TAXII  Sentinel Connector – Threat intelligence Platforms  Security Events | (Preview) TI map File Hash to Security Event | Identifies a match in Security Event data from any File Hash IOC from TI |
| #023 | Threat Intelligence | Sentinel Connector – Threat Intelligence – TAXII  Sentinel Connector – Threat intelligence Platforms | (Preview) TI map File Hash to CommonSecurityLog Event | Identifies a match in CommonSecurityLog Event data from any FileHash IOC from TI |
| #024 | General | Built-in - None Required | Multistage Attack Detection | Using Fusion technology based on machine learning, Azure Sentinel automatically detects multistage attacks by identifying combinations of anomalous behaviours and suspicious activities observed at various stages of the kill chain. |
| #025 | General | Built-in - None Required | Azure DevOps Agent Pool Created Then Deleted | As well as adding build agents to an existing pool to execute malicious activity within a pipeline an attacker could create a completely new agent pool and use this for execution. |
| #026 | General | Built-in - None Required | Azure DevOps Personal Access Token (PAT) misuse | This Alert detects whenever a PAT is used in ways that PATs are not normally used. |
| #027 | General | Built-in - None Required | Azure DevOps Audit Stream Disabled | Azure DevOps allow for audit logs to streamed to external storage solutions such as SIEM solutions. An attacker looking to hide malicious Azure DevOps activity from defenders may look to disable data streams before conducting activity and them re-enabling them after (so as not to raise data threshold-based alarms). |
| #028 | General | Built-in - None Required | High count of failed logons by a user | Identifies when 100 or more failed attempts by a given user in 10 minutes occur on the IIS Server. This could be indicative of attempted brute force based on known account information. This could also simply indicate a misconfigured service or device. |
| #029 | General | Built-in - None Required | High count of connections by client IP on many ports | Identifies when 30 or more ports are used for a given client IP in 10 minutes occurring on the IIS server. This could be indicative of attempted port scanning or exploit attempt at internet facing web applications. |
| #030 | General | Built-in - None Required | High count of failed attempts from same client IP | Identifies when 20 or more failed attempts from a given client IP in 1 minute occur on the IIS server. This could be indicative of an attempted brute force. This could also simply indicate a misconfigured service or device. |
| #031 | Windows Machines | Sentinel Connector – Security Events | Exchange OAB Virtual Directory Attribute Containing Potential Webshell | This query uses Windows Event ID 5136 in order to detect potential webshell deployment by exploitation of CVE-2021-27065. |
| #032 | Windows Machines | Sentinel Connector – Security Events | User account enabled and disabled within 10 mins | Identifies when a user account is enabled and then disabled within 10 minutes. |
| #033 | Windows Machines | Sentinel Connector – Security Events | Rare RDP Connections | Identifies when an RDP connection is new or rare related to any logon type by a given account today based on comparison with the previous 14 days. |
| #034 | Windows Machines | Sentinel Connector – Security Events | Starting or Stopping HealthService to Avoid Detection | This query detects events where an actor is stopping or starting HealthService to disable telemetry collection/detection from the agent. |
| #035 | Windows Machines | Sentinel Connector – Security Events | Gain Code Execution on ADFS Server via Remote WMI Execution | This query detects instances where an attacker has gained the ability to execute code on an ADFS Server through remote WMI Execution. |
| #036 | Windows Machines | Sentinel Connector – Security Events | RDP Nesting | Identifies when an RDP connection is made to a first system and then an RDP connection is made from the first system to another system with the same account within the 60 minutes. |
| #037 | Windows Machines | Sentinel Connector – Security Events | Security Event log cleared | Checks for event id 1102 which indicates the security event log was cleared. |
| #038 | Windows Machines | Sentinel Connector – Security Events | (Preview) Anomalous RDP Login Detections | This detection uses machine learning (ML) to identify anomalous Remote Desktop Protocol (RDP) login activity, based on Windows Security Event data |
| #039 | Palo Alto | Sentinel Connector – Palo Alto | Palo Alto - possible internal to external port scanning | Identifies a list of internal Source IPs (10.x.x.x Hosts) that have triggered 10 or more non-graceful tcp server resets from one or more Destination IPs which results in an "ApplicationProtocol = incomplete" designation. |
| #040 | Palo Alto | Sentinel Connector – Palo Alto | Palo Alto - potential beaconing detected | Identifies beaconing patterns from Palo Alto Network traffic logs based on recurrent timedelta patterns. |
| #041 | Active Directory | Sentinel Connector – Active Directory | Credential added after admin consented to Application | This query will identify instances where Service Principal credentials were added to an application by one user after the application was granted admin consent rights by another user. |
| #042 | Active Directory | Sentinel Connector – Active Directory | Full Admin policy created and then attached to Roles, Users or Groups | Identity and Access Management (IAM) securely manages access to AWS services and resources. Identifies when a policy is created with Full Administrators Access (Allow-Action:,Resource:). |
| #043 | Active Directory | Sentinel Connector – Active Directory | User added to Azure Active Directory Privileged Groups | This will alert when a user is added to any of the Privileged Groups |

|  |
| --- |
| **Design Note** |
|  |
| Playbooks and incident response are out-of-scope and therefore will not be configured when the use-cases are deployed. |

# Workbooks

The following table lists which out-of-the-box workbooks will be enabled in Azure Sentinel.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Description | Required Data Types / Connector | Owner |
| Azure AD Audit, Activity and Sign-in logs | Gain insights into Azure Active Directory Audit, Activity and Sign-ins with one workbook. This workbook can be used by Security and Azure administrators. | Azure Active Directory |  |
| Azure Activity | Learn about all user operations, trends, and anomalous changes over time.  This workbook provides the ability to drill down into caller activities and summarize detected failure and warning events. | Azure Activity |  |
| Azure DDoS Protection Workbook | This workbook visualizes security-relevant Azure DDoS events across several filterable panels. Offering a summary tab, metrics and a investigate tabs across multiple workspaces. | Azure DDoS Protection |  |
| ASC Compliance and Protection | Gain insight into regulatory compliance, alert trends, security posture, and more with this workbook based on Azure Security Center data. | Azure Security Centre |  |
| Azure Kubernetes Service (AKS) Security | See insights about the security of AKS clusters. The workbook helps to identify sensitive operations in the clusters and get insights based on Azure Defender alerts. | Azure Security Centre |  |
| Azure Key Vault Security | See insights about the security of Azure key vaults. The workbook helps to identify sensitive operations in the key vaults and get insights based on Azure Defender alerts. | Azure Security Centre  Azure Key Vault |  |
| Microsoft Web Application Firewall (WAF) - Azure WAF | Gain insights into Azure web application firewall (WAF) across various services such as Azure Front Door Service and Application Gateway. View event triggers, full messages, attacks over time, among other data. Several aspects of the workbook are interactable to allow users to further understand their data | Azure Web Application Firewall (WAF) |  |
| Security Alerts | Security Alerts dashboard for alerts in the Azure Sentinel environment. | Azure Security Centre |  |
| Incident overview | The Incident Overview workbook is designed to assist in triaging and investigation by providing in-depth information about the incident, including:   * General information * Entity data * Triage time (time between incident creation and first response) * Mitigation time (time between incident creation and closing) | Azure Security Centre |  |

# Implementation

Azure Sentinel is built on top of a Log Analytics workspace. For the PLATFORM , Sentinel will utilize the existing Log Analytics workspace within the subscription it is deployed so that data is not duplicated across multiple Log Analytics workspaces and operational costs are kept to a minimum. This will also ensure that reserved capacity discounts can be fully utilized in Log Analytics. For more information on see the Prycing section of this document.

Azure Sentinel will be implemented in the non-prod and production environments only. The initial deployment of Sentinel will be performed using the PLATFORM CI/CD pipeline which utilizes Terraform, Azure DevOps and Build Kite.

Terraform will be used to connect those data sources and use-cases to Sentinel that it supports. Other data sources, use-cases and workbooks will be configured via the Azure Portal.

# Prycing

Prycing for the products mentioned in this document can be found within this section. These costs are purely for estimation purposes.

**Please note:**

* All Prycing is for **one** subscription only
* Prycing **does not** include implementation charge (professional services)
* Prycing **does not** include any existing Log Analytics workspaces

It is important to note that the following data is ingested into Sentinel free of charge:

* Activity Logs
* Azure Security Centre

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Product | Description | Prycing | Assumed Quantity | COMPANY |
| **Azure Sentinel** | Azure SIEM / SOAR Solution  Prycing determined based on GB logs ingested per day into Azure Sentinel | $132 per day (including 50% capacity reservation discount on first 100GB) | 1 | $4,015.00 per month (est. 100GB per day based on data ingestion in existing Log Analytics workspace in non-prod) |
| **Total Charge per Year** | | | | **$48,180.00** |

# Appendix A – COMPANY Use-Cases

The following Excel files contain the current SIEM use-cases that COMPANY currently use on-premise. Deloitte and MSFT have looked to map these use-cases to Azure Sentinel and added appropriate commentary.

