

**Solution Architecture**

High Level Design

Programme Title: MTC Skysight Microsoft Sentinel

Project Title: MTC Skysight

Solution Title: Microsoft Sentinel

Date: 25 June 2025

Document Version Control

|  |  |
| --- | --- |
| Document Information | |
| Document Name | MTC Skysight Microsoft Sentinel |
| Client Name & Region | Capgemini UK Utility Services |
| Document Version | 1.0 |
| Published date of this version | 12 June 2025 |
| Effective date of this version | 25-06-2025 |
| Author | Akshay Kochar |
| Owner | Chetan |

|  |  |  |  |
| --- | --- | --- | --- |
| Revision History | | | |
| Document Version | **Date** | **Change Description** | **Author** |
| 1.0 | 16-01-2025 | Initial Draft | Akshay Kochar |
| 2.0 | 12-06-2025 | Update Draft | Chetan |
| 2.1 | 25-06-2025 | Final Draft | Chetan |

|  |  |  |  |
| --- | --- | --- | --- |
| Approvals History | | | |
| Document Version | **Date** | **Approved by** | **Rôle** |
|  |  |  |  |
|  |  |  |  |

**NOTICE TO THE RECIPIENT OF THIS PROPOSAL**

The information contained herein is the proprietary and confidential information of Capgemini, and its unauthorised disclosure or release would offer substantial benefit to competitors offering similar services. This material includes descriptions of methodologies and concepts derived through substantial research and development efforts undertaken by Capgemini. Therefore, the use or release of the information contained in this proposal for purposes other than for the evaluation of its contents as a basis for contract award is strictly prohibited unless required by law.

This proposal must not be reproduced (in whole or in part) by any means or transmitted without the prior written permission of Capgemini, except with respect to copies made or transmitted internally by you for the purpose of evaluating this proposal. All copies of this proposal (or any portion hereof) and any accompanying electronic copies should be returned to Capgemini or, at Capgemini’s option, destroyed at the end of the proposal evaluation period if Capgemini is not selected.

Neither submission by Capgemini nor your acceptance of this proposal, in whole or in part, constitutes acceptance by Capgemini of any contractual terms contained in your Request for Proposal, if any, and shall not form a binding agreement between the parties. Such an agreement shall only exist upon the execution of a mutually acceptable contract by both parties. Except as otherwise set forth in such a contract, Capgemini makes no representations or warranties to you in relation to the accuracy or completeness of any information or data provided in the proposal.

Copyright ©2024 Capgemini. All rights reserved.

**Table of Contents**

[**Table of Contents** 5](#_Toc183187069)

[1. Executive Summary 7](#_Toc183187070)

[2. Context 8](#_Toc183187071)

[2.1 References 8](#_Toc183187072)

[3. Scope 9](#_Toc183187073)

[3.1 In-Scope 9](#_Toc183187074)

[3.2 Out-of-Scope: 11](#_Toc183187075)

[3.3 License 11](#_Toc183187076)

[3.3.1 Licensing Model Overview 11](#_Toc183187077)

[3.4 Log Retention and Archiving 12](#_Toc183187078)

[3.5 Design Principle 12](#_Toc183187079)

[3.6 Risk Identified 13](#_Toc183187080)

[3.7 High Level Design Architecture 14](#_Toc183187081)

[3.8 Design Components 14](#_Toc183187082)

[3.9 Build Workflow 15](#_Toc183187083)

[3.10 Rules/Use cases 15](#_Toc183187084)

[3.11 Log Collection and configuration 15](#_Toc183187085)

[3.11.1 Log Source type by device type 17](#_Toc183187086)

[3.12 Authentication 17](#_Toc183187087)

[3.13 Connectivity and Access Details 19](#_Toc183187088)

[4. Roles and Responsibilities 21](#_Toc183187089)

[5. Support/Escalation Matrix 23](#_Toc183187090)

[6. Backup and Restore 24](#_Toc183187091)

[5.1 Backup 24](#_Toc183187092)

[5.2 Restore 24](#_Toc183187093)

[7. Disaster Recovery 25](#_Toc183187094)

[Appendix A : Document Control 27](#_Toc183187095)

[A.1 : Change History 27](#_Toc183187096)

[A.2 : Review and Approval 27](#_Toc183187097)

[A.3 : Distribution 27](#_Toc183187098)

[Appendix B : Use Cases: TBC 28](#_Toc183187099)

1. Executive Summary

The executive summary outlines the strategic initiative to migrate from IBM QRadar to Microsoft Azure Sentinel, aiming to leverage Sentinel's advanced capabilities for enhanced security analytics and threat management. This document provides a detailed migration framework, emphasizing efficient data transfer, system integration, and the adoption of Sentinel's AI-driven analytics. It addresses the technical and strategic considerations for a seamless transition, ensuring continuity in security operations and positioning the organization to better respond to evolving cybersecurity threats.

1. Context

2.1 References

|  |  |  |
| --- | --- | --- |
| **Reference ID** | **Title** | **Document Details** |
| **REF1** | Microsoft Sentinel Introduction | https://docs.microsoft.com/en-us/azure/sentinel/overview |
| **REF2** | Data Collection | https://docs.microsoft.com/en-us/azure/sentinel/best-practices-data |
| **REF3** | Prerequisites | https://docs.microsoft.com/en-us/azure/sentinel/prerequisites |
| **REF4** | Permissions/Roles | https://docs.microsoft.com/en-us/azure/sentinel/roles |

Table 1: References

1. Scope

This Microsoft Sentinel Implementation, tailored for the MTC Skysight, is focused on strengthening security measures through continuous monitoring and analysis of security events. Key objectives include ensuring compliance with industry regulations, integrating various log sources for comprehensive coverage, and implementing event normalization, correlation, and predefined use cases.

The configuration will cover aspects such as alerting mechanisms, incident response workflows, and user access management for the MTC Skysight. Integration with existing security tools is planned to enhance the overall security posture. The implementation will also include the development of customized reports and dashboards to provide the MTC Skysight with actionable insights.

Training sessions for security analysts and administrators are part of the plan, and comprehensive documentation will be maintained for ongoing operations. It's important to note that the scope is limited to the outlined objectives and functionalities for the MTC Skysight. Any deviations from this plan will require further evaluation and approval.

The following elements are in scope of this project:

3.1 In-Scope

|  |  |
| --- | --- |
| **Work Order** | **Description** |
| **Azure Sentinel Activation** | Pre-Activation Tasks:  **Prepare and Check Azure Subscription:**  Ensure that the Azure subscription is properly configured for Azure Sentinel activation.  Verify subscription details, limits, and prerequisites.  **Check and Prepare Log Analytics Workspace:**  Validate that the Log Analytics workspace is set up correctly.  Address any issues or configuration gaps.  **Develop and Deploy RBAC Permissions:**  Define RBAC (Role-Based Access Control) roles for MTC SKYSIGHT and Capgemini users to MTC SKYSIGHT subscription in Capgemini tenant.  Assign appropriate permissions for Azure Sentinel.  **Review Additional Permissions for Data Sources:**  Identify specific production data sources to be connected.  Ensure necessary permissions are granted for data collection.  **Azure Sentinel Activation:**  Activate Azure Sentinel in MTC SKYSIGHT created in Capgemini tenant:  Follow the Azure Sentinel activation process within the MTC SKYSIGHT in Capgemini tenant.  Configure data connectors for log collection.  **MSSP Management:**  **Configure MSSP Capabilities**:  Set up dashboards, queries, and hunting capabilities that cover multiple workspaces.  **Test Interconnection:**  Conduct thorough testing to ensure seamless interconnection between MTC SKYSIGHT and Capgemini tenants.  Validate the effectiveness of Azure Lighthouse for remote management.  **Approval and Documentation:**  Obtain approval from relevant stakeholders for the successful interconnection.  **Post-Activation Tasks:**  Monitor and Optimize:  Implement ongoing monitoring for Azure Sentinel health and performance.  Optimize configurations based on usage patterns and evolving security requirements.  **Incident Response Planning:**  Develop an incident response plan for handling security incidents detected by Azure Sentinel.  Ensure that MTC SKYSIGHT and Capgemini teams are familiar with the response procedures.  **Training and Knowledge Transfer:**  Provide training sessions for Capgemini teams supporting MTC SKYSIGHT on Azure Sentinel features and best practices. |
| **Azure Sentinel Deployment (Architecture, Implementation)** | Tasks and activities related to the data collection from log sources in MTC SKYSIGHT on Azure Sentinel from On-Prem. |
| **Log Collection (including technical action on Log sources)** | Log collection will encompass collection of data from Cisco Nexus, Cisco IOS, Dell EMC Switch, F5 Networks BIG-IP LTM and Fortinet FortiGate Security Gateway. The process will involve thorough testing and approval of log collection, ensuring compatibility with various log formats and employing appropriate log collection methods.  Post log collection, the focus will shift to testing and documentation. This phase includes rigorous testing of the collected logs, validating their accuracy and completeness. Additionally, documentation will be generated to cover the entire log collection process. As part of this documentation effort, parser specifications will be created to outline the specific parsing requirements and formats for the collected logs, ensuring clarity and consistency in log processing. |
| **Rules Definition & Integration & Deployment** | Capgemini will make sure the analytical rules are enabled to ensure a foundational level of detection. The coverage of these rules is estimated to link to MTC SKYSIGHT's risks associated with Mitre ATT&CK Tactics. Each rule will be meticulously configured, optimized, and thoroughly tested to enhance effectiveness.  The implementation will include SOAR (Security Orchestration, Automation, and Response) Playbooks with a specific focus on OTX (Open Threat Exchange) threats and GEO location automated lookup. These playbooks will be designed to streamline response actions and enhance the automated handling of threats associated with OTX intelligence and geographical locations. |
| **Process Definition (remediation catalogue initialization…) + Governance organization (dashboard/reports)** | Capgemini will take the initiative to define and develop a communication process that facilitates seamless interaction among MTC SKYSIGHT, Capgemini outsourcing activities, and the SOC (Security Operations Center). The objective is to establish robust communication channels that enhance collaboration and ensure effective information flow.  The process development will involve close collaboration with MTC SKYSIGHT team leaders to identify key communication requirements and nuances. Through joint efforts, all processes will be meticulously identified, defined, and documented in a dedicated process notebook. This documentation will serve as a comprehensive reference for all stakeholders involved, fostering clarity and consistency in communication practices across the teams. |

3.2 Out-of-Scope:

The following aspects are explicitly excluded from the scope of this document:

* Automating Deployment of additional Azure Resources and Services

Future Enhancements:

Future enhancements or features that are not part of the current development cycle will be considered as part of documentation review on a frequency agreed.

Third-Party Systems:

Detailed specifications of third-party systems or components that integrate with Sentinel are considered out of scope. This document will provide an overview of integration points but will not delve into the specifics of third-party implementations.

Operational Procedures:

Operational procedures, such as deployment instructions, maintenance tasks, and troubleshooting guides, are not within the scope of this document.

3.3 License

The chosen licensing model for this Azure Sentinel deployment is the \*\*Enterprise Agreement (EA)\*\*.

3.3.1 Licensing Model Overview

Enterprise Agreement (EA):

* As an MSSP, Capgemini have opted for the EA licensing model for this Microsoft Sentinel deployment on behalf of the MTC SKYSIGHT.
* The EA model is tailored for large-scale service providers managing predictable workloads, offering significant discounts based on the volume of Azure services consumed across multiple customers.
* This approach allows us to offer a more structured and cost-effective service to our customers, ensuring committed and optimized Azure service consumption.

Considerations:

* The EA model provides a more structured and potentially cost-effective approach for organizations with predictable workloads.
* Discounts within the EA model is based on the overall consumption of Azure services and MTC SKYSIGHT agreement with Microsoft.
* The commitment and predictability associated with EA may align with the organization's long-term strategic goals.

3.4 Log Retention and Archiving

|  |  |
| --- | --- |
| **Storage Group** | **Duration** |
| Online - Searchable data | 3 months |
| Offline - Archive | 6 months |

3.5 Design Principle

|  |  |  |
| --- | --- | --- |
| **Decision ID** | **Decision Description** | **Architecture/Design Implication** |
| **DD1** | Solution to be deployed for Centralized Log Collection | Aggregate logs and events from diverse sources into a centralized Log Analytics Workspace. |
| **DD2** | Solution to Event Normalization | Standardize event formats and normalize data from different sources. |
| **DD3** | Correlation and Aggregation | Develop correlation rules to identify patterns and relationships between events using Analytical rules |
| **DD4** | Data Retention Policies | Establish clear data retention policies aligned with regulatory requirements. |
| **DD5** | Data Encryption | Use encryption for data in transit and at rest to protect sensitive information |
| **DD6** | Incident Response Integration | Integrate with incident response processes and tools for effective incident handling |
| **DD7** | Customization and Flexibility | Allow customization of dashboards, reports, and alerting rules to meet specific needs |
| **DD8** | Regular Auditing and Monitoring | Implement auditing capabilities and continuously monitor system health and performance |
| **DD9** | Training and Documentation | Provide training for administrators and maintain comprehensive system documentation |

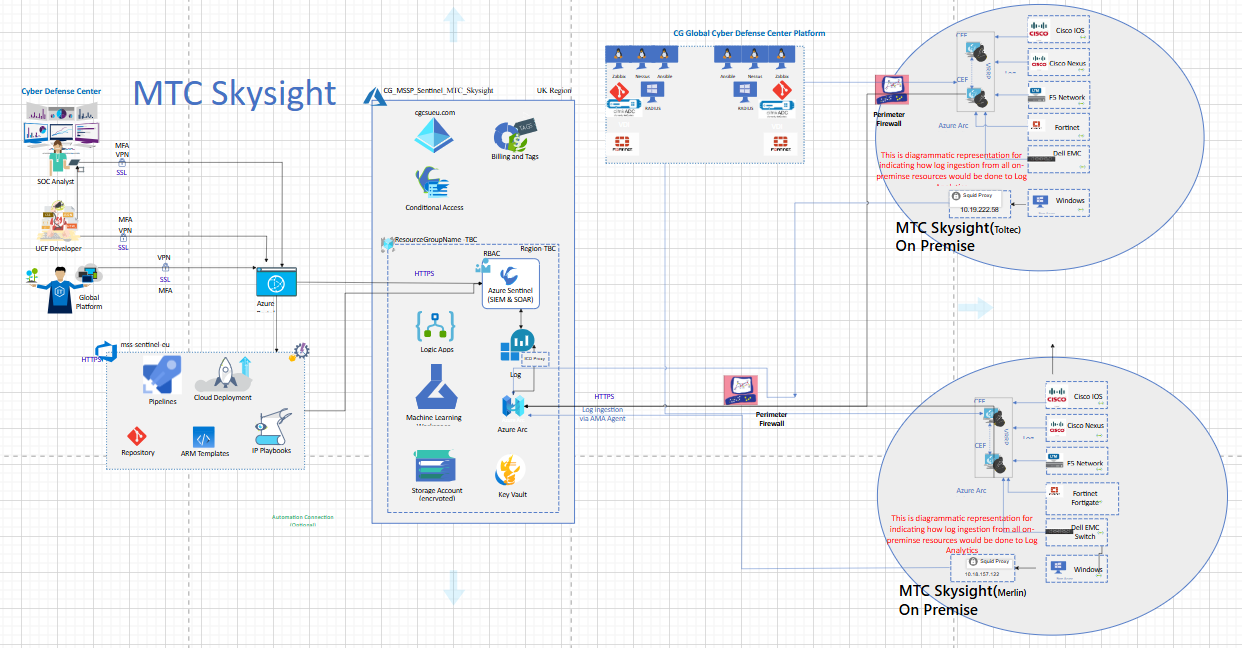
3.6 Risk Identified

For the above suggested solution to maintain resilience which is important for our approach to work without any issues, considering Linux server is created in on-prem environment. If the active server goes down/crashes, the backup/standby server will start ingesting the data it receives once the active server stops working. However, the data that was sent to the active server may not be completely forwarded to Sentinel before the server crash (as AMA maintains a queue for forwarding to Sentinel).

The solution suggested above is therefore possible but there may be loss of events (specially events in the AMA agent forwarding queue on active server) while switching to passive/backup server.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk ID** | **Risk / Configuration Requirement** | **Description** | **Mitigation** |
| **RS 1** | **Event Data Loss During Failover** | During failover, events in the queue on the active server may not be forwarded to Sentinel. | Implement periodic queue flushing and regular failover testing to minimize data loss during switchover. |
| **RS 2** | **Lack of Common Storage for Event Logs** | Without shared or SAN storage, separate logs on each server could lead to inconsistencies. | Use centralized logging solutions or alternative storage options, if available, to ensure log continuity across both servers. |
| **RS 3** | **Automated Failover Configuration** | Failover should occur automatically to minimize downtime. | Use clustering tools to automate failover between active and standby servers, ensuring uninterrupted log forwarding to Sentinel. |
| **RS 4** | **Access Management and Security** | Secure access to servers is critical to prevent unauthorized actions. | Control access to Linux servers via Capgemini’s tools and restrict server access to trusted IPs only, using SSH and firewall configurations for security. |
| **RS 5** | **Monitoring and Alerts** | Servers need to be monitored for performance and failures. | Set up monitoring tools to track server health, resource usage, queue size, and network connectivity. Configure alerts to notify teams in case of failure or issues. |

3.7 High Level Design Architecture



3.8 Design Components

**Log Analytics Workspace (Event storage and retention)**

* Log Analytics workspace is a SaaS service used for storing and analysing logs. The analysis can be performed using KQL queries on the logs.
* The log analytics workspace is connected with Azure Sentinel solution hence the free retention for logs in log analytics workspace is 3 months.

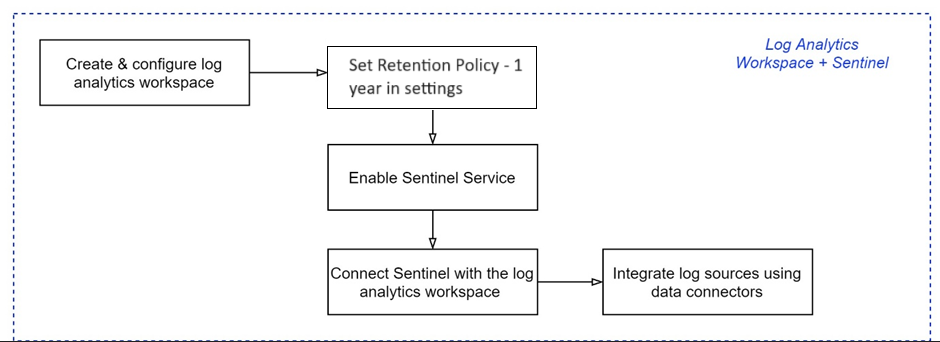
**Azure Sentinel (SIEM)**

* Azure Sentinel SaaS service can be enabled only after creating a Log Analytics Workspace for storage of the logs being sent to Sentinel for analysis. Sentinel stores the alerts and incidents it generates in the Log Analytics Workspace.
* Activities that will be performed by Azure Sentinel:
  + Detect suspicious actions and raise alerts/incidents based on the events from the Azure Active Directory.
  + Raise incidents from alerts generated by Microsoft services like ASC, MCAS and ATP which are monitoring the Virtual machines, networks and hybrid workloads deployed in the cloud tenant.
  + Perform scheduled scans based on custom rules/queries to detect any suspicious activity/behaviour in the cloud resources.

**Long term storage – LA workspace/ADX/Storage Account**

* We have different options for configuring the long-term retention of logs.
* The Logs stored in Log analytics workspace are free for 3 months’ duration.
* After 3 months, the retention can be upgraded in Log analytics workspace which will incur additional pricing. (MTC SKYSIGHT has opted for a total retention of 9 months)

3.9 Build Workflow

****Creating Log Analytics Workspace

* A log analytics workspace is required to collect and analyse logs independently as well as in sentinel.
* The logs being sent from the sentinel data connectors are also stored in log analytics workspace. Also, the incidents generated by sentinel and the alerts sent by Microsoft security services are all stored in the log analytics workspace.
* Log Analytics workspace can be accessed by searching it in the portal.

3.10 Rules/Use cases

* Rules/Use cases for covering the log sources will be created using KQL. There will be use of existing rule templates in sentinel + custom rules created from scratch based on the log sources.

3.11 Log Collection and configuration

**Other Application logs**

* Other Applications like firewall, network devices, application gateways, WAF, etc. can be integrated with sentinel using syslog/CEF forwarders and the logs can be parsed at log analytics workspace.

# 

**Syslog server requirement**

|  |  |  |
| --- | --- | --- |
| **Category** | **Requirement** | **Details** |
| Hardware Requirements | CPU and RAM | Minimum of 4 CPU cores and 8 GB RAM |
|  | Performance | Supports up to 10,000 events per second (EPS) using the rsyslog daemon |
|  | Storage | 200GB |
| Operating Systems | Ubuntu | Ubuntu 22.4 LTSR |
| Daemon Versions | rsyslog | Version 8 |
| Software Packages | Python | Version 3 (Check with python --version or python3 --version) |
|  | GNU Wget | Must be installed |
| Syslog RFC Support | Supported Standards | Syslog RFC 3164, Syslog RFC 5424 |
| Configuration Requirements | Permissions | Elevated permissions (sudo) required |
|  | Pre-Installation Requirement | Linux machine must not be connected to Azure workspaces before agent installation |
| Data Management | Microsoft Sentinel Integration | Workspace ID and Primary Key needed, found under Agents management in settings |

**Note**

* All operating systems listed are assumed to be x64. x86 isn't supported for any operating system.

The following document describes how the support will be provisioned for this syslog server.



**Bandwidth Requirements (estimated):**

The calculation of bandwidth is done using the following:

Data (kbps) = [EPS (max) \* data size (max in bytes) \*8 (bytes-to-bits) / 3 (assumed compression)] / 1000 (bits-to-kbits)

Data (Mbps) = Data (kbps) / 1000 \* (1+ packetization loss)

Packetization efficiency using TCP transport takes account of the following:

1. Packet Loss Rate

2. Transmission Efficiency

3. Retransmission Overhead

4. Impact on Throughput

We have assumed a maximum transmission loss of the above at 20%. So, added this loss to the data to be transported. This will create a multiplier of 1+packetization loss.

Rounding up the Data (Mbps) to the next integer value and following would be the calculated internet bandwidth requirement, based on the assumptions and calculation above.

EPS (max estimated as avg. eps is 161.37) = 162, Data(bytes)=2048, Compression=3:1, Packetization loss=20%

Data (Mbps) = ((162 \* 2048 \* 8) /3 / 1000 / 1000) \*(1+0.2) = 1.061 Mbps

Current internet bandwidth allocated as per data from Qradar = 1.0 Mbps.

The assumption here is that this traffic remains constant over time and have not allowed for any growth, but this should be met within the calculation because of the rounding up.

As per Microsoft, the data compression is done as follows:

***“AMA uses compressions capabilities built on top of the zlib library and utilizes level 3. On average this leads to a 1:10 compression but really depends on the data being transferred.***

***We have observed compression ratio in AMA to be typically between 2:1 and 5:1, with a theoretical maximum at 1032:1, but really depends on the data.”***

3.11.1 Log Source type by device type

* The data provided outlines a comprehensive inventory of log source types from MTC SKYSIGHT, categorized by their corresponding device types, along with the quantity of each log source type available. This inventory spans a diverse range of device types such as firewalls, network devices and more. It includes technologies and platforms like Cisco IOS, Cisco Nexus, Dell Switch, FortiGate Security Gateway and F5 Networks BIG-IP.

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Log Source Type** | **Device Type** |
| 1 | Cisco IOS | Network Device |
| 2 | F5 Networks BIG-IP LTM | Firewall |
| 3 | Fortinet FortiGate Security Gateway | Firewall Gateway |
| 4 | Cisco Nexus | Network Device |
| 5 | Dell Switch | Network Device |
| 6 | Microsoft Windows Security Event Log | Windows |

3.12 Authentication

* Capgemini acts as a Managed Security Service Provider (MSSP) for MTC SKYSIGHT, with the task of managing and securing Microsoft Sentinel instances hosted within MTC SKYSIGHT Azure environment, the approach incorporates strategic use of Azure Active Directory (AD), Multi-Factor Authentication (MFA), granular access controls etc. for seamless, secure access management.

Please find below high-level diagram:



* **Implementation of Multi-Factor Authentication (MFA):** To safeguard against unauthorized access, Capgemini enforces MFA for all users accessing the Microsoft Sentinel environment. This adds a critical layer of security, ensuring that access to MTC SKYSIGHT's resources is protected by both a password and a second form of verification.
* **Granular Access Control via Azure AD Groups**: Capgemini utilizes Azure AD groups to delineate access levels across MTC SKYSIGHT's resources. This method ensures that Capgemini's team members are granted access rights that precisely match their operational roles and responsibilities, adhering to the principle of least privilege.
* **Precise IAM Role Assignments:** Capgemini AD team assigns specific Identity and Access Management (IAM) roles to the appropriate Azure AD groups. This step is crucial for managing permissions related to administration, monitoring, and development within Microsoft Sentinel, ensuring that access is both necessary and appropriate for the tasks at hand.
* **Subscription Access Management:** Essential to the operational efficacy, Capgemini's SOC Analyst must have access to the Azure Resource group where MTC SKYSIGHT Sentinel is configured. This enables them to manage and monitor the Microsoft Sentinel environment effectively.

3.13 Connectivity and Access Details

* Azure Sentinel can be accessed after logging into Azure portal. The user must have roles to access Azure portal and Sentinel.
* Since it is a SaaS service, there is no requirement of opening flows. All the services are accessible using the Azure portal itself provided the user who is trying to access the service has the access for the service which can be provided using RBAC (Role Based Access Control).
* Only Security events will be enabled on the endpoints and forwarded to sentinel for correlation alerts generation.

|  |  |  |  |
| --- | --- | --- | --- |
| Source | Destination | Function | Protocol/ Port |
| Cisco IOS | Syslog Collector-IP | Receiving syslog/CEF messages from logged devices in the internal environment. | TCP/UDP 514 |
| F5 Networks BIG-IP LTM | Syslog Collector-IP | Receiving syslog/CEF messages from logged devices in the internal environment. | TCP/UDP 514 |
| Fortinet FortiGate Security Gateway | Syslog Collector-IP | Receiving syslog/CEF messages from logged devices in the internal environment. | TCP/UDP 514 |
| Cisco Nexus | Syslog Collector-IP | Receiving syslog/CEF messages from logged devices in the internal environment. | TCP/UDP 514 |
| Dell Switch | Syslog Collector-IP | Receiving syslog/CEF messages from logged devices in the internal environment. | TCP/UDP 514 |

Network access for local DC internet for VM connection to Azure:

|  |  |  |  |
| --- | --- | --- | --- |
| Source | Destination | Function | Protocol/ Port |
| Azure Arc Requirements | Microsoft Azure Arc | Outbound connection for Azure Arc onboarding to Microsoft Azure via HTTPS with TLS encryption using URL whitelisting:   * download.microsoft.com * packages.microsoft.com * login.microsoftonline.com * \*login.microsoft.com * pas.windows.net * management.azure.com * \*.his.arc.azure.com * \*.guestconfiguration.azure.com * guestnotificationservice.azure.com * \*.guestnotificationservice.azure.com * azgn\*.servicebus.windows.net * \*.servicebus.windows.net * \*.blob.core.windows.net * dc.services.visualstudio.com * \*.uksouth.arcdataservices.com * www.microsoft.com/pkiops/certs | TCP 443 |
| Syslog/CEF Collector | Microsoft Sentinel | Outbound connection for Syslog/CEF forwarding to Microsoft Sentinel via HTTPS with TLS encryption using URL whitelisting:   * global.handler.control.monitor.azure.com * uksouth.handler.control.monitor.azure.com * a033e055-7c9b-462e-9058-5f965bf9c246.ods.opinsights.azure.com * management.azure.com | TCP 443 |
| ICD Proxy  10.18.157.122 (Merlin)  10.19.222.58 (Toltec) | To Provide Internet Access to Infra Devices | * global.handler.control.monitor.azure.com * uksouth.handler.control.monitor.azure.com * uksouth.prod.la.ingest.monitor.core.windows.net * a033e055-7c9b-462e-9058-5f965bf9c246.ods.opinsights.azure.com | TCP 443 |

Network details for VPN connection for ICD support and implementation:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Port** | **Protocol** | **Service** |
| 62.145.57.1 62.145.58.1 | 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | 22 | TCP | SSH |
| 62.145.57.1 62.145.58.1 | 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | N/A | ICMP | ICMP (PING) |
| 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | Internet for SaaS | 443 | TCP | HTTPS |
| 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | Provided by local resources | 123 | UDP | NTP |
| 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | Provided by local resources | 53 | TCP/UDP | DNS |
| 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | 62.145.57.5 62.145.58.5 | 1812-1813 | UDP | RADIUS |
| 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | 62.145.57.6 62.145.58.6 | 3142 | TCP | Ubuntu Patching Repository |
| 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | 62.145.57.7 62.145.58.7 | 8834 | TCP | Tenable Nessus Agent |
| 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | 62.145.57.8 62.145.58.8 | 10050-10051 | TCP | Zabbix Agent - bidirectional |
| 62.145.57.8 62.145.58.8 | 10.20.10.181 10.20.10.182 10.16.10.181 10.16.10.182 | 10050-10051 | TCP | Zabbix Agent - bidirectional |

Network details for local DC internet connection for VM support:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Port** | **Protocol** | **Service** |
| Syslog Servers | Internet access for Trend Micro | 443 | TCP | HTTPS |
| ICD Proxy  10.18.157.122 (Merlin)  10.19.222.58 (Toltec) | Internet access for Linux and clamav updates | 80;443;  udp-53;  udp-123 | Both | HTTP; HTTPS DNS NTP |

Proxy Configuration:

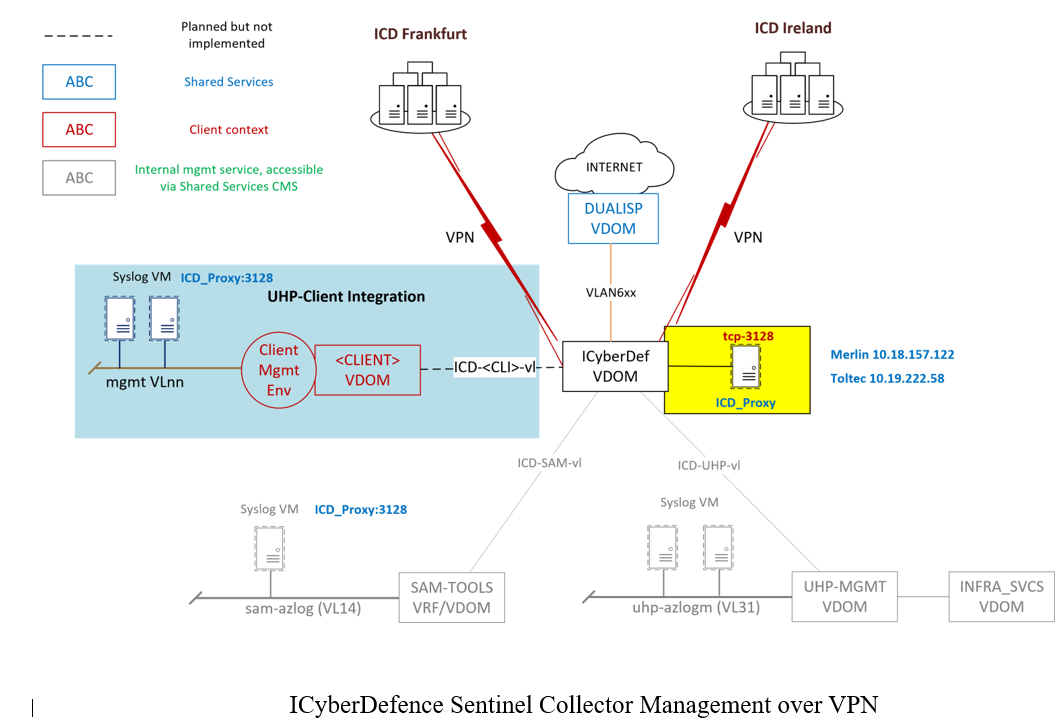
To enable centralized monitoring and threat detection, network devices were onboarded to Microsoft Sentinel using on-premises Syslog servers. These Syslog servers, located in a secure internal network without direct internet access, were configured to forward logs to Sentinel via a proxy setup. A NAT (Network Address Translation) IP was assigned to each Syslog server to facilitate secure and identifiable communication through proxy.

This architecture ensures:

* Secure log forwarding from isolated environments.
* Compliance with network segmentation policies by avoiding direct internet exposure.
* The configuration supports scalable and secure integration of network infrastructure into Sentinel for enhanced visibility and threat analytics.

The following IP addresses need to be included for this ICD Proxy configuration on each site.  The same IP is used for all clients.

|  |  |  |  |
| --- | --- | --- | --- |
| **Location** | **Proxy IP** | **Proxy port** | **Service** |
| Merlin | 10.18.157.122 | tcp-3128 | http; https |
| Toltec | 10.19.222.58 |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S.no | Activity Description | SOC/ ICD Team | MTC Team | UHP Network Team | Infra\_UK |
| 1 | Configuring Proxy servers | I | C, I | C, I | R, A |
| 2 | Managing the Proxy Servers | I | C, I | C, I | R, A |
| 3 | Network Configuration Related to Proxy | I | C, I | R, A | C, I |

1. Roles and Responsibilities

Following is the RACI (Responsible-Accountable-Consulted-Informed) matrix that describes the responsibilities of the Parties in the provision of the Services. For each of the below activities, the following indicators will identify the part’s role in the performance of the specific task for a given service activity.

* An “R” is placed in the column under the party who is responsible for completing a task.
* An “A” is placed in the column under the party who is accountable for a task’s accurate completion.
* A “C” is placed in the column under the party who is consulted for their technical expertise when performing a task.
* An “I” is placed in the column under the party who must be informed after the decision has been made regarding a task.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sr. No. | Activity Description | SOC/ ICD Team | Client/  Network Team | Security Manager | Support /Resolver Team |
| 1 | Providing business objective for correlation rules and reports development | C, I | R, A | C, I | Not Applicable |
| 2 | Sign-off on use-cases (rules and reports) mapping with business objectives. | C, I | R, A | C, I | Not Applicable |
| 3 | Developing and implementing correlation rules and reports based on MTC SKYSIGHT provided business objectives. | R, I, A | C | C, I | Not Applicable |
| 4 | Provide list of log sources to be integrated with Sentinel. | I, C | R, A | R | C |
| 5 | Reconciliation of log sources for integration. | R, A | R, C, I | R, C, I | Not Applicable |
| 6 | Identifying the log sources requiring custom parser development and its integration. | R, A | C, I | C, I | Not Applicable |
| 7 | Monitoring of Log sources and check log receiving status on Sentinel console. | R, A | I, C | I, C | Not Applicable |
| 8 | 24x7 Monitoring and Reporting of Security Incident | R, A | I, C | I, C | Not Applicable |
| 9 | Provide Configuration of logging level on monitored devices. | I, C | R, A | I, C | C |
| 10 | Store log data in secure manner and retrieval of data if a request is made (within the retention period). | R, A, C | I | R, C, I | Not Applicable |
| 11 | Approval of the configuration change | C, I | R, A | I, C | I, C |
| 12 | In-scope log source configuration. | C, I | R, A | C, I | R |
| 13 | Use Case and Playbook development/deployment | R, A | C, I | C, I | Not Applicable |
| 14 | Incident Response | R, C | C, I | R, A, C, I | R, I |
| 15 | Incident Resolution | R, C | C, I | R, A, C, I | R, I |
| 16 | Modification to existing security components/posture | C, I | C, I | R, A, C, I | I |
| 17 | OS level support (including patching) and monitoring of syslog server | R, A, C | I | Not Applicable | Not Applicable |

|  |  |  |
| --- | --- | --- |
| Support/Escalation MatrixCompany | Role/Team | Name |
| Capgemini | Network Team | DL IN SkySight Network <skysightnetwork.in@capgemini.com> Network TL: shaktidutta.swain@capgemini.com |
| Capgemini | Platform Team DL and Team Lead | DL IN SkySight Platform <skysightplatform.in@capgemini.com>;  Platform TL: herold.koli@capgemini.com |
| Capgemini | Infra Team Lead | Karmalkar, Prathmesh (prathmesh.karmalkar@capgemini.com) |
| Capgemini | Change Manager | DL GLOBAL CnR Change and Release [cnrchangeandrelease.global@capgemini.com](mailto:cnrchangeandrelease.global@capgemini.com) |
| Capgemini | SDM – CG MTC Skysight | Spencer, Sinead (sinead.spencer@capgemini.com) |
| Capgemini | Security Manager (MTC Skysight – Utility Services) | Porter, John (john.a.porter@capgemini.com) |
| Capgemini | Lead – SOC MSSP (Azure Sentinel) | Jamadar, Mahammadshareef (mahammadshareef.liyakhatali-jamadar@capgemini.com) |
| Capgemini | UHP Network Team Lead | Sarkar, Bishwanath (bishwanath.sarkar@capgemini.com) |
| Capgemini | Infra\_UK Team | Mudaliar, Krishnan (krishnan.mudaliar@capgemini.com) |
| Capgemini | Escalation Manager – SOC MSSP (Azure Sentinel) | Shabbirsab Mulla (shabbirsab.mulla@capgemini.com) |

1. Backup and Restore

Within any production environment, Backup and Recovery is the basic Business Continuity feature that is used. This solution makes use of mostly SaaS tools or managed Azure services which are highly available and reliable. The availability and data reliability are guaranteed and governed by service agreement with Microsoft. However, unplanned service outages may occur. Hence this solution leverages geo-redundant storage accounts (GRS) and Server resilience so that management platform log data is copied to a second region and backup server respectively.

5.1 Backup

As log data for management platform is stored in geo-redundant storage account (GRS) under MTC SKYSIGHT Azure Subscription, which highly available and durable, hence there is no exclusive backups required.

5.2 Restore

As there are no backups, the restore request are not under considerations. The geo-redundant storage account (GRS) is configured with data retention period of one year for MTC SKYSIGHT. In case there is failure in primary region and endpoints are available, data can be access, read, recover, and restore to another storage account from secondary endpoint.

1. Disaster Recovery

This solution use Microsoft Sentinel and other azure services which highly available, SaaS in nature and managed by Microsoft, there is no disaster recovery and test, or failover procedure required.

All the log data is stored in geo-redundant storage accounts (GRS) which provides built-in protection of data using managed replication to secondary region.

Azure Storage supports account failover for geo-redundant storage accounts. With account failover, one can initiate the failover process for their storage account if the primary endpoint becomes unavailable. The failover updates the secondary endpoint to become the primary endpoint for this storage account. Once the failover is complete, log analytics can begin writing to the new primary endpoint.

**Geo-redundant storage (GRS)** or **geo-zone-redundant storage (GZRS)** copies your data asynchronously in two geographic regions that are at least hundreds of miles apart. If the primary region suffers an outage, then the secondary region serves as a redundant source for your data. You can initiate a failover to transform the secondary endpoint into the primary endpoint.

**Read-access geo-redundant storage (RA-GRS)** or read-access geo-zone-redundant storage (RA-GZRS) provides geo-redundant storage with the additional benefit of read access to the secondary endpoint. If an outage occurs in the primary endpoint, applications configured for read access to the secondary and designed for high availability can continue to read from the secondary endpoint. Microsoft recommends RA-GZRS for maximum availability and durability for your applications.

SOC and Platform Team will regularly check the [[Azure Service Health Dashboard](https://azure.microsoft.com/status/)](https://azure.microsoft.com/status/) to track the health and status of Azure Storage and other Azure services. If there are any failures or errors, the same could be picked up using alerts in monitoring.

Customer-managed account failover enables you to fail your entire storage account over to the secondary region if the primary becomes unavailable for any reason. When you force a failover to the secondary region, clients can begin writing data to the secondary endpoint after the failover is complete. The failover typically takes about an hour.

Under normal circumstances, a client writes data to an Azure Storage account in the primary region, and that data is copied asynchronously to the secondary region. The following image shows the scenario when the primary region is available:

Diagram

Description automatically generated

*Figure 19: GRS Storage Account Async Replication*

If the primary endpoint becomes unavailable for any reason, the client is no longer able to write to the storage account. The Platform Team or customer initiates the account failover to the secondary endpoint. The failover process updates the DNS entry provided by Azure Storage so that the secondary endpoint becomes the new primary endpoint for your storage account, as shown in the following image:

Diagram

Description automatically generated

*Figure 20: GRS Storage Account Failover to Secondary*

Write access is restored for geo-redundant accounts once the DNS entry has been updated and requests are being directed to the new primary endpoint. Existing storage service endpoints for blobs, tables, queues, and files remain the same after the failover. Because data is written asynchronously from the primary region to the secondary region, there is always a delay before a write to the primary region is copied to the secondary region. If the primary region becomes unavailable, the most recent writes may not yet have been copied to the secondary region.

Document Control

* 1. Change History

|  |  |  |  |
| --- | --- | --- | --- |
| **Publish Version** | **Date** | **Changes** | **Updated by** |
|  |  |  |  |

* 1. Review and Approval

|  |  |  |  |
| --- | --- | --- | --- |
| **Function** | **Name** | **Role** | **Approval Email Attachment** |
| Client |  |  |  |
|  |  |  |  |
| Capgemini |  |  |  |
|  | Ravi Amardeep Kucheria | Senior Architect |  |
|  |  |  |  |
|  |  |  |  |

* 1. Distribution

|  |  |  |
| --- | --- | --- |
| **Function** | **Name** | **Role** |
| Client |  |  |
|  |  |  |
| Capgemini |  |  |
| Architecture | Ravi Amardeep Kucheria | Senior Architect/Author |

Use Cases: TBC

|  |  |  |
| --- | --- | --- |
| **Sr No** | **Use case name** | **Log source type** |
| 1 | UC-IA.CA-357 - All - Concurrent Logins from Multiple Sources | TBC |
| 2 | UC-IM-497 - All - Syslog Service Stopped | TBC |
| 3 | UC-IM-497 - All - Syslog Stopped and Has Not Been Restarted | TBC |
| 4 | UC-IM-506 - Windows - Windows Security Log full | TBC |
| 5 | UC-DE-498 - Windows - System Time Changed - Windows | TBC |
| 6 | Unauthorized Access Exploit Followed by Suspicious Host Activity Chained-GSOC | TBC |
| 7 | UC-CC-245 - EPP - Multiple Exploit Types Against Single Destination | TBC |
| 8 | UC-IA.EX-368 - IPS - Exploits Events with High Magnitude Become Offenses | TBC |
| 9 | UC-IM-255 - EPP - Possible Local Worm Detected | TBC |
| 10 | UC-DE-170 - DB - Attempted Configuration Modification by a remote host | TBC |
| 11 | UC-PR-749 - Windows - Account Added to a Privileged Group | TBC |
| 12 | UC-IA-178 - DB - Remote Login Success | TBC |
| 13 | UC-DE-505 - Windows - Windows Event Logging Service Shut down | TBC |
| 14 | UC-CA -1187 - AWS - AWS Cloud: Multiple Console Login Failures from Different Source Ips | TBC |
| 15 | UC-IM-441 - All - Log Source Stopped Reporting - Medium Severity | TBC |
| 16 | UC-IM-440 - All - Log Source Stopped Reporting - Low Severity | TBC |
| 17 | UC-IA-1021 - X-Force Premium: Mail Server Sending Mail to Servers Categorized as SPAM | TBC |
| 18 | UC-IA-1022 - X-Force Premium: Non-Mail Server Sending Mail to Servers Categorized as SPAM | TBC |
| 19 | Suspected Loss Of Information Manipulation of Log Files-Windows - GSOC | TBC |
| 20 | UC-CA-904 - Windows - Multiple Login Failures from the Same Source | TBC |
| 21 | UC-LM-885 - Windows - Login Successful After Scan Attempt | TBC |
| 22 | UC-CA-905 - Windows - Multiple Login Failures to the Same Destination | TBC |
| 23 | UC-CA-903 - Windows - Multiple Login Failures for Single Username | TBC |
| 24 | UC-CA-456 - All - Login Failures Followed By Success to the same Destination IP | TBC |
| 25 | UC-IM. LM-279 - EPP - Worm Detected (Events) | TBC |
| 26 | UC-IM. LM .CC-280 - EPP – Worm Detection: Successful Connections to the Internet on Common Worm Ports | TBC |
| 27 | UC-IM.DE-1200 - AWS - AWS Cloud: S3 Bucket has been deleted - CCP | TBC |
| 28 | UC-CA -1189 - AWS - AWS Cloud: Multiple Console Login Failures from Same Source IP - CCP | TBC |
| 29 | UC-EX-271 - EPP - Treat Backdoor Trojans and Virus Events as Offenses | TBC |
| 30 | UC-IM-1615-Qradar-Event Collector is in UNKNOWN state-GSOC | TBC |
| 31 | UC-IM-441 - All - Log Source Stopped Reporting - Medium Severity- CCP | TBC |
| 32 | UC-EX.PE.PR-990 - Windows - Suspicious scheduled task created | TBC |
| 33 | UC-PE-58 - AD - User Removed from Protected Domain Group - CG Infra UK | TBC |
| 34 | UC-DE-59 - AD - Windows Firewall Policy Changed - CG Infra UK | TBC |
| 35 | UC-IM-60 - AD - Windows Firewall Stopped - CG Infra UK | TBC |
| 36 | UC-DE-17 - AD - Critical server RegKey changes - CG Infra UK | TBC |
| 37 | UC-CA-21 - AD - DPAPI Domain Master Key Backup Attempt detected - CG Infra UK | TBC |
| 38 | UC-DE-4 - AD - Addition of Domain Trusts - CG Infra UK | TBC |
| 39 | UC-EX-14 - AD - Creation of Scheduled Tasks or Services on Critical Servers - CG Infra UK | TBC |
| 40 | UC-DE-498 - Windows - System Time Changed - CG Infra UK | TBC |
| 41 | UC-DE-864 - Windows - Event or Audit Log Cleared - CG Infra UK | TBC |
| 42 | UC-IM-506 - Windows - Windows Security Log full - CG Infra UK | TBC |
| 43 | UC-DI-459 - Windows - Multiple Login Failure on Windows Device - Unknown User Name or Bad Password - CG Infra UK | TBC |
| 44 | UC-CA-1034 - Linux - Excessive Failed Logins for one user - CG Infra UK | TBC |
| 45 | UC-CC.IM-271 - EPP - Treat Backdoor Trojans and Virus Events as Offenses - CG Infra UK | TBC |
| 46 | UC-IM-255 - EPP - Possible Local Worm Detected - CG Infra UK | TBC |
| 47 | UC-IM.LM.CC-280 - EPP - Worm Detection: Successful Connections to the Internet on Common Worm Ports - CG Infra UK | TBC |
| 48 | UC-CA-904 - Windows - Multiple Login Failures from the Same Source IP - CG Infra UK | TBC |
| 49 | UC-CA-905 - Windows - Multiple Login Failures to the Same Destination IP - CG Infra UK | TBC |
| 50 | UC-CA-903 - Windows - Multiple Login Failures for Same Username - CG Infra UK | TBC |
| 51 | UC-CA-883 - Windows - Login Failures Followed By Success from the same Source IP - CG Infra UK | TBC |
| 52 | UC-IA-22 - AD - Failed Login to disabled/expired account - CG Infra UK | TBC |
| 53 | UC-DI-458 - AD - Login Successful After Scan Attempt - CG Infra UK | TBC |
| 54 | UC-CA-915 - Windows - One Account - Multiple Sources - CG Infra UK | TBC |
| 55 | UC-EF-476 - Mail - Local Mass Mailing Host Detected - CG Infra UK | TBC |
| 56 | UC-IA-1021 - X-Force Premium: Mail Server Sending Mail to Servers Categorized as SPAM - CG Infra UK | TBC |
| 57 | UC-IA-1022 - X-Force Premium: Non-Mail Server Sending Mail to Servers Categorized as SPAM - CG Infra UK | TBC |
| 58 | UC-CO. EX-273 - EPP - Treat Spyware and Virus as Offenses - CG Infra UK | TBC |
| 59 | UC-PE-243 - EPP - Malware or Virus Clean Failed - CG Infra UK | TBC |
| 60 | UC-CC-245 - EPP - Multiple Exploit Types Against Single Destination - CG Infra UK | TBC |
| 61 | UC-IM. LM-279 - EPP - Worm Detected (Events) - CG Infra UK | TBC |
| 62 | UC-EX-1266 - EPP -Malicious connections originated or linked from Ukraine or Russia - File Hash | TBC |
| 63 | UC-DE-505 - Windows - Windows Event Logging Service Shut down | TBC |
| 64 | UC-DI-458 - AD - Login Successful After Scan Attempt | TBC |
| 65 | UC-CA-456 - All - Login Failures Followed by Success to the same Destination IP - CG\_Infra\_UK | TBC |
| 66 | UC-CC-257 - EPP - Potential Botnet Events Become Offenses - CG\_Infra\_UK | TBC |
| 67 | UC-IM-173 - DB - Excessive Database Connections - CG\_Infra\_UK | TBC |
| 68 | UC-IA-624 - UBA - Expired Account Used- CG\_Infra\_UK | TBC |
| 69 | UC-PR-1152 - AD - Windows Privileged Escalation from a user account - CG\_INFRA\_UK | TBC |
| 70 | UC-PR-1242 - Linux - Privileged Escalation Succeded for Non-Privileged Account - CG\_INFRA\_UK | TBC |
| 71 | UC-RD-273 - EPP - Treat Spyware and Virus as Offenses | TBC |
| 72 | UC-CA-903 - Windows - Multiple Login Failures for Single Username (DC) | TBC |
| 73 | UC-DI-459 - Windows - Multiple Login Failure on Windows Device - Unknown Username or Bad Password | TBC |
| 74 | UC-CA-436 - Linux - Multiple Authentication Failure by Unknown Usernames | TBC |
| 75 | UC-CA-350 - Windows - Account Failed to Logon - Expired Password | TBC |
| 76 | UC-IM-438 - All - Log Source Stopped Reporting - High Severity | TBC |
| 77 | UC-IM-440 - All - Log Source Stopped Reporting - Low Severity-CG\_INFRA\_UK | TBC |
| 78 | UC-EX.LM-1619-Windows-Remote Procedure Call Service Anomaly - CVE-2022-26809 | TBC |
| 79 | UC-EX.LM-1620-Windows-A Remote Procedure Call (RPC) was Attempted - CVE-2022-26809 | TBC |
| 80 | UC-EX.LM-1621-Windows-Suspicious RDP Redirect Using TSCON - CVE-2022-26809 | TBC |
| 81 | UC-EX.LM-1622-Windows-MSTSC Shadowing Detected - CVE-2022-26809 | TBC |
| 82 | UC-EX.LM-1623-Windows-RDP Shadowing Detected - CVE-2022-26809 | TBC |
| 83 | UC-PR-1629-Linux-Privilege Escalation Privileged Escalation Failed For Privileged Account - GSOC | TBC |
| 84 | UC-EX-2211 - Windows - Fileless malware distributed through spam mail | TBC |
| 85 | UC-DE-2213 - Windows - HTML Smuggling Leads to Domain Wide Ransomware | TBC |
| 86 | UC-EX-2212 - Windows - Redeyes Transmitting Malicious LNK Through the Backdoor | TBC |
| 87 | UC-EX-2214 - Windows - Red Eyes, a CHM Virus that Utilizes Contaminated Water from Fukushima | TBC |
| 88 | UC-EX-2216 - Windows - Low-profile Threat Actor Observed Imitating NoEscape Ransomware | TBC |
| 89 | UC-DE-2215 - Windows - Threat Actors Target MSSQL Servers in DB%23JAMMER Campaign to Deliver Free World Ransomware | TBC |
| 90 | UC-DE.PR-2217 - Windows - Blue Shell Malware Used in APT Attacks Targeting South Korea and Thailand | TBC |
| 91 | UC-DE-2220 - Windows - Detect the execution of new and uncommon MSI installer files. | TBC |
| 92 | UC-DE-2235- Email Gateways -Detection of New Slimmed-Down ROMCOM Variant | TBC |
| 93 | UC-CC-2230 - Windows - Earth Lusca Proxy Tools and Commands | TBC |
| 94 | UC-DE.PE.PR-2226 - Windows - Detect potential Midge Dropper malware activity | TBC |
| 95 | UC-DE-2231 - Windows - Detection of Agent Tesla Uses VBS And Steganography for Delivery And Intrusion | TBC |
| 96 | UC-IA.EX-2234 - Windows - Detect DinodasRAT Activity | TBC |
| 97 | UC-IA.CO-2236- Windows -BbyStealer Malware Detection | TBC |
| 98 | UC-DE-2229 - Windows - Turla Group Lateral Movement (via process\_creation) | TBC |
| 99 | UC-PE.DE-2240 - Windows - Detection of process used New DarkGate Variants | TBC |
| 100 | UC-EX-2242 - Windows - Possible infection by TA402 phishing | TBC |
| 101 | UC-IA-2245 - Proxy - Analysis of Tycoon Phishing-as-a-Service System on events which are detected | TBC |
| 102 | Suspected Loss of Sensitive Information\_Windows Firewall Stopped -GSOC | TBC |

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients’ opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Learn more about us at [www.capgemini.com](http://www.capgemini.com)



This document contains information that may be privileged or confidential and is the property of the Capgemini Group.  
Copyright © 2019 Capgemini. All rights reserved.