A logo with blue and orange letters

AI-generated content may be incorrect.A blue dots on a black background

AI-generated content may be incorrect.

**Prepared By:** {{ team[0].name }}

**E-mail:** {{ team[0].email }}

▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬

{{ company.name.upper() }} PRIVILEGED AND CONFIDENTIAL

{{ client.name }}

**{{ project.type }}**

**{{ report\_date }}**

[Executive Summary 3](#_Toc195535449)

[Assessment Scope 3](#_Toc195535450)

[Observed Findings 4](#_Toc195535451)

Executive Summary

{{ company.name }} was engaged by {{ client.name }} to perform a {{ project.type }} against their environment. The assessment began on {{ project.start\_date }}.

Table 1 shows the following domains/objects that were in scope for the assessment:

|  |  |
| --- | --- |
| {%tr for objectscope in scope %} |  |
| Object Type | Value |
| {{ objectscope.name }} | {{ objectscope.scope }} |
| {%tr endfor %} |  |

Table 1: In Scope Objects

During the engagement several recommendations were created to improve the confidentiality, integrity and availability of the {{ client.name }} environment. {{ company.name }} identified the following key strengths:

{%p for observation in observations %}

{%p if observation.extra\_fields.type == “Strength” %}

**{{ observation.title }}**

{{observation.description\_rt }}

{%p endif %}

{%p endfor %}

{{ company.name }} has identified the following areas with opportunities for improvement:

{%p for observation in observations %}

{%p if observation.extra\_fields.type == “Weakness” %}

**{{ observation.title }}**

{{observation.description\_rt }}

{%p endif %}

{%p endfor %}

Table 2 shows the aggregated recommendations as well as the severity levels.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Critical | High | Medium | Low | Informational |
| {{ totals.findings\_critical }} | {{ totals.findings\_high }} | {{ totals.findings\_medium }} | {{ totals.findings\_low }} | {{ totals.findings\_info }} |

Table 2: Discovered Findings

Assessment Methodology

Overview

{{ company.name }}’ assessment methodology includes three phases:

**Phase 1: Initial Engagement and Information Gathering**

The assessment begins with meetings involving {{ client.name }}'s leadership and key technical personnel to understand the organization’s infrastructure, business priorities, and security objectives. This phase ensures alignment between assessment goals and operational context.

**Phase 2: Scanning and Data Collection**

{{ company.name }} deploys a combination of open-source assessment tools and internally developed scripts to scan the environment and gather relevant security data. These tools identify vulnerabilities, misconfigurations, and exposures, while custom scripts extract detailed configuration and system information directly from hosts, directory services, and network components. This approach provides a comprehensive and tailored view of the current security posture.

**Phase 3: Manual Review, Validation, and Recommendations**

Collected data is manually reviewed and validated against the live environment to eliminate false positives and confirm accuracy. Based on these verified findings, we provide prioritized security recommendations and tailored remediation guidance to strengthen {{ client.name }}'s overall posture.

Findings and Observations

This section presents the findings identified during each phase of the assessment. Each finding has been assigned a severity rating—Critical, High, Medium, Low, or Informational—based on the criteria outlined in [*Appendix A: Rating System Breakdown*](#AppendixA). Additionally, a Level of Effort rating and Remediation Impact rating and assigned to each finding with the criteria outlined in [Appendix B](#AppendixB) and [Appendix C](#AppendixC) respectively.

A finding represents a potential weakness within the in-scope environment that could affect the confidentiality, integrity, or availability of systems or data. Supporting evidence for each finding is drawn from configuration analysis, automated tooling, manual validation, and, where applicable, penetration testing activities.

Additional context may be based on discussions with {{ client.name }}’s personnel, documentation provided during the engagement, and informed observations made during the assessment.

The findings and observations below reflect the current security posture and highlight areas where improvements may be warranted.

{%p if totals.findings\_critical > 0 %}

Critical Findings

{%p endif %}

|  |  |  |
| --- | --- | --- |
| {%tr for finding in findings|filter\_severity(["Critical"]) %} | | |
| {% set id = finding.finding\_type ~ '-C-' ~ '%02d' % loop.index %}{{ id }} | {{ finding.title }} | |
| **Severity: {% cellbg finding.severity\_color %}{{ finding.severity }}** | | |
| Level of Effort: {% set effort = finding.extra\_fields.levelofeffort %}  {%p if effort == "Low" %}  ● {{ effort }}  {%p elif effort == "Medium" %}  ● {{ effort }}  {%p elif effort == "High" %}  ● {{ effort }}  {%p else %}  {{ effort }}  {%p endif %} | | Remediation Impact: {% set rem\_impact = finding.extra\_fields. remediation\_impact %}  {%p if rem\_impact == "Low" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "Medium" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "High" %}  ● {{ rem\_impact }}  {%p else %}  {{ rem\_impact }}  {%p endif %} |
| **Description** | | |
| {{ finding.description\_rt }} | | |
| **Recommendation** | | |
| {{ finding.mitigation\_rt }} | | |
| **Affected Hosts/Objects** | | |
| {{ finding.affected\_entities\_rt }} | | |
| **References** | | |
| {{ finding.references\_rt }} | | |
|  | | |
|  | | |
| {%tr endfor %} | | |

{%p if totals.findings\_high > 0 %}

High Findings

{%p endif %}

|  |  |  |
| --- | --- | --- |
| {%tr for finding in findings|filter\_severity(["High"]) %} | | |
| {% set id = finding.finding\_type ~ '-H-' ~ '%02d' % loop.index %}{{ id }} | {{ finding.title }} | |
| **Severity: {% cellbg finding.severity\_color %}{{ finding.severity }}** | | |
| Level of Effort: {% set effort = finding.extra\_fields.levelofeffort %}  {%p if effort == "Low" %}  ● {{ effort }}  {%p elif effort == "Medium" %}  ● {{ effort }}  {%p elif effort == "High" %}  ● {{ effort }}  {%p else %}  {{ effort }}  {%p endif %} | | Remediation Impact: {% set rem\_impact = finding.extra\_fields. remediation\_impact %}  {%p if rem\_impact == "Low" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "Medium" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "High" %}  ● {{ rem\_impact }}  {%p else %}  {{ rem\_impact }}  {%p endif %} |
| **Description** | | |
| {{ finding.description\_rt }} | | |
| **Recommendation** | | |
| {{ finding.mitigation\_rt }} | | |
| **Affected Hosts/Objects** | | |
| {{ finding.affected\_entities\_rt }} | | |
| **References** | | |
| {{ finding.references\_rt }} | | |
|  | | |
|  | | |
| {%tr endfor %} | | |

{%p if totals.findings\_medium > 0 %}

Medium Findings

{%p endif %}

|  |  |  |
| --- | --- | --- |
| {%tr for finding in findings|filter\_severity(["Medium"]) %} | | |
| {% set id = finding.finding\_type ~ '-M-' ~ '%02d' % loop.index %}{{ id }} | {{ finding.title }} | |
| **Severity: {% cellbg finding.severity\_color %}{{ finding.severity }}** | | |
| Level of Effort: {% set effort = finding.extra\_fields.levelofeffort %}  {%p if effort == "Low" %}  ● {{ effort }}  {%p elif effort == "Medium" %}  ● {{ effort }}  {%p elif effort == "High" %}  ● {{ effort }}  {%p else %}  {{ effort }}  {%p endif %} | | Remediation Impact: {% set rem\_impact = finding.extra\_fields. remediation\_impact %}  {%p if rem\_impact == "Low" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "Medium" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "High" %}  ● {{ rem\_impact }}  {%p else %}  {{ rem\_impact }}  {%p endif %} |
| **Description** | | |
| {{ finding.description\_rt }} | | |
| **Recommendation** | | |
| {{ finding.mitigation\_rt }} | | |
| **Affected Hosts/Objects** | | |
| {{ finding.affected\_entities\_rt }} | | |
| **References** | | |
| {{ finding.references\_rt }} | | |
|  | | |
|  | | |
| {%tr endfor %} | | |

{%p if totals.findings\_low > 0 %}

Low Findings

{%p endif %}

|  |  |  |
| --- | --- | --- |
| {%tr for finding in findings|filter\_severity(["Low"]) %} | | |
| {% set id = finding.finding\_type ~ '-L-' ~ '%02d' % loop.index %}{{ id }} | {{ finding.title }} | |
| **Severity: {% cellbg finding.severity\_color %}{{ finding.severity }}** | | |
| Level of Effort: {% set effort = finding.extra\_fields.levelofeffort %}  {%p if effort == "Low" %}  ● {{ effort }}  {%p elif effort == "Medium" %}  ● {{ effort }}  {%p elif effort == "High" %}  ● {{ effort }}  {%p else %}  {{ effort }}  {%p endif %} | | Remediation Impact: {% set rem\_impact = finding.extra\_fields. remediation\_impact %}  {%p if rem\_impact == "Low" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "Medium" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "High" %}  ● {{ rem\_impact }}  {%p else %}  {{ rem\_impact }}  {%p endif %} |
| **Description** | | |
| {{ finding.description\_rt }} | | |
| **Recommendation** | | |
| {{ finding.mitigation\_rt }} | | |
| **Affected Hosts/Objects** | | |
| {{ finding.affected\_entities\_rt }} | | |
| **References** | | |
| {{ finding.references\_rt }} | | |
|  | | |
|  | | |
| {%tr endfor %} | | |

{%p if totals.findings\_info > 0 %}

Informational Findings

{%p endif %}

|  |  |  |
| --- | --- | --- |
| {%tr for finding in findings|filter\_severity(["Informational"]) %} | | |
| {% set id = finding.finding\_type ~ '-I-' ~ '%02d' % loop.index %}{{ id }} | {{ finding.title }} | |
| **Severity: {% cellbg finding.severity\_color %}{{ finding.severity }}** | | |
| Level of Effort: {% set effort = finding.extra\_fields.levelofeffort %}  {%p if effort == "Low" %}  ● {{ effort }}  {%p elif effort == "Medium" %}  ● {{ effort }}  {%p elif effort == "High" %}  ● {{ effort }}  {%p else %}  {{ effort }}  {%p endif %} | | Remediation Impact: {% set rem\_impact = finding.extra\_fields. remediation\_impact %}  {%p if rem\_impact == "Low" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "Medium" %}  ● {{ rem\_impact }}  {%p elif rem\_impact == "High" %}  ● {{ rem\_impact }}  {%p else %}  {{ rem\_impact }}  {%p endif %} |
| **Description** | | |
| {{ finding.description\_rt }} | | |
| **Recommendation** | | |
| {{ finding.mitigation\_rt }} | | |
| **Affected Hosts/Objects** | | |
| {{ finding.affected\_entities\_rt }} | | |
| **References** | | |
| {{ finding.references\_rt }} | | |
|  | | |
|  | | |
| {%tr endfor %} | | |

Appendix A: Rating System Breakdown

The table below outlines each severity level used in this report, along with the criteria required to assign a finding to that level. These classifications help prioritize remediation efforts by indicating the potential impact and urgency associated with each finding. The severity ratings range from Critical to Informational and are determined based on factors such as exploitability, potential business impact, and likelihood of occurrence.

|  |  |
| --- | --- |
| Severity | Criteria |
| Critical | Critical-severity findings represent immediate and readily exploitable weaknesses that could result in unauthorized access, data loss, or disruption of core services. These often involve compromised hypervisor access, unauthenticated network storage exposure, unencrypted or misconfigured backup repositories, or critical vulnerabilities in network segmentation or routing that could lead to enterprise-wide compromise of availability, confidentiality, and integrity. |
| High | High-severity findings indicate significant security gaps or misconfigurations that, while not immediately exploitable without additional conditions (e.g., insider access, chaining attacks), pose a real risk to infrastructure resilience. Examples include insufficient isolation between virtual machines, improper access controls on storage or backup environments, or insecure protocols used for management interfaces that could be leveraged for lateral movement or unauthorized data manipulation. |
| Medium | Medium-severity findings highlight moderately exploitable conditions or outdated configurations that could be used to gain limited access or visibility into virtual or physical infrastructure. These include incomplete logging on network devices, outdated hypervisor patches, or weak role-based access controls (RBAC) in backup systems. The impact is typically localized, but could be a steppingstone in a multi-phase attack. |
| Low | Low-severity findings represent weak or suboptimal configurations that, while not directly exploitable on their own, may reduce the overall effectiveness of security controls or support the success of other attacks under specific conditions. These issues are not readily accessible to adversaries and cannot be used independently in the attack lifecycle. |
| Informational | Informational findings provide contextual insights into environment. These include architecture diagrams, software inventories, default configurations, or system behaviors that have no current security impact but may assist in trend analysis, monitoring strategy, or future infrastructure planning. |

Table 3: Severity Level Breakdown

Appendix B: Level of Effort Breakdown

The Level of Effort rating provides an estimate of the time, resources, and complexity involved in implementing a given remediation step. This classification helps prioritize actions not only based on risk, but also on the practical effort required to address each finding. The levels are defined as follows:

|  |  |
| --- | --- |
| Level of Effort | Criteria |
| High● | Remediation requires significant planning, coordination, or technical changes. This may include architectural redesigns, system overhauls, or widespread policy and process updates. These efforts typically involve multiple teams and extended timelines. |
| Medium● | Remediation involves moderate complexity and resource allocation. Changes may include system configuration adjustments, implementation of new controls, or limited software deployments. These tasks generally require some coordination but are achievable within standard operational cycles. |
| Low● | Remediation is straightforward and requires minimal time or resources. These changes can often be implemented quickly by a single team or administrator with little disruption to existing systems or processes. |

Table 4: Level of Effort Breakdown

Appendix C: Remediation Impact Breakdown

The Remediation Impact rating reflects the potential effect a remediation action may have on users, systems, or business operations. While some changes may be technically simple, they can still introduce significant disruption or require user adaptation. This rating helps weigh the organizational impact of implementing each recommendation. The levels are defined as follows:

|  |  |
| --- | --- |
| Remediation Impact | Criteria |
| High● | Remediation is likely to cause noticeable disruption to users or business processes. This may include changes that affect how users access systems, require widespread training, or result in temporary downtime or workflow interruptions. For example, enabling MFA for all users can significantly impact user experience if not already adopted. |
| Medium● | Remediation has a moderate effect on users or operations. It may require some user communication, limited downtime, or adjustments to processes, but can generally be absorbed without major disruption. |
| Low● | Remediation has minimal or no noticeable impact on users or business operations. These changes are typically transparent, require no user interaction, and can be implemented without affecting productivity. |

Table 5: Remediation Impact Breakdown