[CLIENT] [DATE]
White Box Risk Analysis Report

Date / Version

Project Objective

Abacus Group was contracted by [CLIENT] to perform a scoped white box risk analysis on corporate systems between the dates of [DATE]-[DATE].

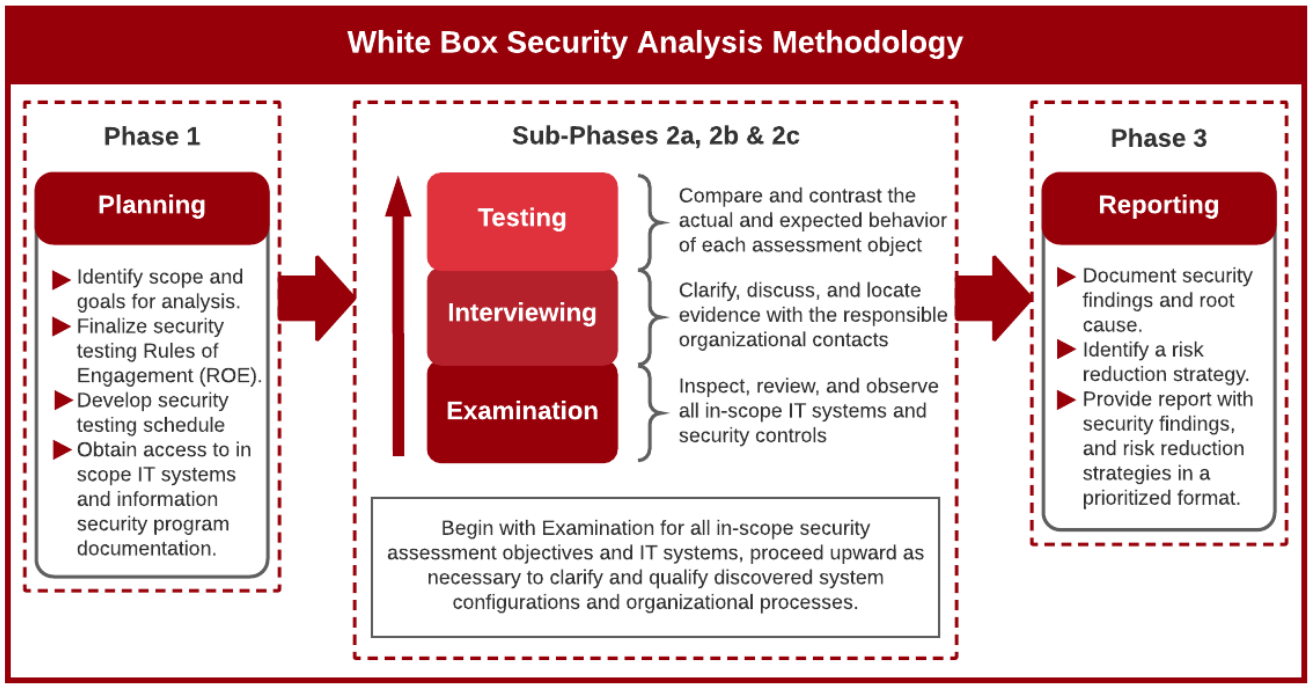
Objectives of This Exercise:

- **Identify and evaluate controls across three key areas:**
  - **Management Controls – Management of the information technology security system and the management and acceptance of risk**
  - **Operational Controls – Security methods focusing on mechanisms implemented and executed primarily by people, including media safeguards, and inventory controls**
  - **Technical Controls – Hardware and software controls provide automated protection to the system or applications.**
- **Collect, scan, and analyze platform AWS and Azure configurations, including BLOB storage permissions, identity management, database configs, security groups/ACLs, DB schema, isolation and segregation mechanisms, web application firewall configs, dependency versions, logging and accounting mechanisms, data-at-rest and data-in-transit cryptography, HIDS/HIPS configs, access control mechanisms and more.**
- **Outline the potential impact and severity of each vulnerability, weakness, and risk, including observed deviations from standard information security best practices and principles.**
- **Present information that identifies the root causes behind the vulnerabilities, weaknesses, and risks identified in the assessment while conveying a message of how those problems relate to the inherent security posture of [CLIENT].**
- **Provide [CLIENT] with a full due diligence report, including information such as vulnerability/weakness/risk details, risk mitigation recommendations, analysis methods, information system statistics, and more.**

Abacus Group performed security testing in accordance with NIST SP800-115 Technical Guide to Information Security Testing and Assessment guidelines. The findings in this report are limited to those that were within the scope of the Rules of Engagement (RoE). This report reflects the security position of [CLIENT]'s information systems, as seen during the dates in which the testing was conducted. Future changes to any applications or the infrastructure will change the security position of the environment from its current state. Additionally, as time passes, new types of attacks may arise which were previously unknown to the security industry. Considering this, Abacus Group always recommends that all information systems undergo routine security testing within a reasonable timeframe.

White Box Risk Analysis Methodology

Abacus Group's white box security analysis methodology is an implementation modeled from the standards outlined in NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. Our methodology consists of three phases which include Planning, Examination, Interviewing, Testing, and Reporting, as shown in the figure below. All IT systems and security controls were assessed in consideration of NIST CyberSecurity Framework (CSF) guidelines and using lessons learned during past assessments.



Typical Security Testing Tools Used by Abacus Group:

- **Principle Mapper – A tool used to probe, analyze, and visualize IAM (Identity and Access Management) configurations.**
- **Cloudmapper – A tool used for systematically probing and visualizing AWS (Amazon Web Services) environments.**
- **Scout Suite – A tool used for systematically probing, analyzing, and assessing GCP (Google Cloud Platform), AWS, and Azure environments.**
- **Prowler – A tool that performs AWS security best practices assessments, audits, incident response, continuous monitoring, hardening, and forensics readiness.**
- **Cloudsplaining – An AWS IAM Security Assessment tool that identifies violations of least privilege**
- **Checkov – A static code analysis tool that identifies Terraform compliance misconfigurations using graph-based scanning.**
- **TFScan – A tool used for detecting logical vulnerabilities in Terraform JSON files.**
- **Shodan.io – A search engine for internet-connected devices (such as routers, switches, servers, web cameras, IoT devices, etc.), analyzing things like open ports, service banners, web HTTP headers, and more**

White Box Risk Analysis Executive Overview

SWOT Analysis

Strengths

3.

- Highly capable and responsive IT, security, networking, and cloud administrative teams who demonstrated the ability to rapidly remediate identified vulnerabilities in real time.
- Many well-conceived and well configured policies were identified within O365, Microsoft Azure, and Amazon Web Services.
- The documentation provided showed regular table-top exercises designed to test and refine numerous aspects of incident

Weaknesses

1.

- Inconsistent application of configurations results in gaps in the security posture of the organization such as logging not being universally enforced on infrastructure, inconsistent password policies, and inconsistent enforcement of MFA.
- Many systems are end of life and no longer receive security updates; these devices will always present an inherent risk to the network while they are still in operation.

2.

Opportunities

- Continuing to transition services and infrastructure into Microsoft Azure can provide enhanced security and monitoring capabilities with the proper configurations, compared to those observed during previous internal penetration tests.
- Integrating cloud-based logging facilities with the currently implemented SIEM can increase the situational awareness of the security operations center and amplify the capacity for detection, incident response, and containment of potential threats.

Threats

- Currently configured file share permissions provide a malicious actor the ability to exfiltrate data or implement ransomware immediately upon compromising the internal network, regardless of permission level.
- Unmonitored domain controllers pose the risk of being targeted by malicious actors with a reduced capacity for detection, incident response or containment.
- Several identified vulnerabilities can be linked together into a kill-chain to provide a malicious actor the ability to easily move laterally

Scope of Analyzed Corporate Information Systems

- **Office365**
- **Azure Active Directory**
- **Legacy Active Directory and Connected Systems**
- **Corporate Cisco Network Infrastructure**
    - **Limitation Note: Not all Cisco infrastructure was federated to Active Directory with RADIUS which means those systems may have limited insight.**
- **AWS**
    - **[REDACTED]**
    - **[REDACTED]**
    - **[REDACTED]**
    - **[REDACTED]**
    - **[REDACTED]**
    - **[REDACTED]**
    - **[REDACTED]**
- **Corporate Networks**
    - **[REDACTED]**
    - **[REDACTED]**
    - **[REDACTED]**
    - **[REDACTED]**
    - **[REDACTED]**

White Box Risk Analysis Narrative

Abacus Group's methodology was comprised of two main techniques: including automated, tool-based data collection and analysis, and manual analysis performed by Abacus Group's security engineers. It is important to note that the security findings and risk ratings generated by automated tools are not necessarily accurate on their own, as automated tools lack the context concerning compensating controls or actual environmental impact. That said, the security findings section of this report includes security risks and risk mitigation recommendations with this context in mind.

Abacus Group performed both active and passive scanning on [CLIENT]'s external information systems for the purposes of fingerprinting. The fingerprinting process involved collecting information pertaining to open TCP/UDP ports, listening services, specific software/operating system identifiers, and more. This information and its corresponding analysis can be referenced in the (separate) black-box external network penetration testing report titled "[CLIENT] [DATE] – External Penetration Testing and Social Engineering Report." For brevity, external vulnerabilities identified in that report will be omitted from this report, however, those findings were still analyzed.

Abacus Group performed its white-box analysis activities on [CLIENT]'s internal network by deploying an onsite virtual machine running Kali Linux. Host discovery and Windows systems enumeration began with active, automated Nmap and Network Detective scans. During this time, internal network traffic was also captured and analyzed using WireShark and Yersinia. An in-depth analysis of internal network security risks can be found in the (separate) report titled "[REDACTED]." For brevity, internal vulnerabilities identified in that report will be omitted from this report, however, those findings were still analyzed.

This report will focus primarily on expanding the depth of analysis of the previously referenced external and internal penetration testing findings with insight gained through a white box process. To support this effort, [CLIENT]'s IT team provided Abacus Group with the following: read-only access to

Microsoft Azure, read-only access to Office 365, Amazon AWS API Keys, as well as assistance in performing a Network Detective scan as an active directory domain administrator.

Previously Noted Security Findings for Reference: [REDACTED]

Summary of Risk Results

Report	Risk Title Description	Affected Endpoint(s)	Level of Risk
INTERNAL PENETRATION TESTING REPORT	[redacted]	[redacted]	HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			HIGH
			MODERATE
			MODERATE
			MODERATE
			MODERATE
			MODERATE
			MODERATE
			LOW
			LOW
			LOW

Previously Noted Security Findings for Reference: [REDACTED]

Summary of Risk Results			
Report	Risk Title Description	Affected Endpoint(s)	Level of Risk
EXTERNAL PENETRATION TESTING REPORT	[redacted]	[redacted]	MODERATE
	[redacted]	[redacted]	LOW
	[redacted]	[redacted]	LOW
	[redacted]	[redacted]	LOW
	[redacted]	[redacted]	LOW
	[redacted]	[redacted]	LOW
	[redacted]	[redacted]	LOW
	[redacted]	[redacted]	LOW
	[redacted]	[redacted]	LOW
	[redacted]	[redacted]	LOW

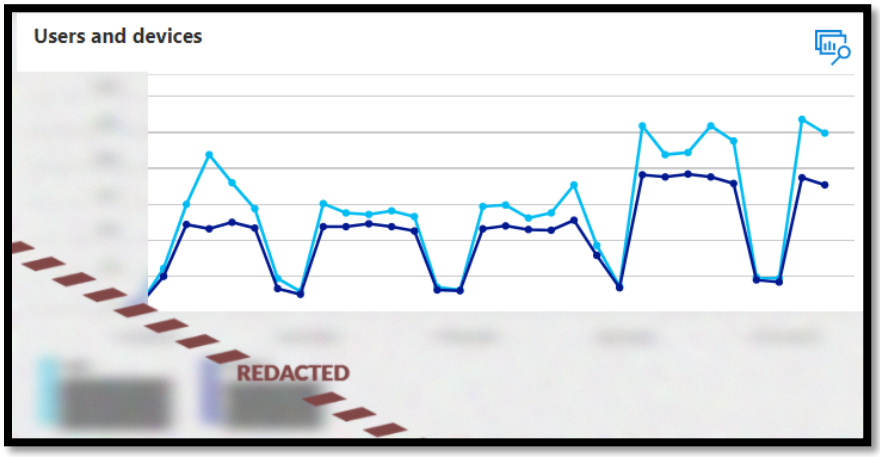
REDACTED

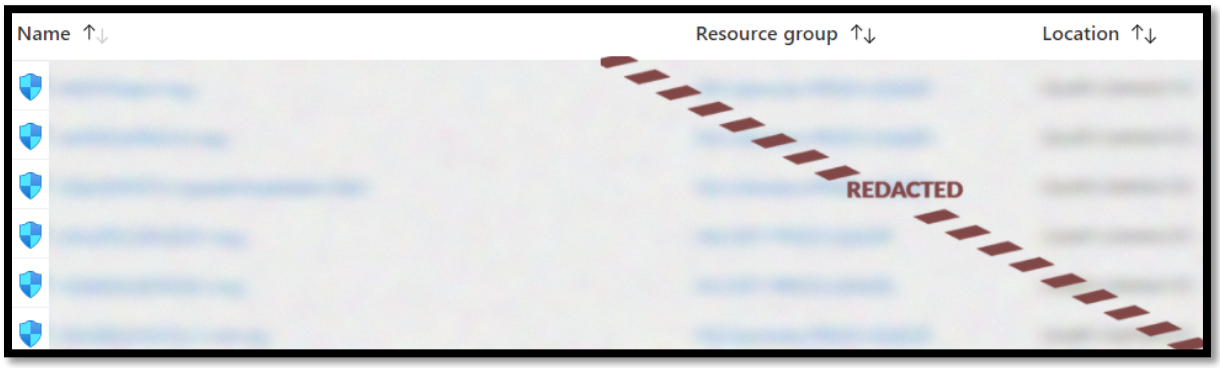
Cloud Infrastructure: Microsoft Azure

Analysis of [CLIENT]'s Microsoft Azure environment began with identifying the users and associated devices, groups, roles, and services being utilized such as logging facilities, SIEM, virtual network firewall coverage, virtual machines, BLOB storage, Microsoft Defender, and multifactor authentication policies (MFA). Next, Abacus Group security engineers analyzed the security posture of the environment holistically to determine if any overlapping security controls are in place to identify potentially vulnerable configurations.

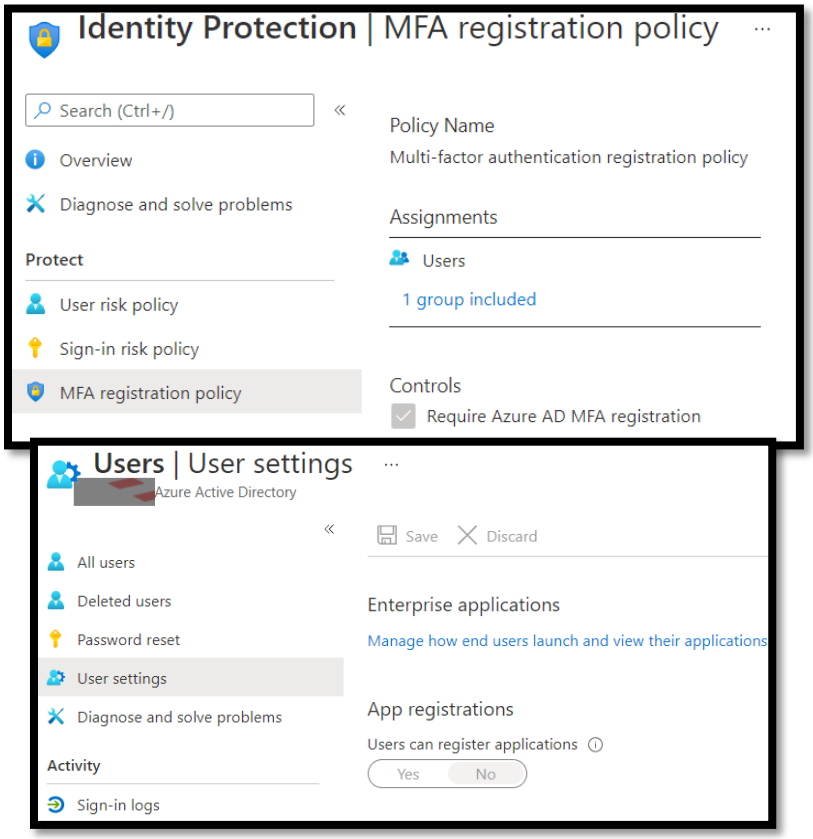
The assessment indicated that Azure is not yet widely used by [CLIENT], although Abacus Group's correspondence with the technology team indicated that a transition to greater utilization of Azure is an objective moving forward. Given this, the identified misconfigurations from a security perspective should be viewed through the *lens of an environment that is still in the process of being optimized*.

The number of users and devices compared to the analysis of the on-premises environment (see section 4.2) demonstrated the environment was established recently and is in the process of being configured.



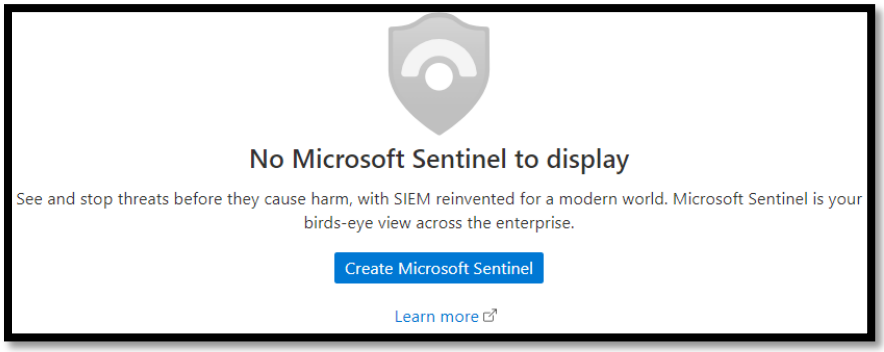


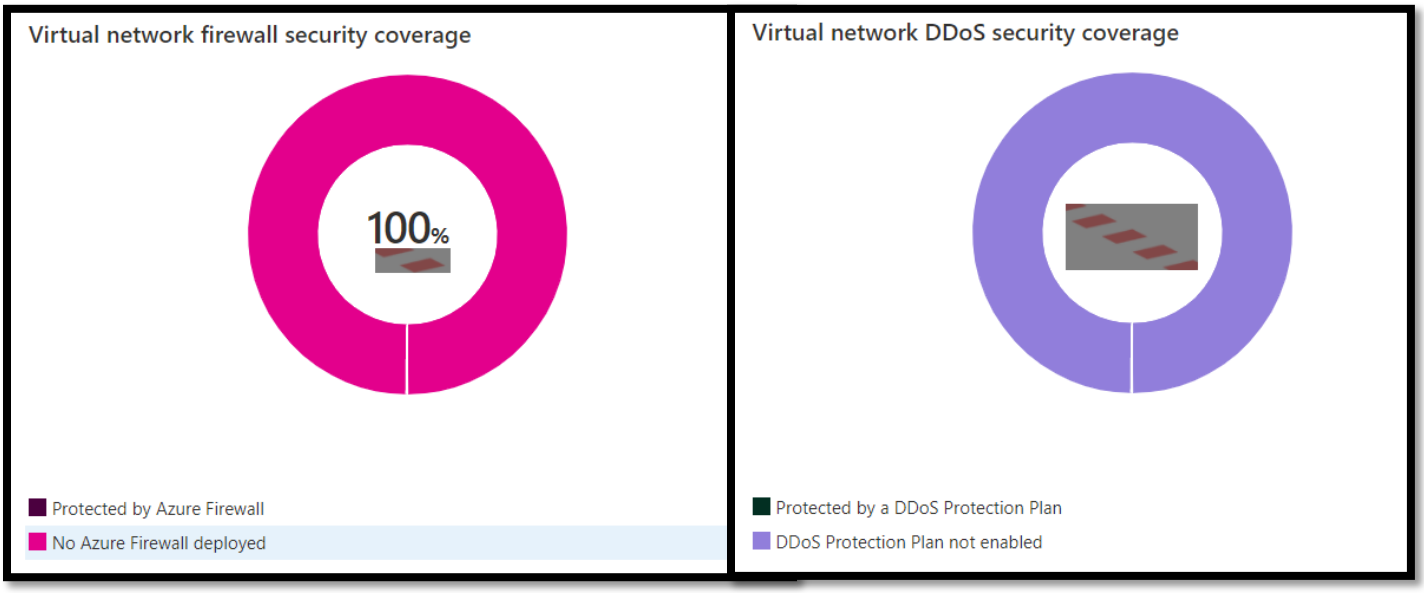
User and role settings were well established with well-implemented security best practices such as requiring all users to use Azure AD MFA, and disallowing users from registering their own applications. A common method of maintaining persistence in an environment is to compromise an account that does not have MFA implemented and then grant an external malicious application access to the environment. These safeguards effectively mitigate that attack vector.



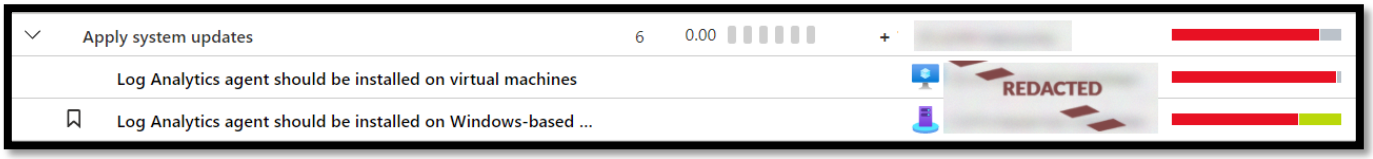
Additionally, several conditional access policies were implemented to further support the security posture, which included blocking legacy authentication, enforcing administrator and user MFA, and establishing a list of blocked countries and IP addresses. Abacus Group considers these conditional access policies to be in line with industry best practices and were well implemented by the [CLIENT] IT team.

Neither Microsoft Sentinel nor virtual network firewalls were configured within the environment; both would provide substantial insight and enhanced configurability to the environment's security posture.

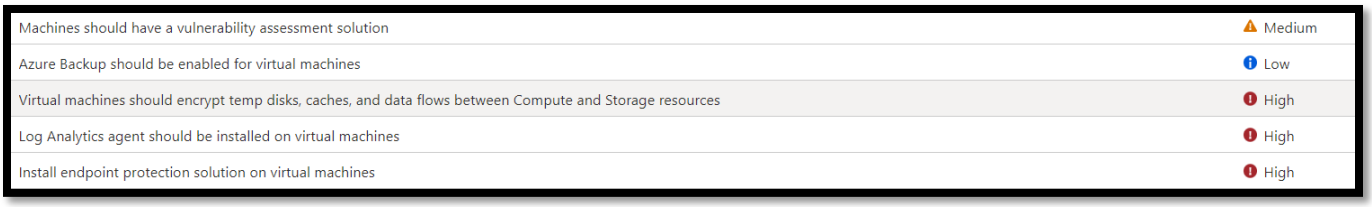




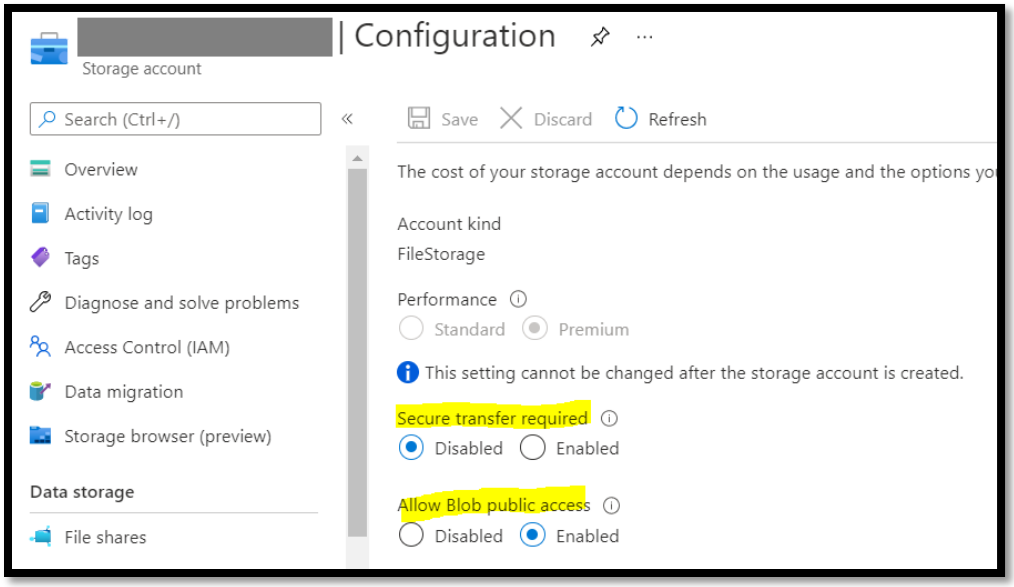
The majority of virtual machines and Azure Arc machines were identified to not have logging enabled on them. This is an important capability from a security perspective to aid in the incident response process to anomalous activity.



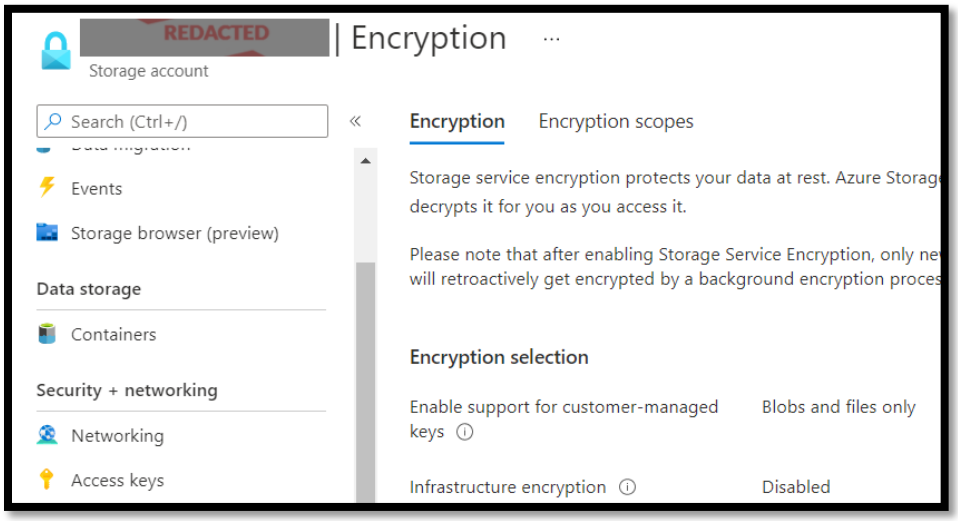
Deeper analysis of virtual machines indicated that in addition to log analytics not being implemented, there were also a lack of backups, vulnerability assessment solutions, and endpoint protection solutions. Furthermore, temp disks, caches, and data flows between compute and storage resources should be encrypted to ensure data integrity.



Abacus Group security engineers identified a concerning configuration regarding the [REDACTED] account in which Secure Transfer was disabled while public BLOB access was enabled. This combination is especially problematic if the BLOB storage can be publicly accessed through plain text means.

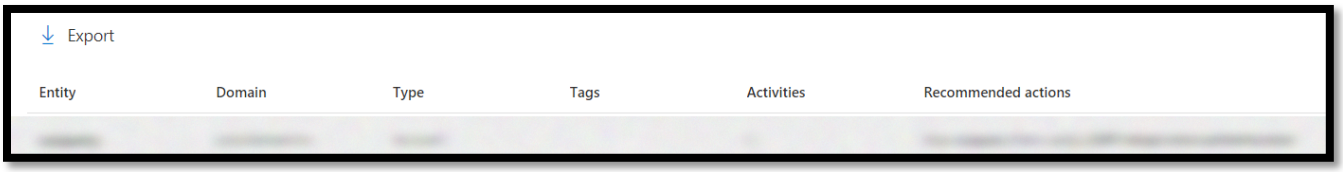


Further opportunities for improvement to data encryption were identified during analysis of the [CLIENT] [REDACTED] storage account which indicated that infrastructure encryption is also disabled.



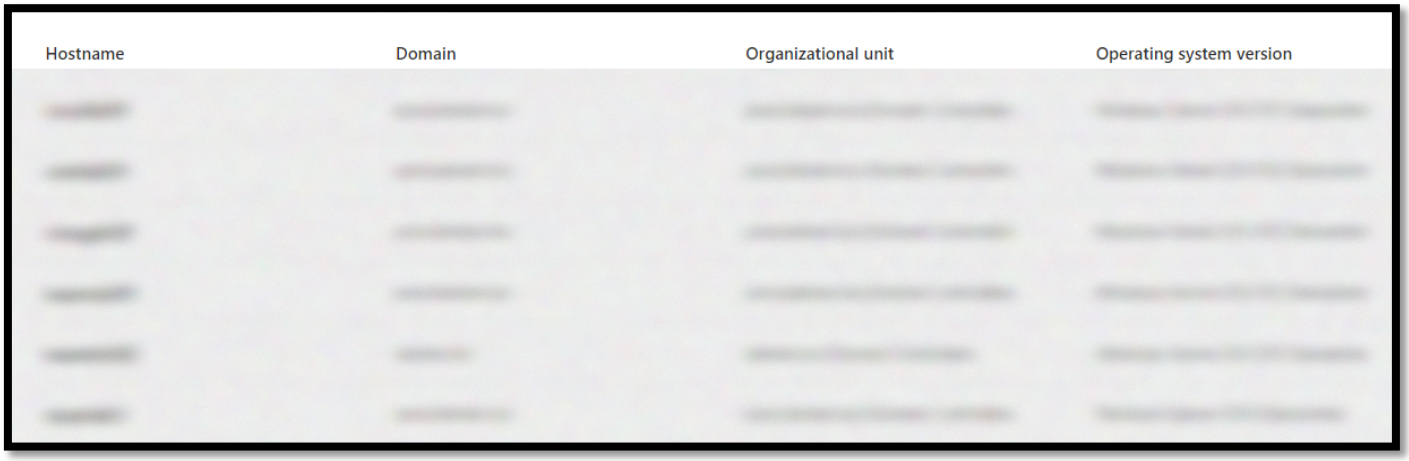
Assessment of Microsoft Defender for Identity's configuration showed several areas of optimization for reducing potential attack and lateral movement vectors of a malicious actor and increasing the situational awareness of network domain controllers.

The first issue identified was the transmission of credentials in clear text. Insecure traffic such as LDAP simple-bind (as seen in the below screenshot) can be easily sniffed by malicious actors performing a man in the middle (MitM) attack. If transmitted data is captured, any credentials that are transmitted in plain text become inherently compromised.



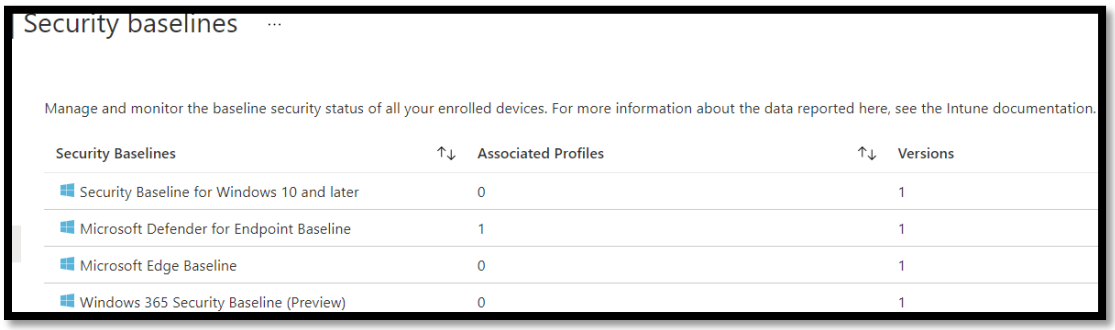
Abacus Group security engineers also identified several entities with unconstrained Kerberos delegation, which is a significant security vulnerability. Kerberos delegation is a functionality that allows applications to request user credentials to access resources on behalf of that user. Unconstrained delegation allows an entity to impersonate users to any service. This is a very common and highly effective method of lateral movement and privilege escalation in active directory environments.

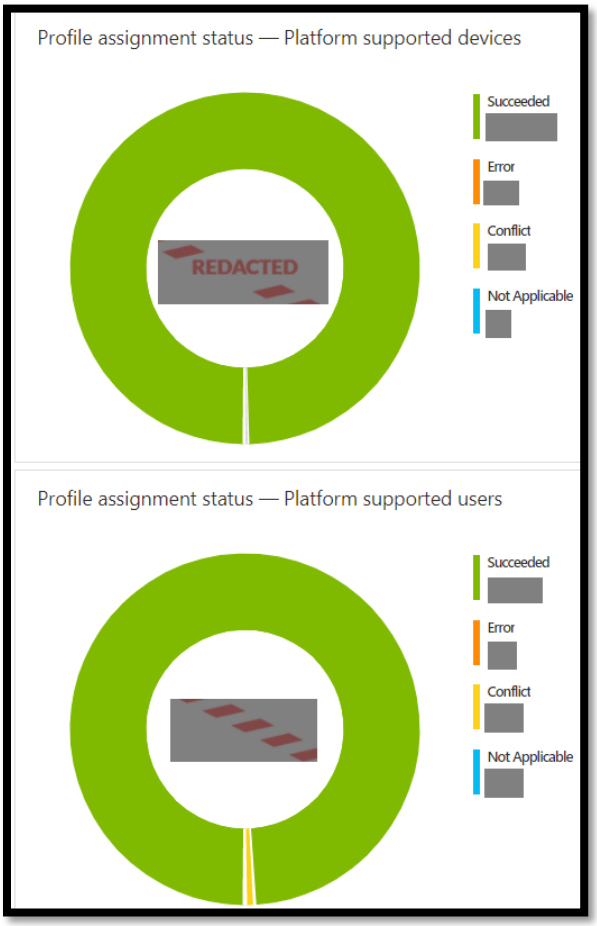
Additionally, six domain controllers were also flagged as being unmonitored by a Microsoft Defender for Identity sensor. These sensors continuously monitor the environment to provide insight related to both risks and efficiencies.



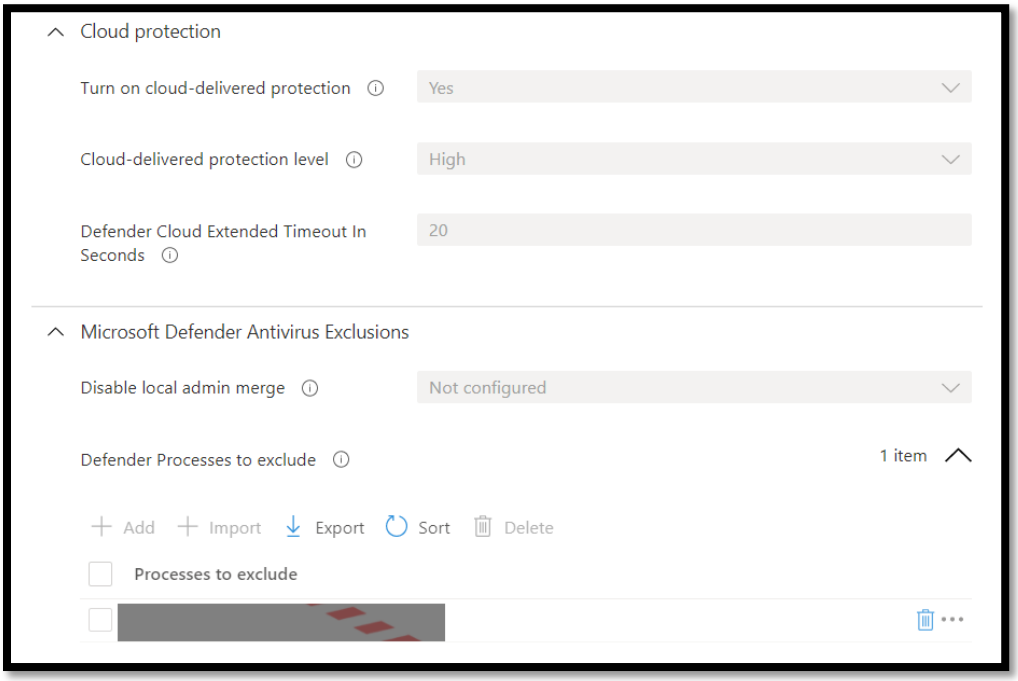
The aggregate of the three vulnerabilities described above elevates the overall risk posture, as a malicious actor could chain these vulnerabilities together into a larger kill chain. First, by performing a MitM attack, the plain text credentials could be captured by exploiting the insecure nature of LDAP simple bind. Next, lateral movement or privilege escalation could be attempted through the unconstrained delegation within Kerberos, potentially impacting one of the domain controllers that are not being monitored by Microsoft Defender for Identity's sensors.

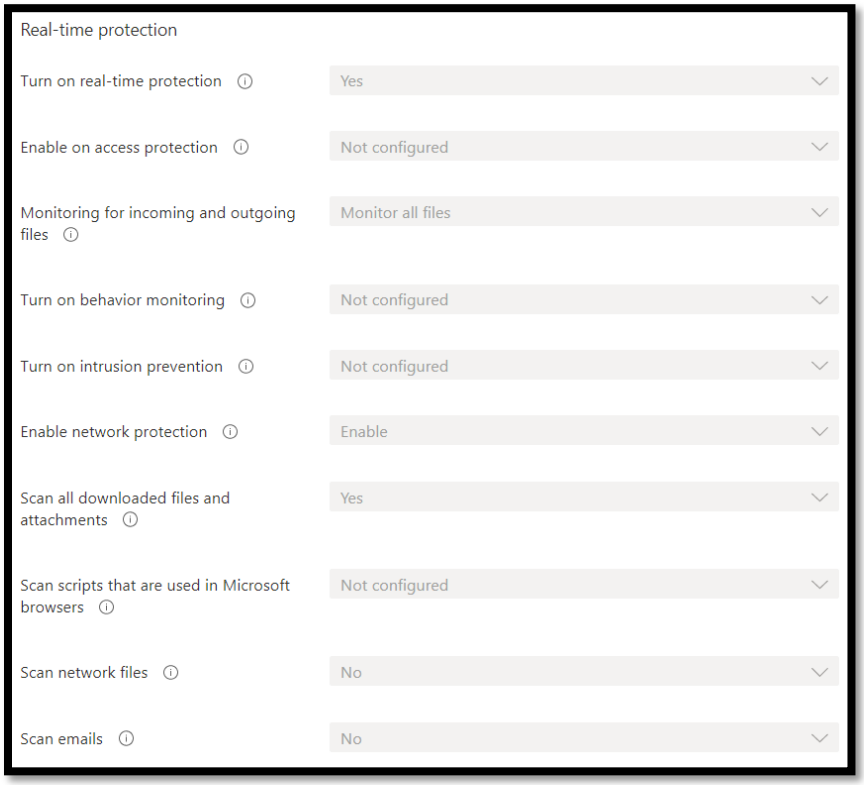
Defender for Endpoint was analyzed by examining endpoint security baselines reports related to antivirus agent status and the results of those reports. This demonstrated all enrolled devices had been validated as clean during reoccurring scanning throughout the engagement period, and that configured settings demonstrated a generally robust security posture.

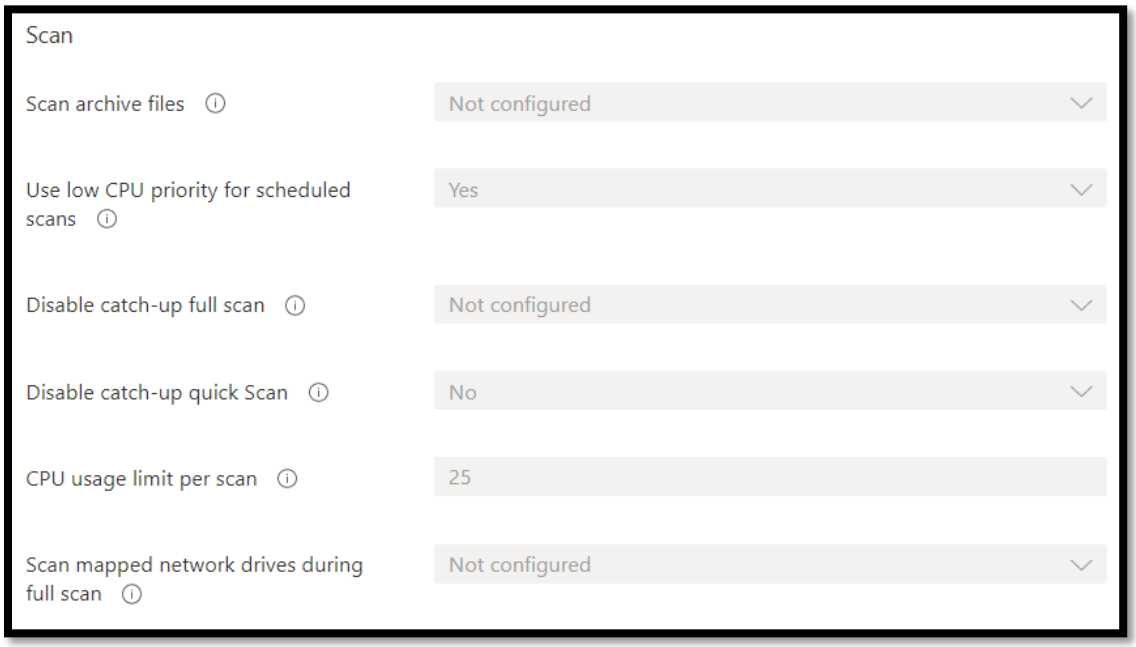




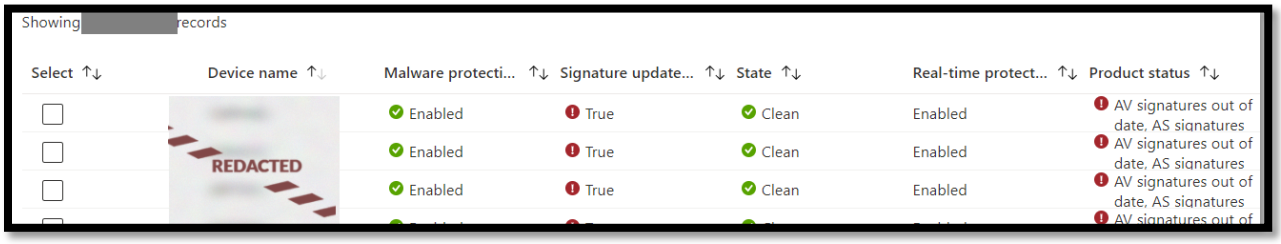
Setting	Succeeded
CPU usage limit per scan	
Scan type	
Turn on real-time protection	
Defender Files And Folders To Exclude	
Check for signature updates before running scan	
Use low CPU priority for scheduled scans	
Cloud-delivered protection level	
Actions for detected threats	
Enable network protection	
Scan emails	
Number of days (0-90) to keep quarantined mal...	
Time of day to run a scheduled scan	
Defender Cloud Extended Timeout In Seconds	
Defender Processes to exclude	
Run daily quick scan at	
Scan all downloaded files and attachments	
Action to take on potentially unwanted apps	
Day of week to run a scheduled scan	
Turn on cloud-delivered protection	
Scan network files	
Disable catch-up quick Scan	




Real-time protection
Turn on real-time protection
Yes
Enable on access protection
Not configured
Monitoring for incoming and outgoing files
Monitor all files
Turn on behavior monitoring
Not configured
Turn on intrusion prevention
Not configured
Enable network protection
Enable
Scan all downloaded files and attachments
Yes
Scan scripts that are used in Microsoft browsers
Not configured
Scan network files
No
Scan emails
No


Scan
Scan archive files
Not configured
Use low CPU priority for scheduled scans
Yes
Disable catch-up full scan
Not configured
Disable catch-up quick Scan
No
CPU usage limit per scan
25
Scan mapped network drives during full scan
Not configured

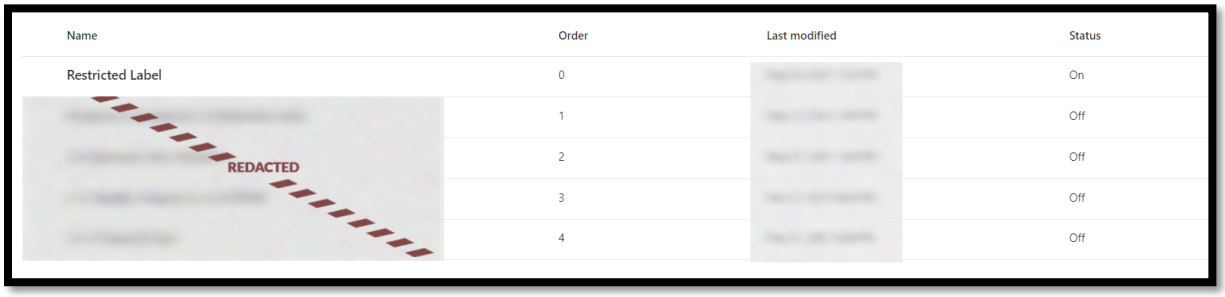
While many of the settings were well configured, room for improvement still exists. Behavior monitoring, intrusion prevention, email scanning, network drive scanning, and archive file scanning should all be enabled to further harden the security of endpoint devices. Furthermore, 19 devices were flagged as unhealthy, citing antivirus signatures to be out of date. This is not an indicator of malware or abnormal activity from those endpoints, but rather an update to the antivirus that had not been applied during the testing period.

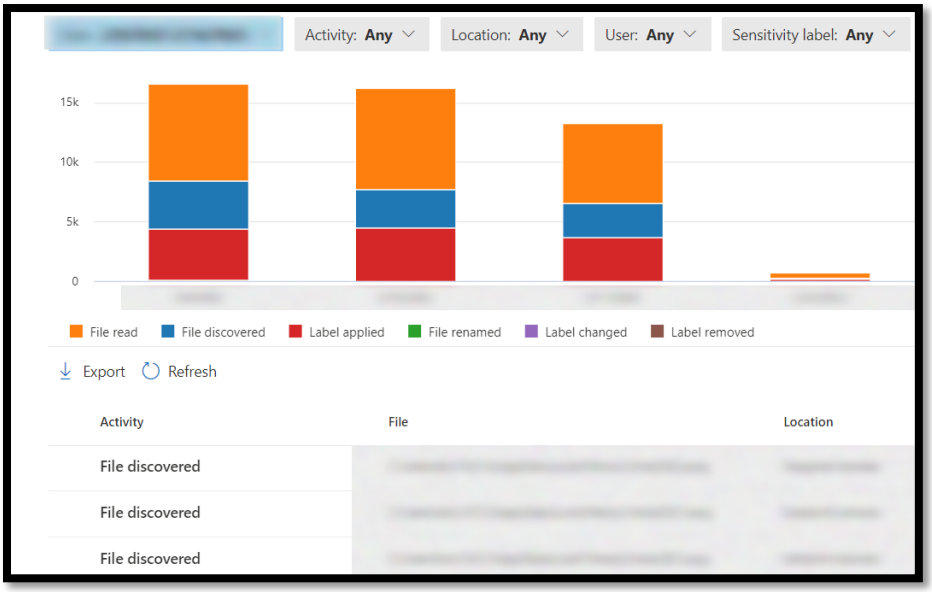


The other two unhealthy devices had malware protection disabled or not running entirely.

Device name	Malware protecti...	Signature update...	State	Real-time protect...	Product status
[redacted]	Disabled	False	Clean	Disabled	No issues
[redacted]	Disabled	False	Clean	Enabled	Service not running

Abacus Group noted the presence of data loss prevention (DLP) policies in place, although several of the custom polices had been disabled in [DATE] in favor of a restricted label policy. Additional insight into DLP was gained by analyzing the labeling actions of endpoint devices. This indicates that DLP is configured on endpoints to automatically detect and prevent data misclassification and loss.



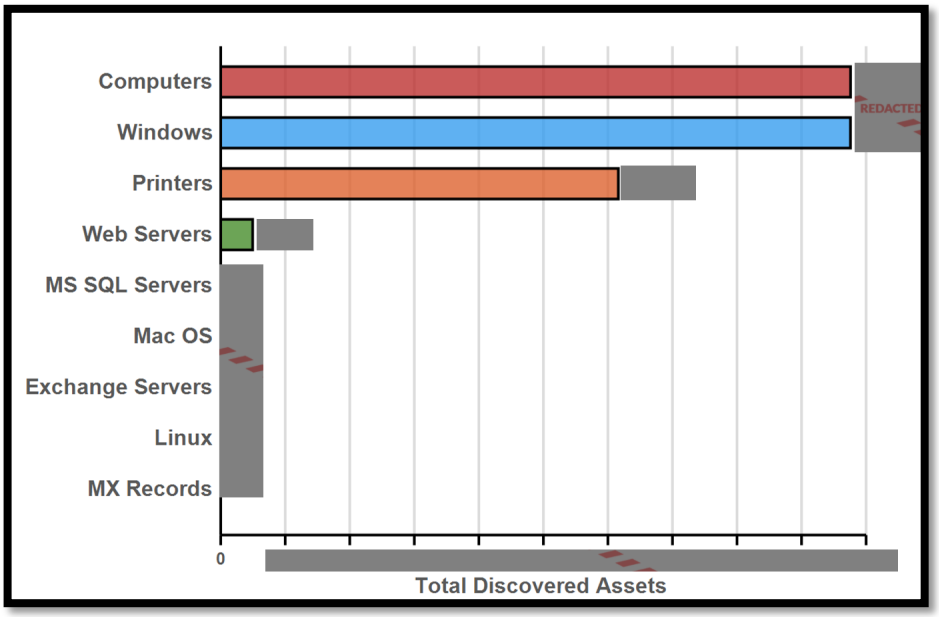


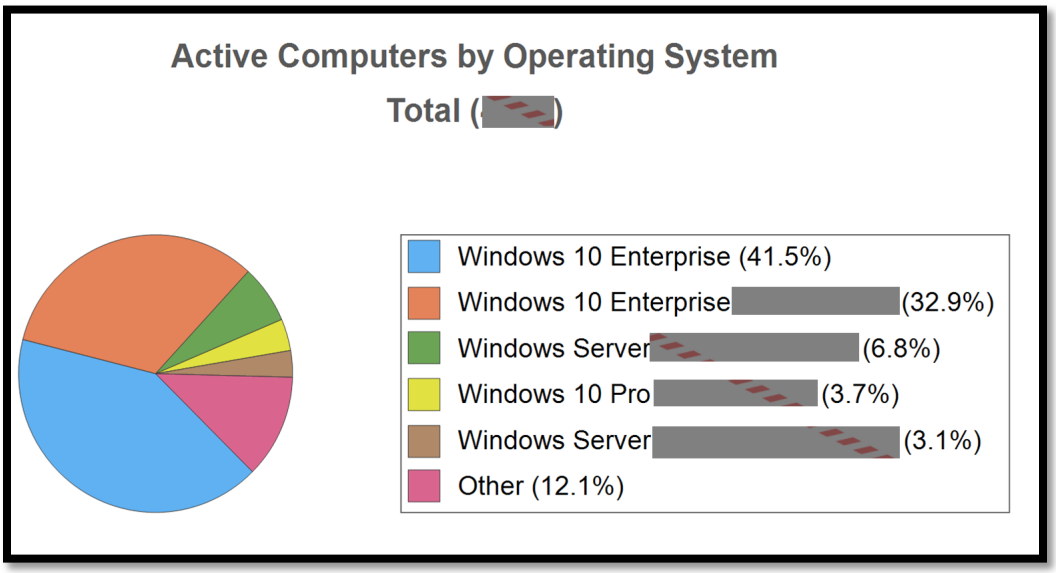
Network Segmentation and Configuration Analysis

Network analysis began with an in-depth look at the on-premises Active Directory environment and associated devices. This was accomplished using a tool called Network Detective which was run on [CLIENT]'s internal network as a domain administrator in conjunction with the [CLIENT] IT team. Abacus Group's security engineers initially collected data to understand the size and scope of the environment and to assess any security vulnerabilities present that were not detected during the previous black box internal penetration test. Initial analysis determined an inventory of systems, software versions, active and inactive users, and security group distribution. Next, detailed analysis of user permission levels and any permissible file shares were analyzed to determine the prevalence of role-based access controls (RBAC) and access control lists (ACLs) in the environment.

Automated Analysis of Active Directory

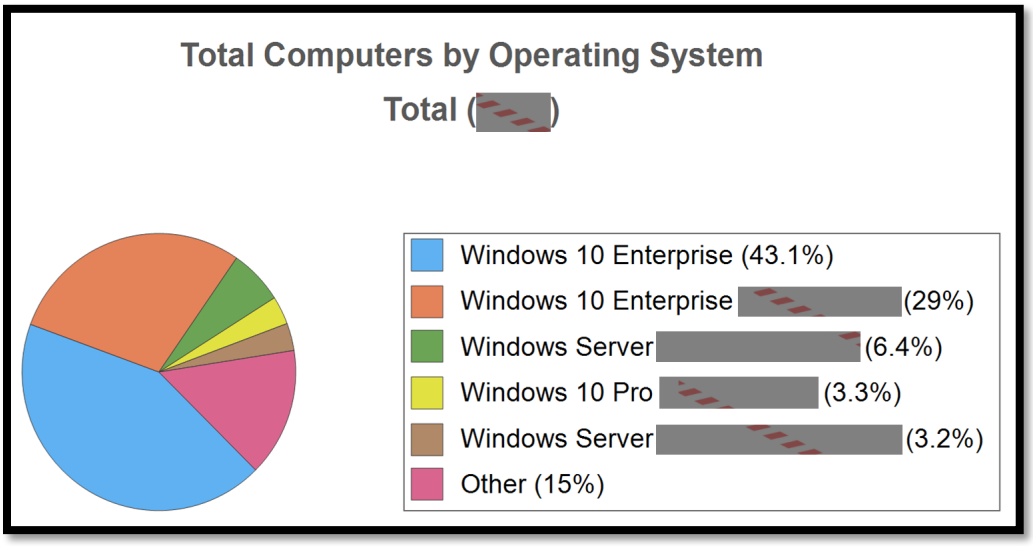
Task	Description
Detect Domain Controllers	Identifies domain controllers and online status.
FSMO Role Analysis	Enumerates FSMO roles at the site.
Enumerate Organization Units and Security Groups	Lists the organizational units and security groups (with members).
User Analysis	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
Detect Local Accounts	Detects local accounts on computer endpoints.
Detect Added or Removed Computers	Lists computers added or removed from the Network since the last assessment.
Detect Local Mail Servers	Detects mail server(s) on the network.
Detect Time Servers	Detects server(s) on the network.
Discover Network Shares	Discovers the network shares by server.
Detect Major Applications	Detects all major apps / versions and counts the number of installations.
Detailed Domain Controller Event Log Analysis	Lists the event log entries from the past 24 hours for the directory service, DNS server and file replication service event logs.
Web Server Discovery and Identification	Lists the web servers and type.
Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
Internet Access and Speed Test	Tests Internet access and performance.
SQL Server Analysis	Lists the SQL Servers and associated database(s).
Missing Security Updates	Identifies computers missing security updates.
System by System Event Log Analysis	Discovers the five system and app event log errors for servers.

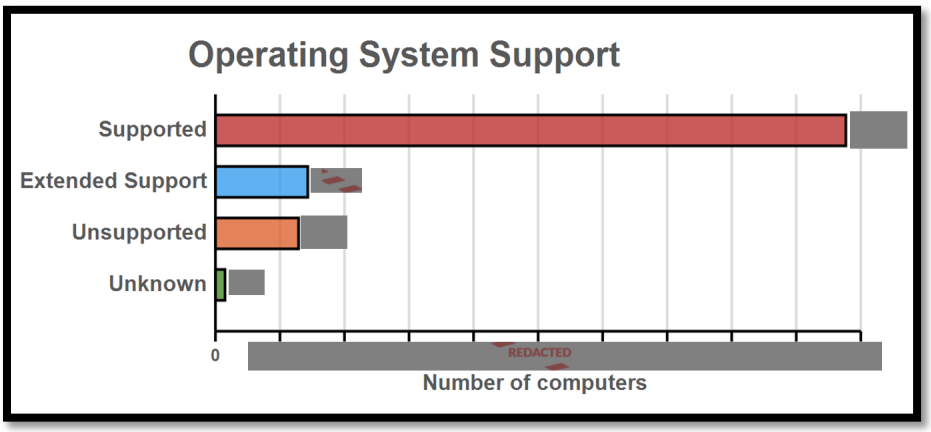


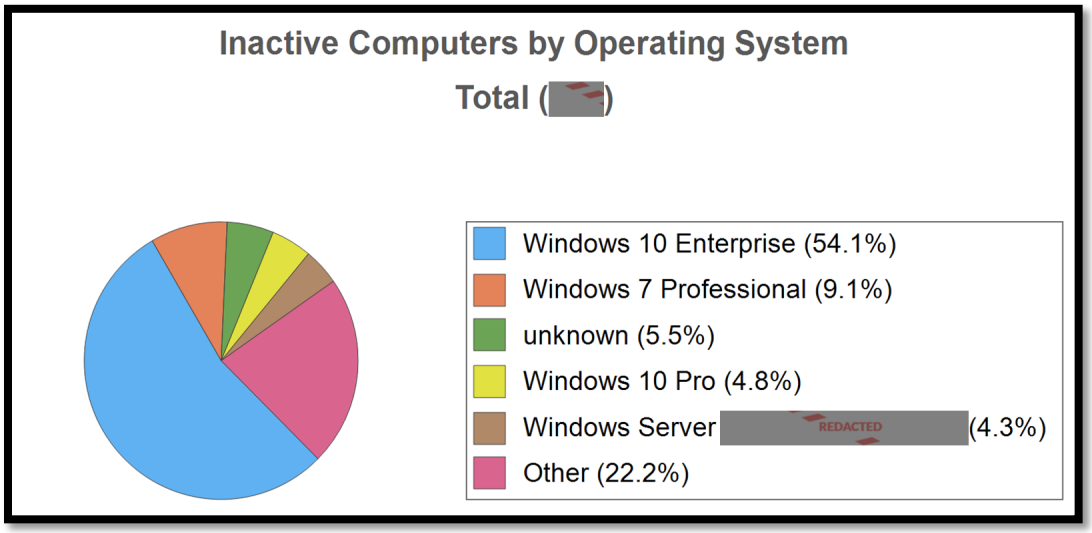


Operating System	Total	Percent
Top Five		
Windows 10 Enterprise		41.5%
Windows 10 Enterprise		32.9%
Windows Server		6.8%
Windows 10 Pro		3.7%
Windows Server		3.1%

Operating System	Total	Percent
Total - Top Five		87.9%
Other		
Windows		2.1%
Windows		1.5%
Windows		1.4%
Windows		1.3%
unknown		1%
Windows		0.9%
Windows		0.7%
Windows		0.7%
Windows		0.5%
Windows		0.3%
Windows		0.3%
Windows		0.3%
Windows		0.2%
Windows		0.2%
Windows		0.2%
Windows		0.1%
Windows		0.1%
NetApp R		0.1%
Unidentit		0%
Windows		0%
Windows		0%
Windows		0%
Windows		0%
macOS		0%
NetApp R		0%
Windows		0%
Windows		0%
Total - Other		12.1%
Overall Total		100%



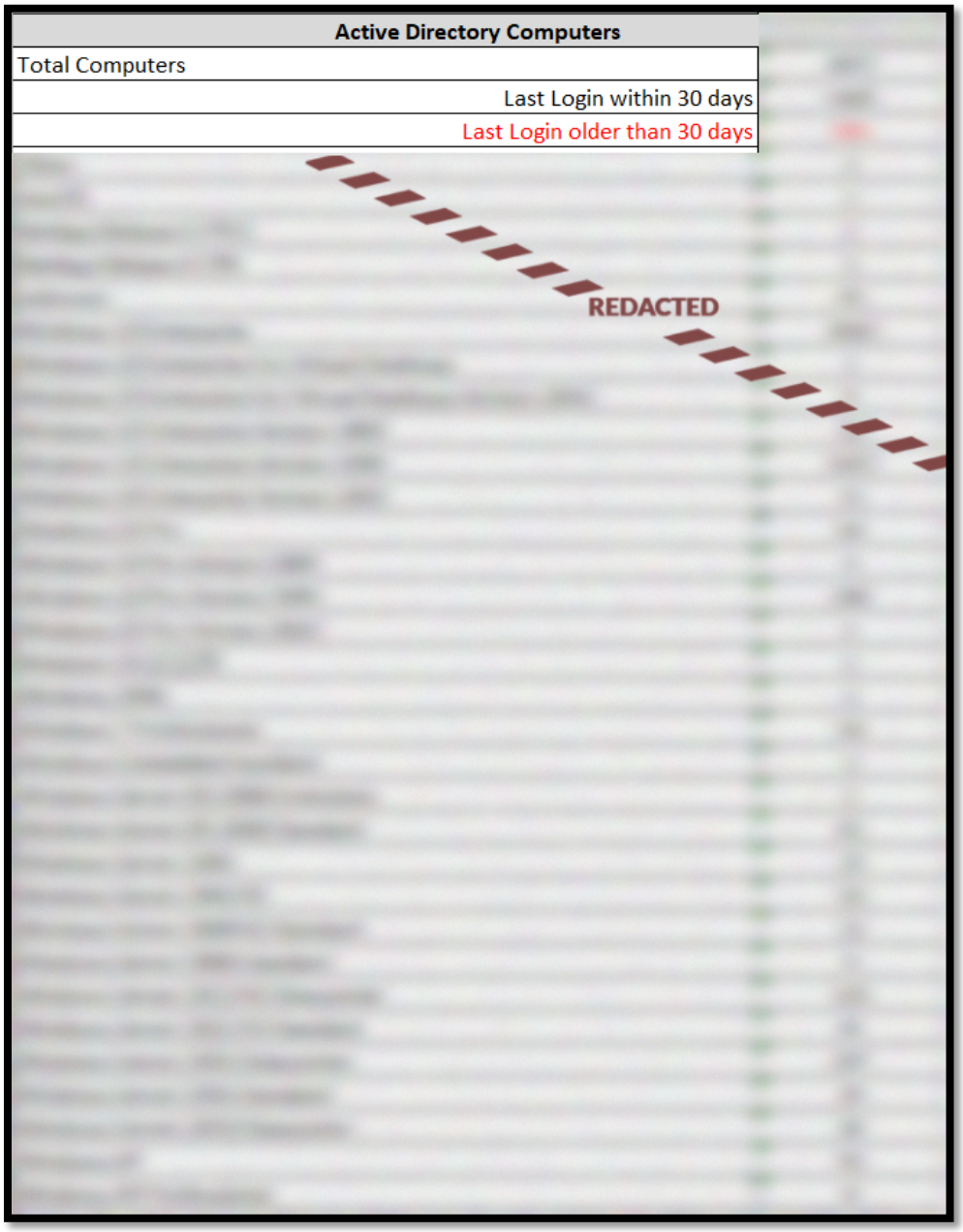


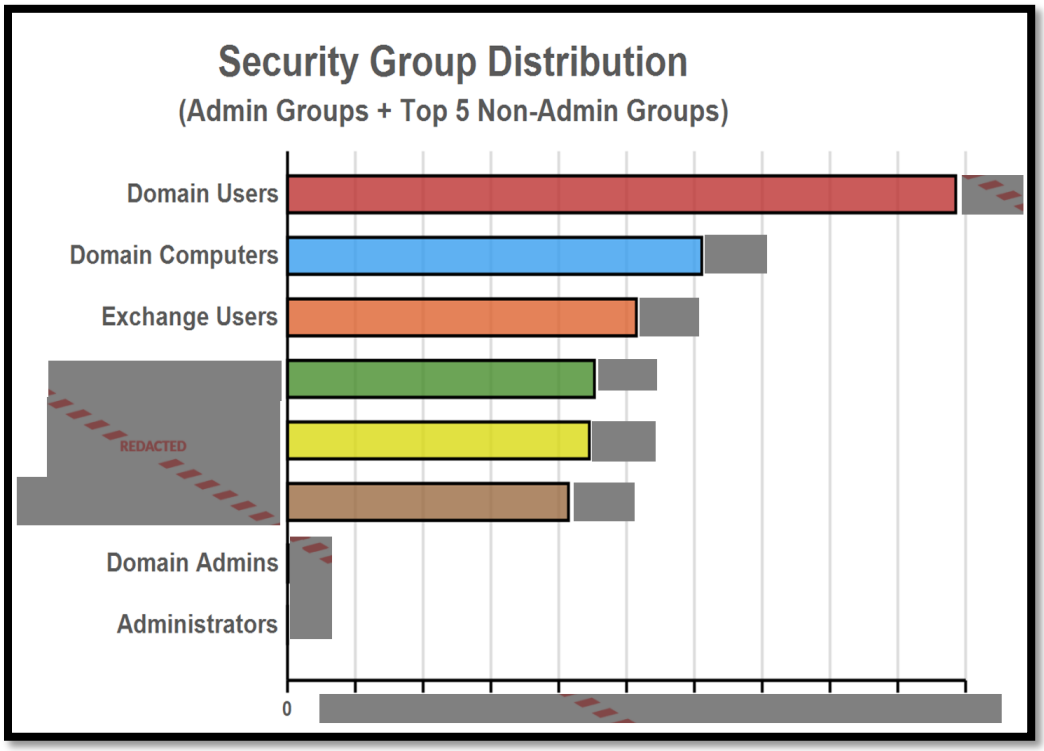


*Not logged into Active directory in the last 30 days

Domain	
Domain Controllers	
Number of Organizational Units	
Users	
# Enabled	
	Last Login within 30 days
	Last Login older than 30 days
# Disabled	
	Last Login within 30 days
	Last Login older than 30 days

Active Directory Computers	
Total Computers	
	Last Login within 30 days
	Last Login older than 30 days

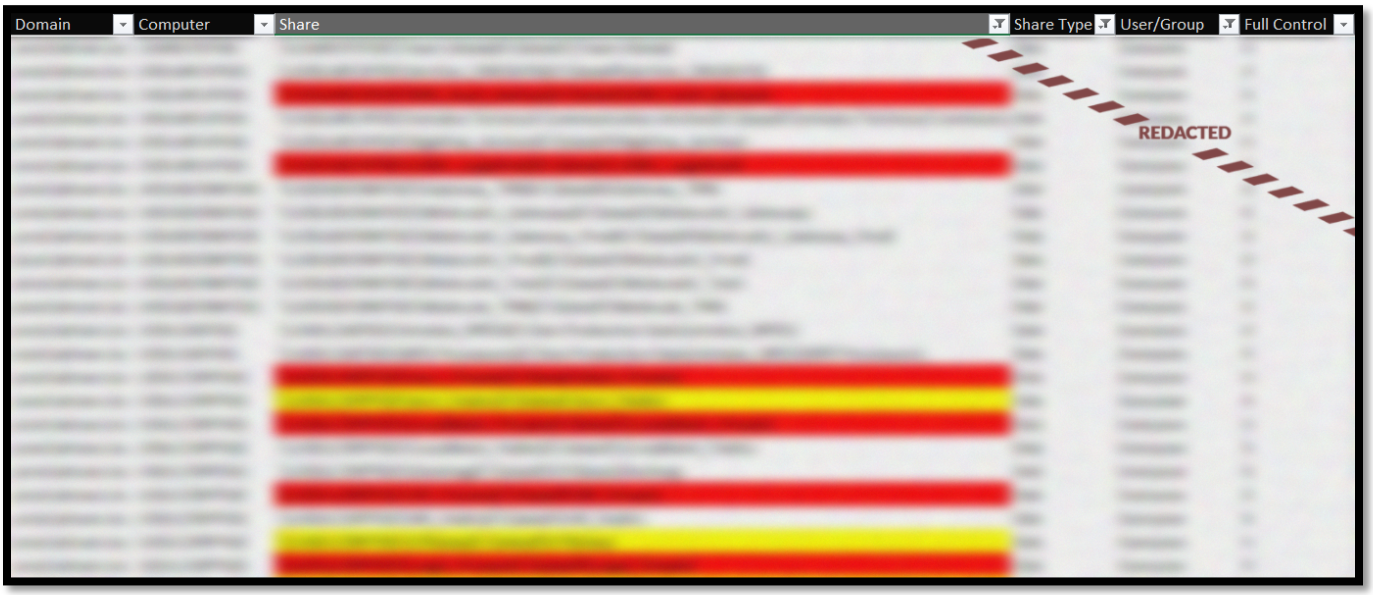




A significant anomaly, and largest security risk to the environment, was the large number of devices running end of life operating systems. This was identified as a high-risk finding in the [DATE] Internal penetration testing report, however, the scale of legacy devices proved to be far more widespread than had been identified in that assessment. A complete list of legacy devices with unsupported software can be seen in appendix A of this report.

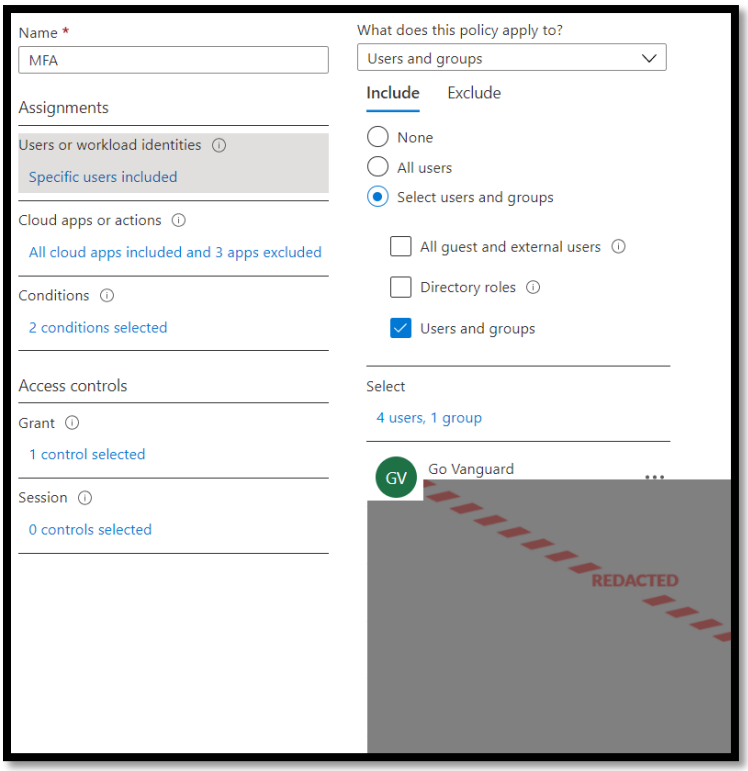
Computer	Operating System	OS Install Date	Age (months)
REDACTED			

Analysis next shifted to an in-depth analysis of network shares and the associated permission levels of user groups. This revealed a general lack of role-based access controls (RBAC) with numerous sensitive shares accessible to every active directory user. This included financial, legal, logs, backups and private human resources data among potentially proprietary engineering and operations information. In most cases, the level of access was full read and write capabilities, meaning any user on the network can modify, delete or cryptographically lock files. This represented the most severe finding in this report as a malicious actor would be able to commit a ransomware attack without having to launch any exploits, run any scans, or compromising any critical infrastructure.

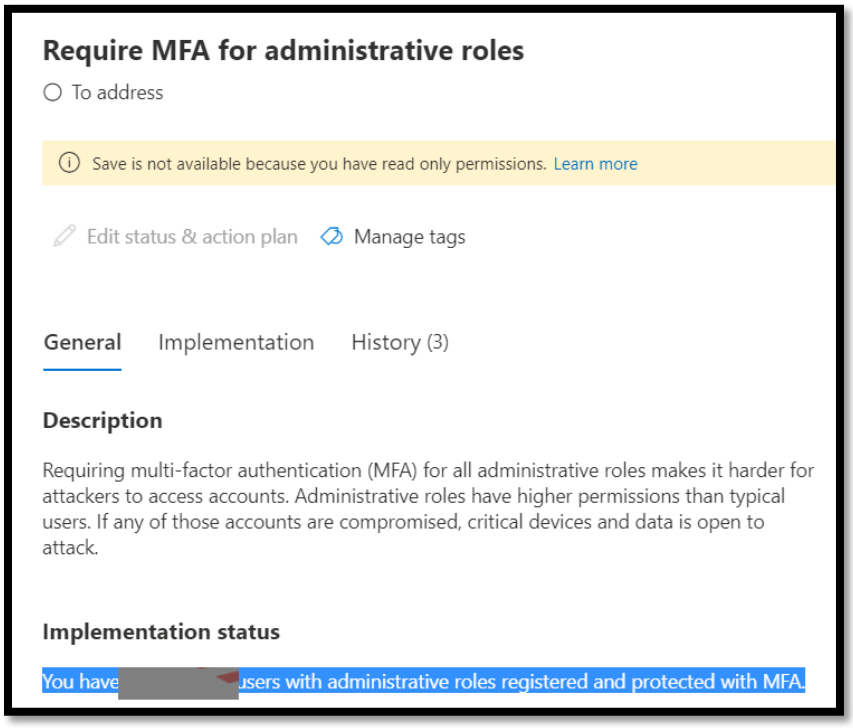


Office 365 Configuration Analysis

Analysis of [CLIENT]'s Office 365 environment began with identifying the configured user groups, conditional access policies, and the prevalence of multifactor authentication. Findings revealed a well configured environment with access and controls assigned appropriately to groups and conditional access policies universally implementing MFA for users. Additional policies related to securing accounts, implementing additional safeguards, and disabling legacy authentication were also observed.



One anomaly in the enforcement of MFA was identified with respect to administrator accounts, as [REDACTED] of the [REDACTED] total users with administrative roles were not protected with MFA.

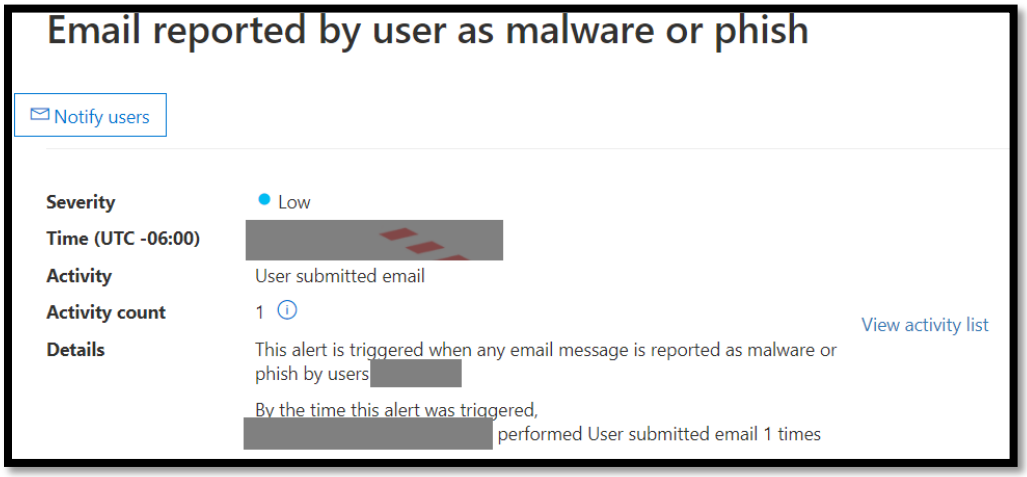


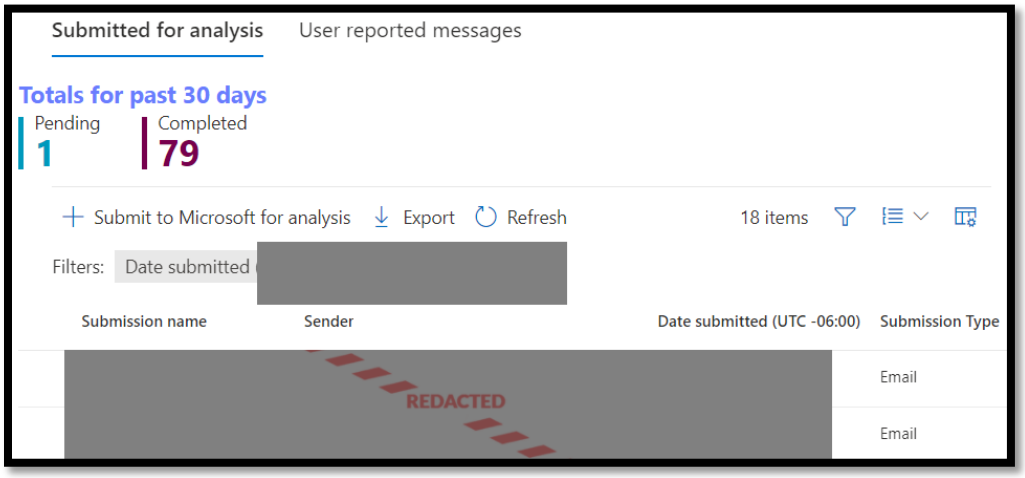
Closer inspection of these accounts revealed that they were service accounts with exceptions purposefully included, not an oversight or misconfiguration. This conclusion was corroborated by the [CLIENT] IT team.

Abacus Group next analyzed security configurations in Microsoft Defender for Office 365. Additional improvements could be made to anti-phishing safeguards by enabling impersonated user and domain protection. This will help mitigate sophisticated phishing attacks in which malicious actors utilize typo-squatted domains to impersonate legitimate users.

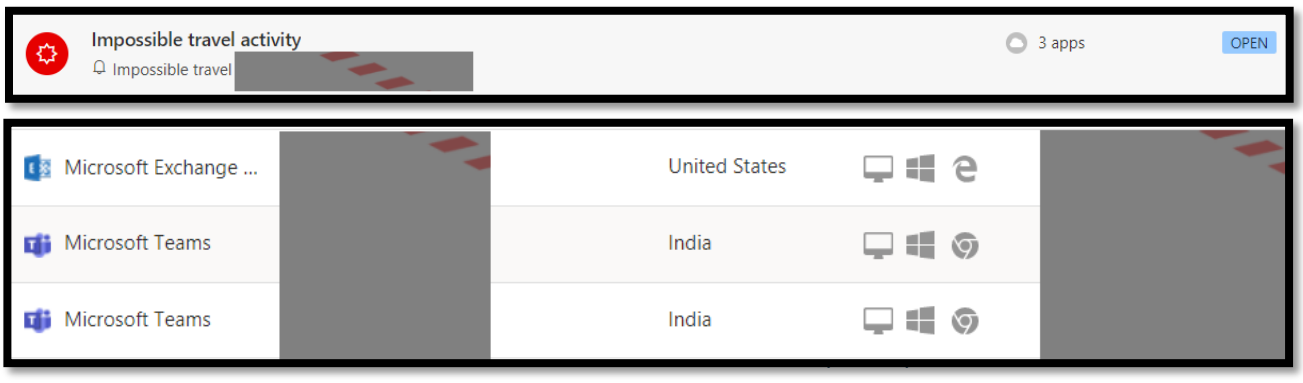
Policy ↓	Policy group/setting name	Policy type	Current configuration
Office365 AntiPhish Default	Add users to protect	Anti-phishing	[redacted]
Office365 AntiPhish Default	Automatically include the domains I own	Anti-phishing	
Office365 AntiPhish Default	Include custom domains	Anti-phishing	
Office365 AntiPhish Default	If email is sent by an impersonated user	Anti-phishing	
Office365 AntiPhish Default	If email is sent by an impersonated domain	Anti-phishing	
Office365 AntiPhish Default	Enable Intelligence for impersonation protection (Rec...	Anti-phishing	

However, Abacus Group also observed an instance of end users reporting a potential phishing email which generated an alert to tenant administrators. This example demonstrates an effective combination of end user security awareness and well configured policy which enabled the [CLIENT] security team to further investigate the instances. Analysis of reported phishing emails shows a timely and effective response process.





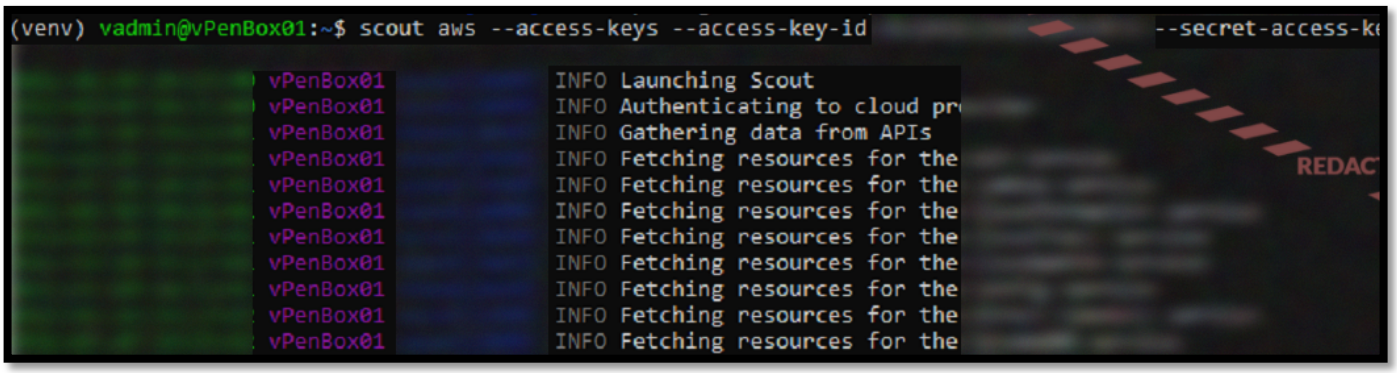
The presence of alerts related to impossible travel was also observed. Impossible travel is an authentication safeguard in which multiple login attempts from geographically distant locations within impossible timeframes get flagged or blocked. In the demonstrated case, logging in from the United States and India occurred within twenty minutes. While this instance is likely a false positive due to the use of a VPN for legitimate work purposes, this implementation is considered a security best practice.



Analysis of [CLIENT]'s AWS environment began with utilizing a publicly available multi-cloud auditing tool called ScoutSuite to gather configuration data and analyze the overall security posture. This was

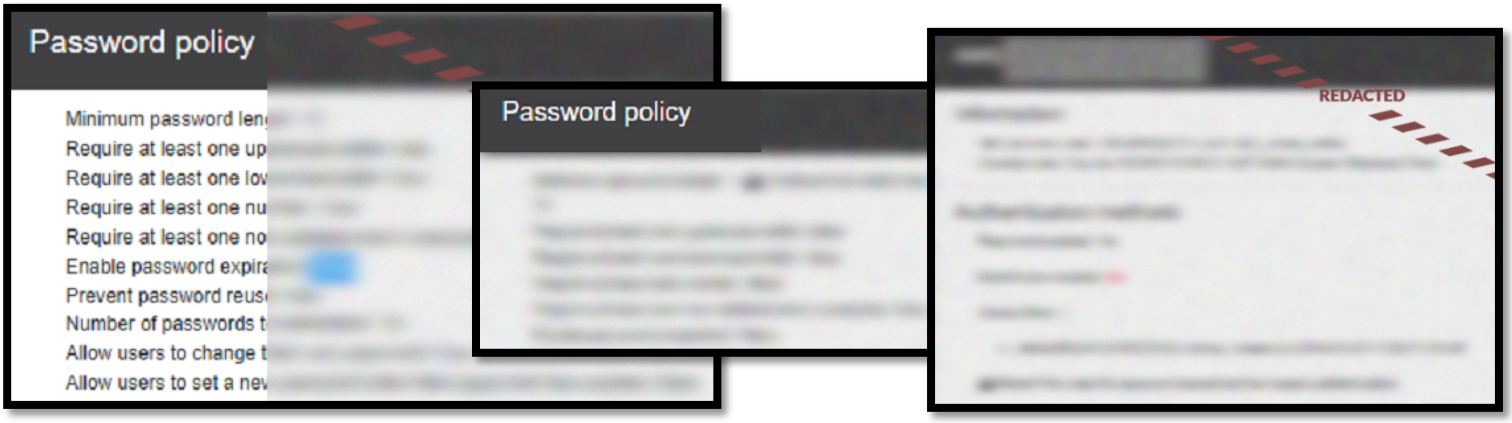
performed on the following domains utilizing API keys generated by [CLIENT]'s IT team for the purposes of this engagement.

- **[REDACTED]**
- **[REDACTED]**
- **[REDACTED]**
- **[REDACTED]**
- **[REDACTED]**
- **[REDACTED]**
- **[REDACTED]**



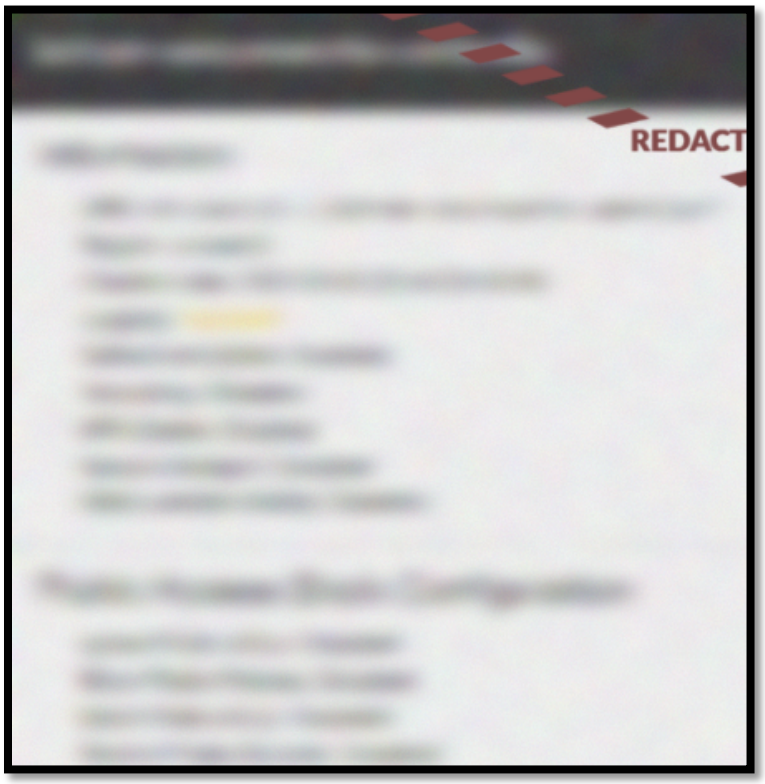
The aggregation of this data provided Abacus Group security engineers the ability to assess numerous components of the AWS environment. Analysis began with Identity and Access Management (IAM) policies surrounding passwords and multifactor authentication, access levels and groups.

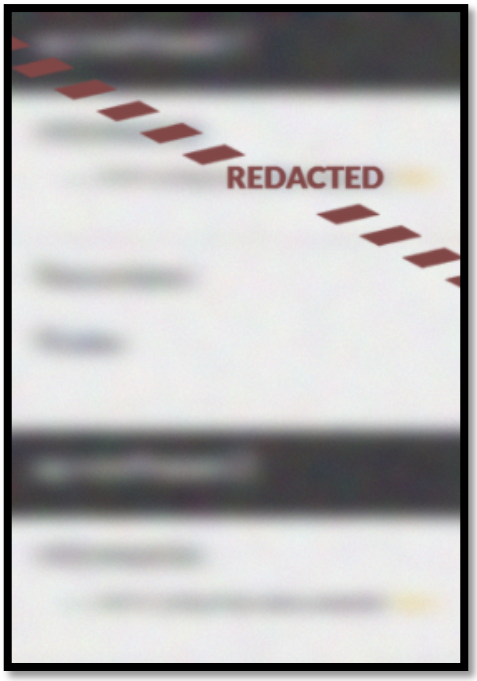
Among the eight domains analyzed, there were a few common themes that were identified to be problematic from a security standpoint. First, password policies are inconsistently configured with some domains having weak and default rules. In some cases, there were [REDACTED], [REDACTED], and [REDACTED].



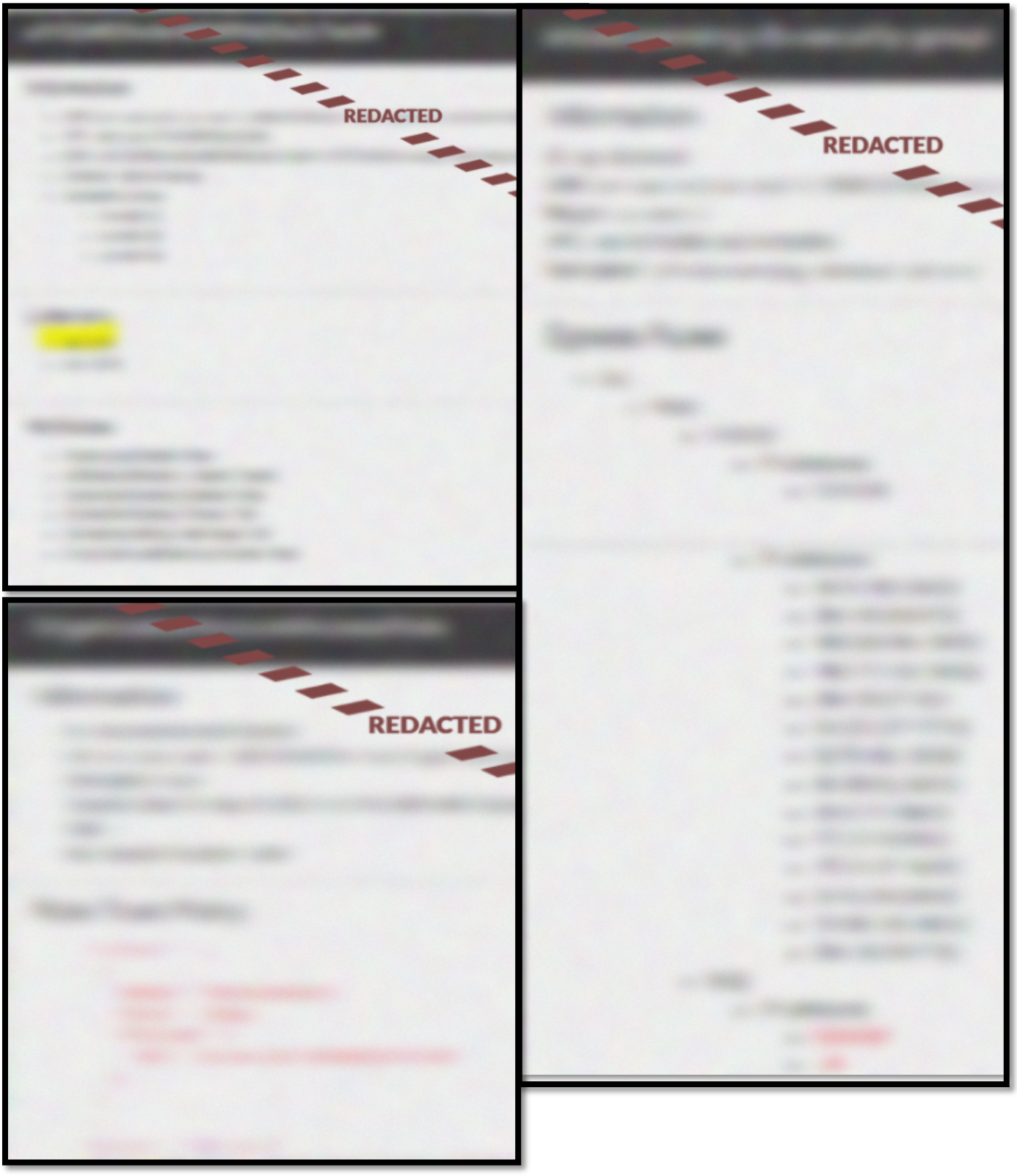
Abacus Group also identified a total of [REDACTED] accounts, primarily administrators, that did not have multifactor authentication enabled. One account of particular concern was the [REDACTED]. The lack of MFA misses out on a critical piece of protection in the event that credentials become compromised through a data breach or social engineering attack.

Another major theme across the entire environment was little to no logging enabled which reduces the situational understanding of potential security anomalies. Specifically, CloudTrail was not enabled on any domain, which is generally considered an AWS best practice for logging API activity. Additional logging improvements could also be made on domains such as [CLIENT] [REDACTED] which was identified as not having AWS Config recorders enabled. AWS Config recorders log changes in AWS resource configuration and the lack of this insight may hamper security analysis, change tracking, and compliance auditing efforts in the future. Furthermore, S3 buckets were also identified with logging disabled.





Additional security concerns were identified such as a load balancer in the [REDACTED] domain allowing clear text HTTP communication, cross-account role assumption not requiring external authentication or MFA, [REDACTED] [REDACTED] externally exposed on port [REDACTED], and default configurations of S3 buckets and EBS volumes lacking data-at-rest encryption.



Policy and Procedures Analysis

At the commencement of this project the [CLIENT] security team informed Abacus Group that their organization was in the process of creating a formally codified written information security program. A written information security program (WISP) is a document (or set of documents) that details an organization's security controls, processes, and policies. Every formally codified WISP should ideally be aligned with well-known and lean security frameworks such as CISv8 or NIST CSF and reference to various industry standards such as utilizing *NIST SP 800-88 Guidelines for Media Sanitization* for securely wiping sensitive data from old hard drives. With that context, Abacus Group focused the analysis processes on the policies and procedures documentation that [CLIENT] did have and provided feedback specific for those documents. Abacus Group was provided the following documentation by [CLIENT] to analyze from a security and compliance standpoint in tandem with this engagement.

Document Title	File Type
[REDACTED]	PNG
[REDACTED]	PNG
[REDACTED]	PDF
[REDACTED]	PDF
[REDACTED]	DOCX
[REDACTED]	PDF
[REDACTED]	DOCX
[REDACTED]	DOCX
[REDACTED]	DOCX
[REDACTED]	DOCX
[REDACTED]	DOCX
[REDACTED]	DOCX
[REDACTED]	PDF

During the policy review process, it was noted that there were several documents that referred to other documents that were provided for review. Those references included:

- **[REDACTED]**
- **[REDACTED]**
- **[REDACTED]**
- **[REDACTED]**

It was observed that some documents were not formalized policies but screenshots or email correspondence. For example, the "[REDACTED]" is a forwarded email that contains a link to contract NDAs. The "[REDACTED]" is also a screenshot of contact information for points of contact within the [REDACTED] Department.

Key items for compliance standards can be addressed with the development of the missing documents listed above. Typical compliance items such as data encryption can be elaborated through a Data Handling Policy, while removable media and password standards can be addressed through an Acceptable Use Policy. Some items are also already in progress but require more formalized documentation. The "[REDACTED] – OneNote" item describes the process for rolling out production server recovery which addresses concerns for CIS v8 Controls and NIST CSF recovery

functions – all of which can be developed through the [REDACTED] and [REDACTED] documentation. While [CLIENT]'s [REDACTED] document is extremely thorough and robust; it incorporates policy, procedure, plan and checklist elements all within one monolithic document that may be difficult for security staff to quickly refer and read through during an ongoing incident. To that note, it is recommended that at least the incident response [REDACTED] be separated into a separate document that does not contain any unnecessary "fluff" when someone is in the process of handling an incident.
To best manage policies and procedures Abacus Group recommends a lean approach that focuses on being specific and concise that is closest to engineers and users (usually a wiki like system such as Confluence). Given that a significant amount of [CLIENT]'s systems are within the Microsoft ecosystem, measuring the efficacy of compliance with company policies would most likely best accomplished with Microsoft 365 Compliance manager which is bundled with E5 licenses. In particular Microsoft 365 Compliance has the ability to ingest and evaluate the configurations of Office365 services, Defender services, Intune, Secure Score, and Azure systems. Unfortunately, AWS systems are not yet evaluated but Microsoft 365 Compliance manager and likely an open-source tool like Prowler should be utilized to evaluate AWS primitives and configurations against CIS controls.

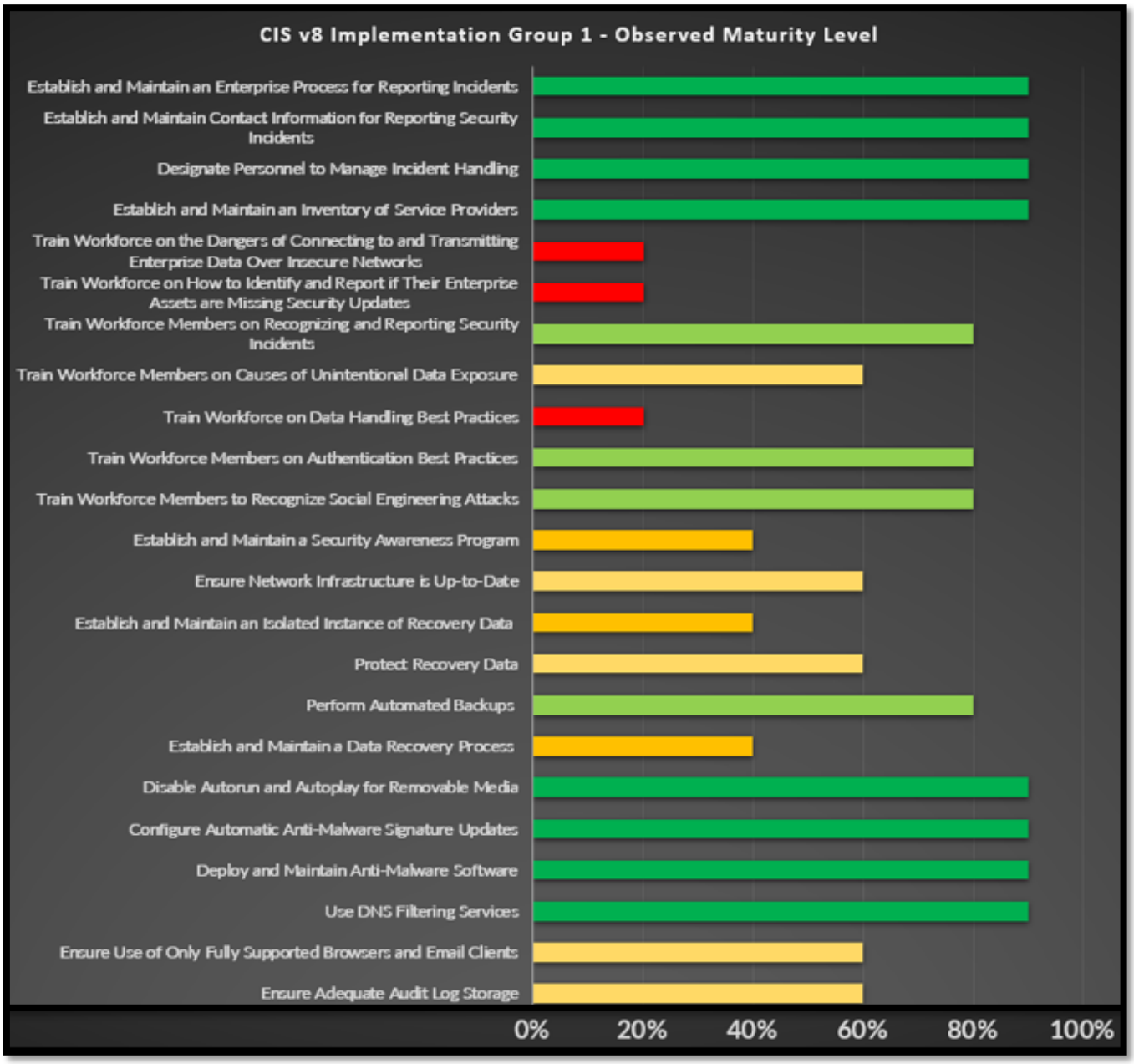
It would be ideal if the Microsoft 365 Compliance CIS assessment dashboards were reviewed on at least a quarterly cadence to ensure a consistent burn-down of security control gaps while also ensuring that new gaps do not appear from unintended regressions. CIS specific references for security control implementation recommendations and security hardening is also provide below. The provided recommendations do not incur any additional opex or capex expenditures beyond staff time configuring and reviewing Microsoft 365 Compliance manager.

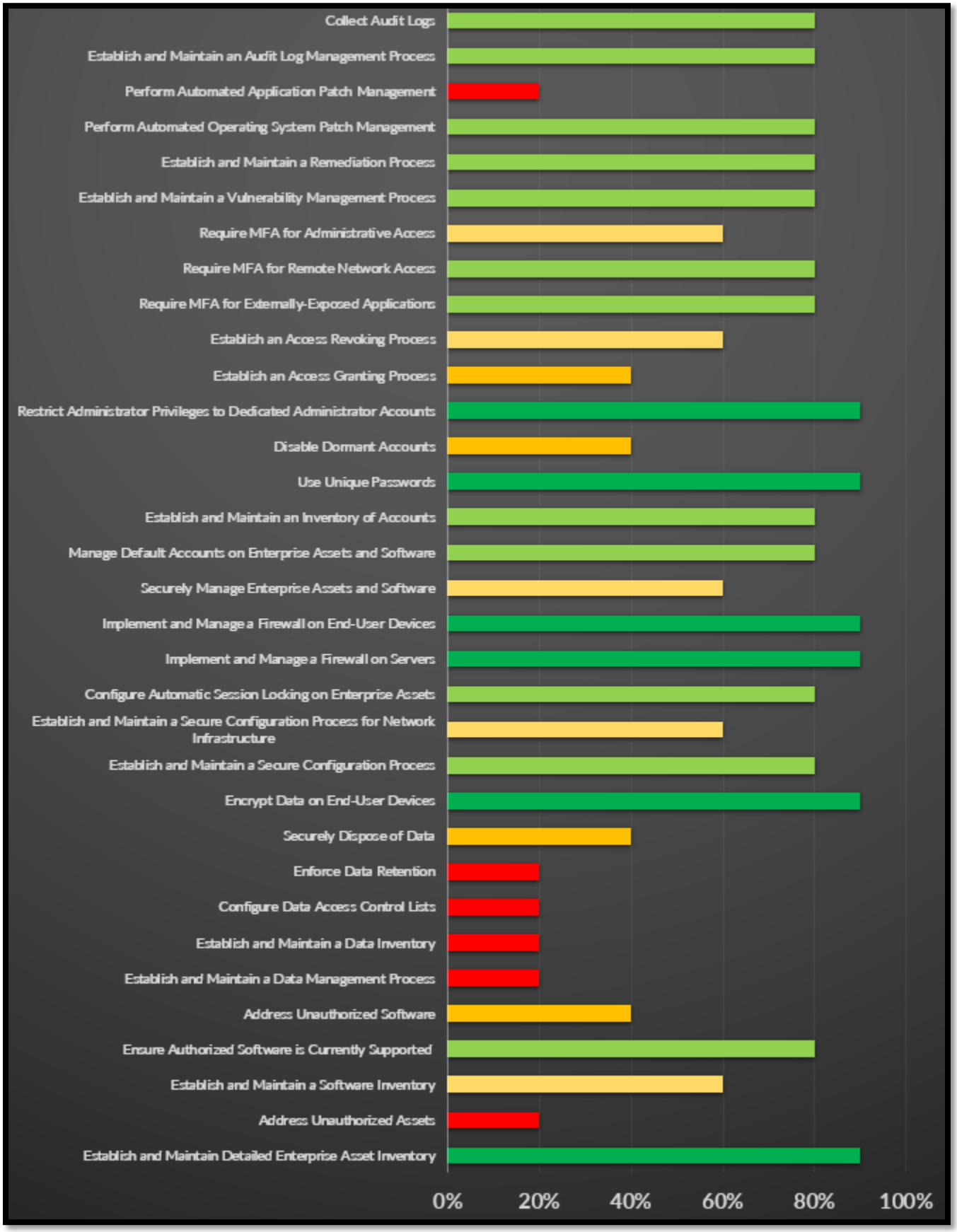
Specific Resources:

Microsoft 365 Compliance Manager helps automatically evaluate and manage your organization's compliance requirements. There are multiple compliance check-list templates that are provided including for CIS which can also be modified and customized.
Microsoft Compliance Configuration Analyzer for Compliance Manager is a preview PowerShell-based utility that will fetch your organization's current configurations and validate them against Microsoft 365 recommended best practices. MCCA can help you quickly see which improvement actions in Compliance Manager apply to your current Microsoft 365 environment. Each action identified by MCCA will give you recommendations for implementation, with direct links to Compliance Manager and the applicable solution to start taking corrective action.
CIS Microsoft Azure Foundations Benchmark provides a step-by-step checklist for securing Azure.
CIS Hardened Images on Microsoft Azure are Azure certified and preconfigured to the security recommendations of the CIS Benchmarks. They are available on both Azure and Azure Government.
Azure Blueprint for CIS Microsoft Azure Foundations Benchmark helps customers deploy a core set of policies for any Azure-based architecture that must implement CIS Azure Foundations Benchmark recommendations.
Azure Policy recommendation mapping provides details on policy definitions included within the above Blueprint and how these policy definitions map to the compliance domains and controls in CIS Microsoft Azure Foundations Benchmark. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions.

CIS Controls Cloud Companion Guide provides guidance on applying security best practices in CIS Controls Version 7 to cloud environments.
CIS Microsoft 365 Foundations Benchmark provides prescriptive guidance for establishing a secure baseline configuration for Microsoft 365.
Microsoft 365 security roadmap: Minimize the potential of a data breach or compromised account by following this roadmap.
Windows security baselines: Follow these guidelines for effective use of security baselines in your organization.

Between policy documents, procedure documents, observed system configurations and technical risks Abacus Group assessed [CLIENT]'s maturity across CISv8 Implementation Group 1 controls.




Collect Audit Logs
Establish and Maintain an Audit Log Management Process
Perform Automated Application Patch Management
Perform Automated Operating System Patch Management
Establish and Maintain a Remediation Process
Establish and Maintain a Vulnerability Management Process
Require MFA for Administrative Access
Require MFA for Remote Network Access
Require MFA for Externally-Exposed Applications
Establish an Access Revoking Process
Establish an Access Granting Process
Restrict Administrator Privileges to Dedicated Administrator Accounts
Disable Dormant Accounts
Use Unique Passwords
Establish and Maintain an Inventory of Accounts
Manage Default Accounts on Enterprise Assets and Software
Securely Manage Enterprise Assets and Software
Implement and Manage a Firewall on End-User Devices
Implement and Manage a Firewall on Servers
Configure Automatic Session Locking on Enterprise Assets
Establish and Maintain a Secure Configuration Process for Network Infrastructure
Establish and Maintain a Secure Configuration Process
Encrypt Data on End-User Devices
Securely Dispose of Data
Enforce Data Retention
Configure Data Access Control Lists
Establish and Maintain a Data Inventory
Establish and Maintain a Data Management Process
Address Unauthorized Software
Ensure Authorized Software is Currently Supported
Establish and Maintain a Software Inventory
Address Unauthorized Assets
Establish and Maintain Detailed Enterprise Asset Inventory
0%
20%
40%
60%
80%
100%

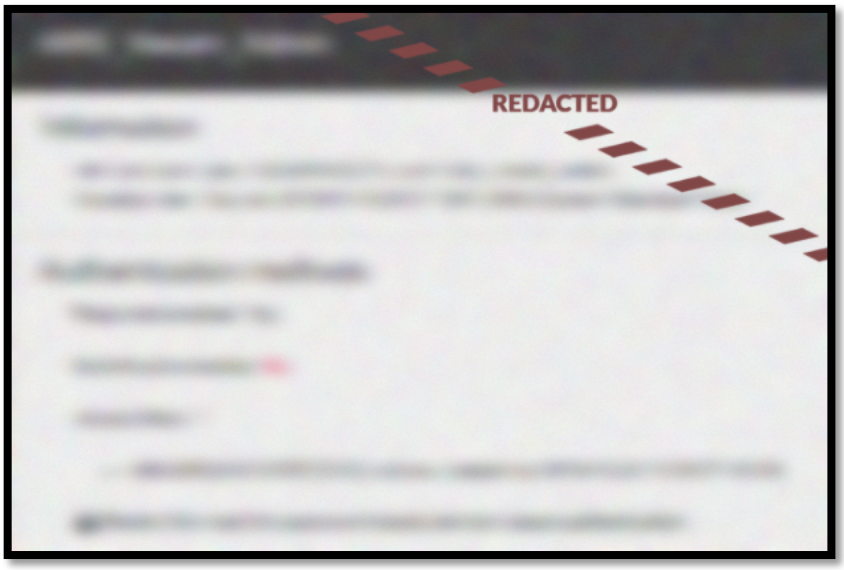
White Box Analysis - Risk Details

Amazon Web Services (AWS) Administrators without Multifactor Authentication Enforced
QoD: 100% | Attack Risk: High | Compliance Risk: Moderate | Remediation Effort: Easy

Summary:
The following AWS administrators do not have MFA enforced on their accounts.

Risk Detection Result(s):

[REDACTED]



Risk Mitigation Recommendation(s):

- **Ensure all root and administrative accounts have MFA enabled.**

Reference(s):
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable.html

Unconstrained Kerberos Delegation
QoD: 100% | Attack Risk: High | Compliance Risk: Moderate | Remediation Effort: Easy

Summary:
Kerberos delegation is a functionality that allows applications to request user credentials to access resources on behalf of that user. Unconstrained delegation essentially allows an entity to impersonate users to any service. This is a very popular, and highly effective, means of lateral movement and privilege escalation in active directory environments.

Risk Detection Result(s):

Risk Mitigation Recommendation(s):

- **Disable delegation if possible. If delegation is required, then consider utilizing constrained delegation in order to restrict which services accounts can impersonate.**

1.

Reference(s):
https://docs.microsoft.com/en-us/defender-for-identity/cas-isp-unconstrained-kerberos

Affected Endpoint(s):
[REDACTED]

End of Life Windows Operating System
QoD: 100% | Attack Risk: High | Compliance Risk: Moderate | Remediation Effort: High

Summary:
The operating system on the host(s) have reached end of life and should not be used in and production capacity. The existence of End Of Life (EOL) / End of Support (EOS) device(s) on the network poses a serious security risk to the organization.

Risk Detection Result(s):

Risk Mitigation Recommendation(s):

- **Host should be recreated with a supported operating system for anything older than Windows 10.**
- **Unsupported versions of Windows 10 should be updated to the latest feature release otherwise they will not receive security updates.**
- **Consider utilizing Microsoft Intune/EMS for managing workstation updates.**
- **If you cannot immediately redeploy servers with EOL/EOS operating systems and cannot disconnect them from the domain, isolate them using network, firewall and GPO controls, limit their ability to right to the domain and strictly limit administrative access to them using local accounts until the they can be replaced or decommissioned, with the utmost priority.**

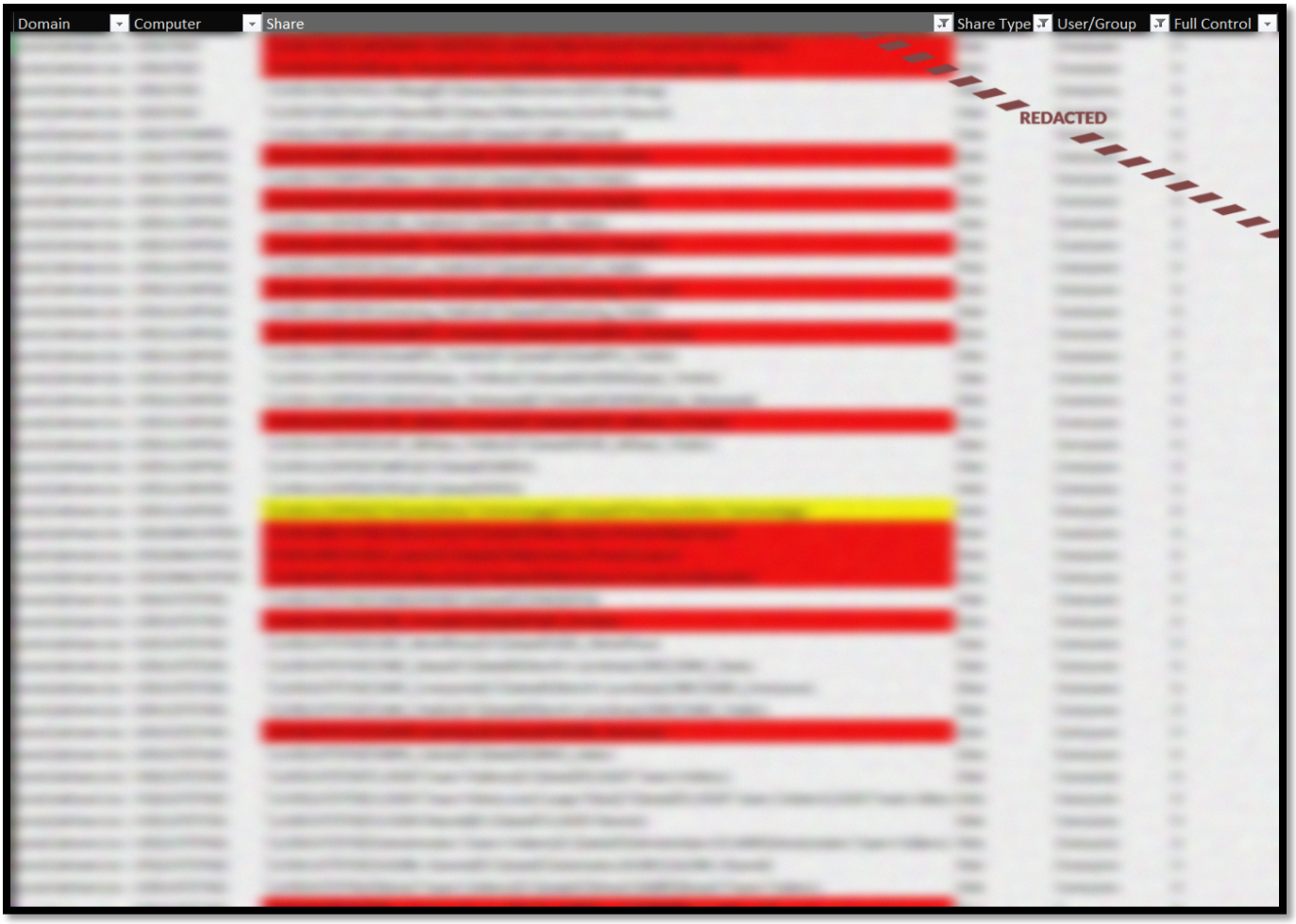
Reference(s):
[REDACTED]
https://en.wikipedia.org/wiki/Windows_10_version_history
https://docs.microsoft.com/en-us/windows/deployment/update/deploy-updates-intune
https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-feature-updates
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/restrict-server-access-to-members-of-a-group-only

Affected Endpoint(s):
See Appendix A for a complete list of affected endpoints

Overly Permissible Windows Fileshares
QoD: 100% | Attack Risk: High | Compliance Risk: Moderate | Remediation Effort: Intermediate

Summary:
The following Windows fileshares appear to have permissions that are beyond the principle of least privilege. Such overly permissible fileshares are frequently employed in ransomware attacks.

Risk Detection Result(s):



A full color-coded breakdown will be provided as a separate supporting document to this report for reference

Risk Mitigation Recommendation(s):

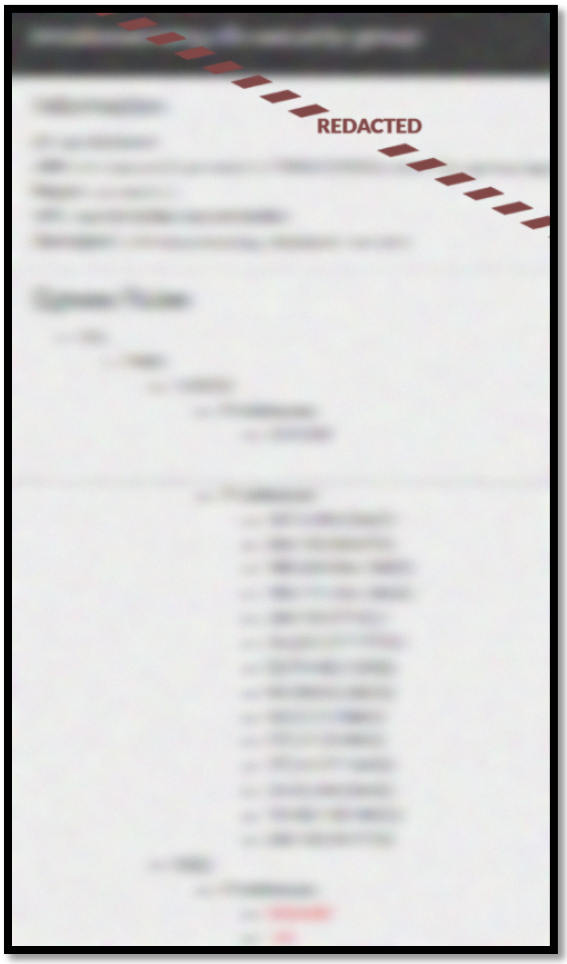
- **Review listed file shares and update permissions accordingly.**
- **Instead of utilizing Everyone permission shares and relying only on NTFS permissions which can vary greatly per directory tree, considers limiting share groups to domain security groups.**

Reference(s):
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780313(v=ws.10)
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd772690(v=ws.10)
https://docs.microsoft.com/en-us/previous-versions/technet-magazine/dd347022(v=msdn.10)

[REDACTED] Externally Exposed Over Port [REDACTED] by Security Group
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Intermediate

Summary:
The identified security group exposes a common port to all source addresses. It is likely that automated scanning tools would identify this resource during a malicious actor's reconnaissance process.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- **If this service needs to be externally exposed then implementing restrictions on the source addresses would reduce the attack surface. Additionally, the highlighted rule above should be removed.**

2.

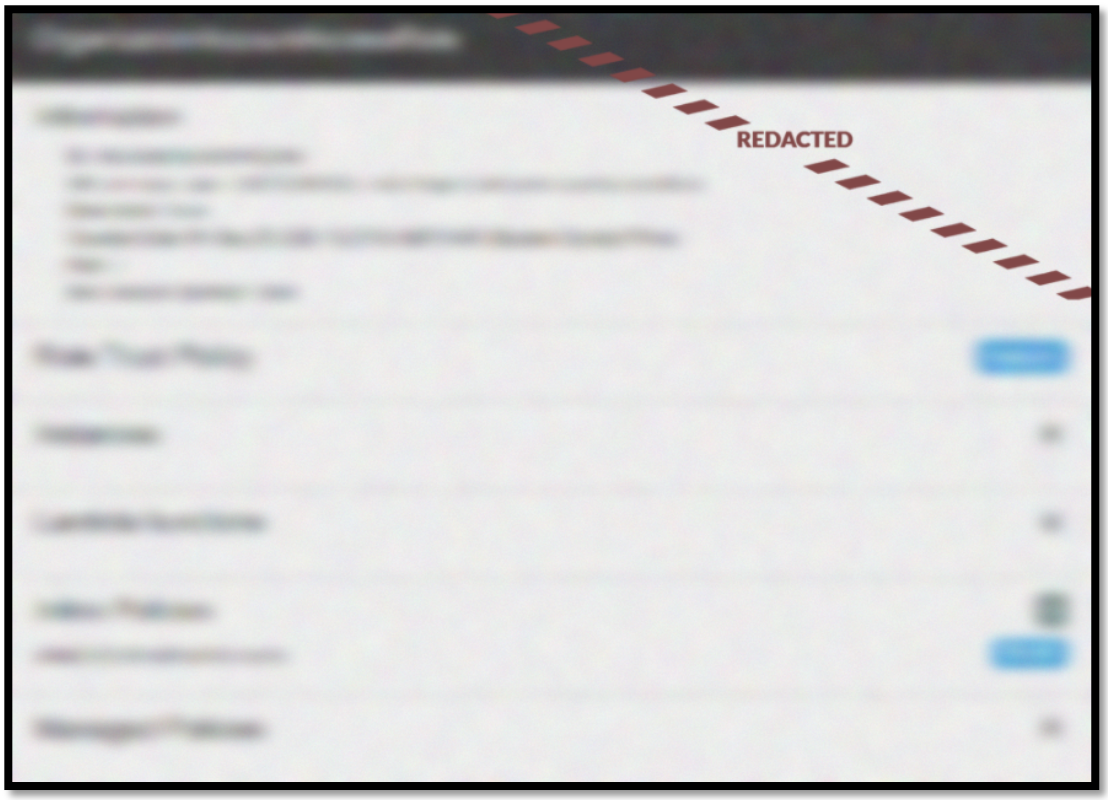
Reference(s):
https://aws.amazon.com/getting-started/hands-on/create-connect-postgresql-db/
https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-creating.html

Affected Security Group(s):
[REDACTED]

Cross-Account AssumeRole Policy Potentially Susceptible to Confused Deputy Attacks QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Intermediate

Summary:
Identified policies related to cross-account role assumption do not require an external identification or MFA. If the role is being used by a service, the external identification requirement effectively mitigates a confused deputy attack. The confused deputy attack refers to a known security issue where an entity of lesser permissions can perform actions on behalf of a more-privileged entity. This attack is used for privilege escalation and requires a previously compromised Azure account in order to be conducted.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

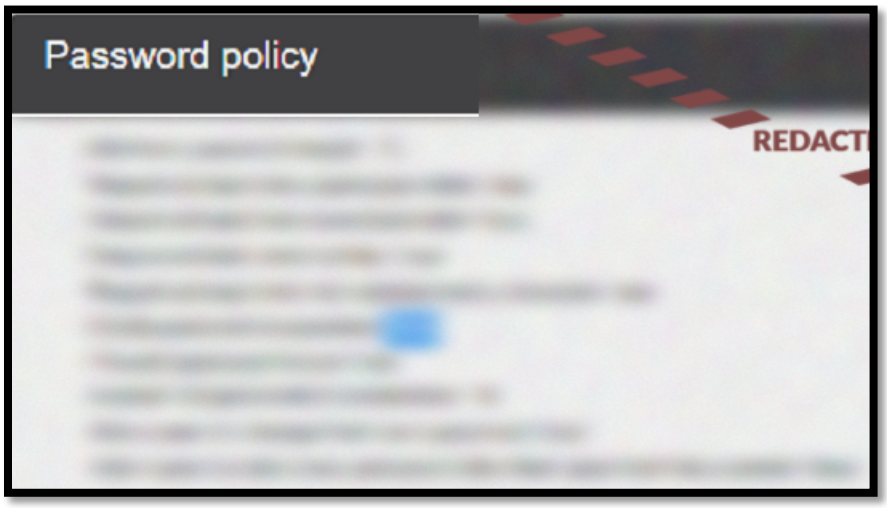
- **Utilize aws:SourceArn and aws:SourceAccount global condition context keys to limit permissions services have to specific resources.**
- **Set External ID with an IAM role trust policy to define who may assume roles.**

Reference(s):
https://research.nccgroup.com/2019/12/18/demystifying-aws-assumerole-and-stsexternalid/
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html
The confused deputy problem - AWS Identity and Access Management (amazon.com)

Weak and Inconsistent Password Policies in AWS Domains
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Easy

Summary:
A discrepancy exists between password policies of different domains with some requiring password length and complexity in line with industry best practices while others have no requirements. This risk is enhanced by the fact that several accounts were identified without MFA being enforced within the AWS environment.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- **Review and update password policies for all cloud tenants to ensure length and complexity requirements are set, passwords are set to expire, and password reuse is prevented.**

Reference(s):
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

End of Life Important Workstation Software
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Intermediate

Summary:
Microsoft Office on the affected endpoints has reached the end of life and should not be used anymore.

Risk Detection Result(s):

Risk Mitigation Recommendation(s):

- **Update to a supported version of Microsoft Office.**

Reference(s):
https://support.microsoft.com/en-us/office/end-of-support-for-office-2010-3a3e45de-51ac-4944-b2ba-c2e415432789

Affected Endpoint(s):
See Appendix A for a complete list of affected endpoints

Unmonitored Domain Controllers
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Intermediate

Summary:
Six domain controllers were identified as being unmonitored by Microsoft Defender for Identity sensors. These sensors provide continuous monitoring and insight into potentially anomalous activity of the endpoints. Lack of endpoint monitoring may hinder the incident response and containment process in the event a malicious actor attempts to exploit these devices.

Risk Detection Result(s):

Risk Mitigation Recommendation(s):

- **Ensure Defender for Identity sensors are configured on each domain controller to ensure consistent situational awareness of the active directory events and changes.**

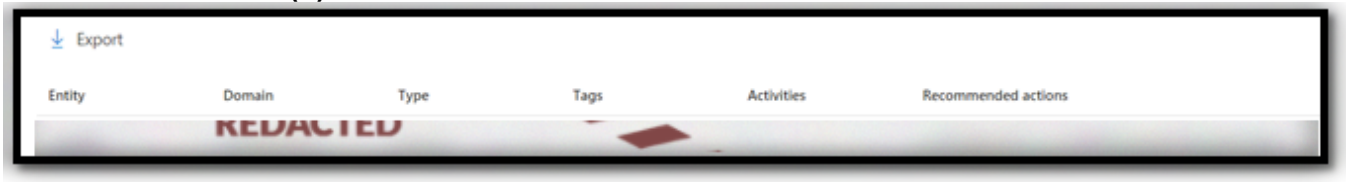
Reference(s):
https://docs.microsoft.com/en-us/defender-for-identity/sensor-monitoring
https://docs.microsoft.com/en-us/defender-for-identity/install-step5

Affected Endpoint(s):
[REDACTED]

Insecure LDAP Simple-Bind Potentially Susceptible to Man-in-the-Middle Attack
QoD: 75% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort:Easy

Summary:
The LDAP simple-bind function provides asynchronous authentication from clients to servers over plain text. In the event of a MitM attack, the passwords could easily be harvested in plain text format resulting in lateral movement or potent privilege escalation attack vectors for a malicious actor.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- **Ensure LDAP sessions are signed or encrypted in accordance with vendor recommendations stemming from security advisory ADV190023.**
- **Enable the following policies:**
  - **LDAPServerIntegrity**
  - **LdapEnforceChannelBinding**

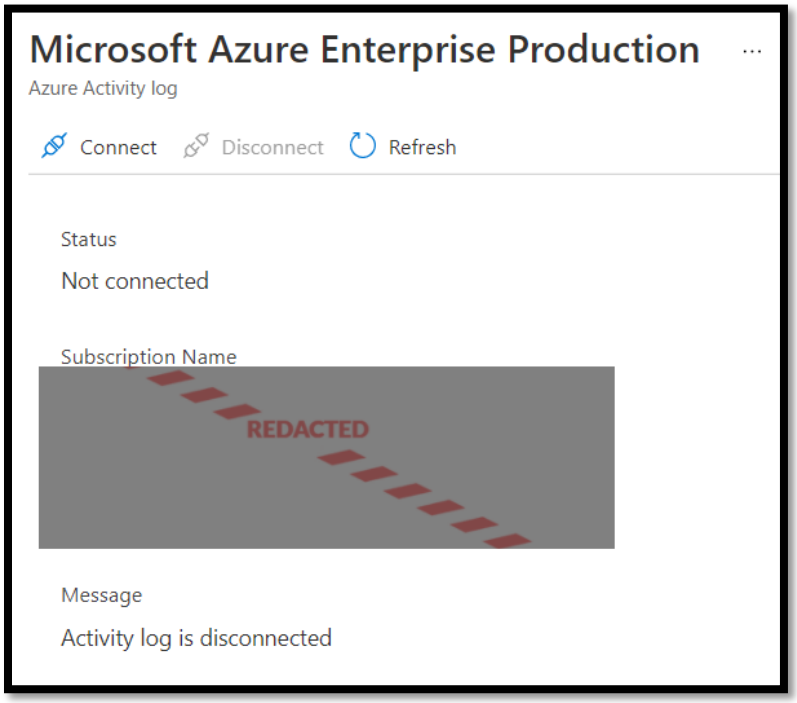
Reference(s):
https://docs.microsoft.com/en-us/windows/win32/api/winldap/nf-winldap-ldap_simple_bind
https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/ldap-session-security-settings-requirements-adv190023
https://msrc.microsoft.com/update-guide/vulnerability/ADV190023

Affected Domain(s):
[REDACTED]

Azure Log Analytics Not Universally Enabled
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Easy

Summary:
Two devices were identified as not having log analytics installed. Without activity logging being enabled insight into potentially anomalous activity within Azure would be in a degraded.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

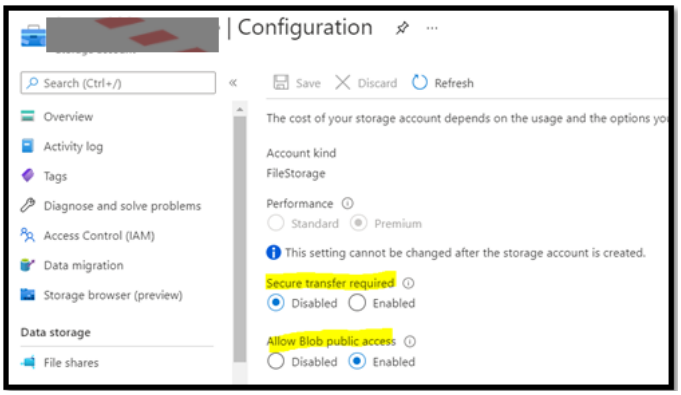
- **Ensure logging facilities have visibility over all devices to ensure a complete situational awareness of anomalous activity within the environment.**

Reference(s):
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

[REDACTED] File Storage Misconfiguration
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Easy

Summary:
Analysis of storage accounts revealed that secure transfer is disabled while public access is enabled for a [REDACTED] account. While public accessibility is not an inherent vulnerability, it is concerning when coupled with secure transfer being disabled. The secure transfer setting requires that all calls to an Azure storage REST API be over HTTPS and thus encrypted rather than in plain text. Furthermore, infrastructure encryption was found to be disabled on storage accounts as well.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- **Require secure transfer for storage accounts via the Azure portal.**
- **Regularly evaluate the necessity for public access of storage accounts and any accompanying whitelists.**
- **Ensure infrastructure encryption is enabled on all storage accounts.**

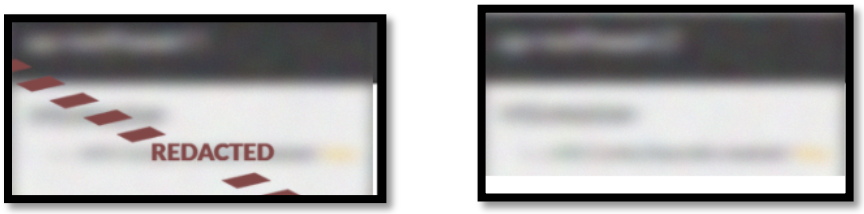
Reference(s):
https://docs.microsoft.com/en-us/azure/storage/common/storage-require-secure-transfer
Enable infrastructure encryption for double encryption of data - Azure Storage | Microsoft Docs

Affected Resource Group(s):
[REDACTED]

AWS Config Not Universally Enabled
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Intermediate

Summary:
AWS config recorder allows for AWS resource configuration logging. By not logging configuration changes, security analytics in response to an anomaly could be hindered.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- **Enable AWS Config in all regions**

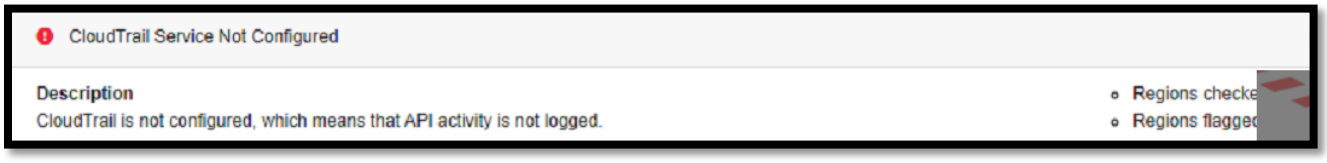
Reference(s):
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-prereq-config.html

Affected Region(s):
[REDACTED]

AWS Cloud Trail Service Not Configured
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Intermediate

Summary:
AWS CloudTrail allows for AWS API activity logging. By not logging API activity security analytics, response to an anomaly could be hindered.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- **Enable AWS Cloud Trail in all regions and ensure that the logging is integrated with the security incident and event management (SIEM) system.**

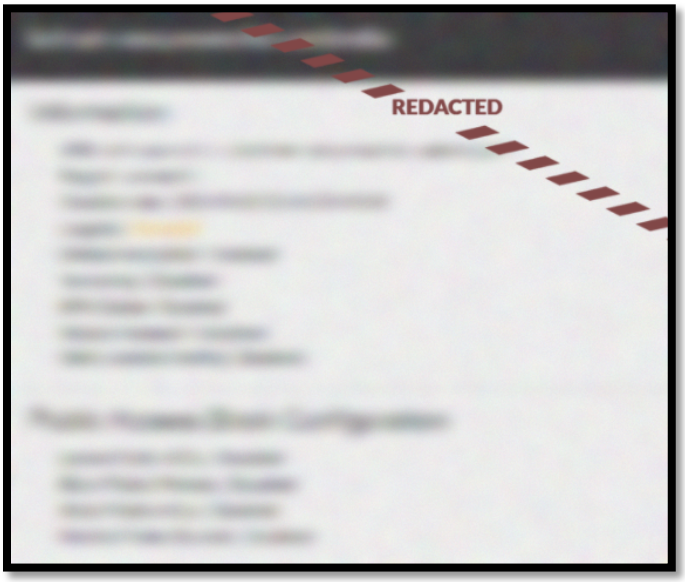
3.

Reference(s):
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-getting-started.html

AWS S3 Buckets Without Logging or Encryption
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Intermediate

Summary:
Analyzed S3 buckets were identified as having default encryption disabled, logging disabled, and MFA delete disabled. Should a malicious actor gain access to an S3 bucket, exploiting or deleting the data could be done with relative ease, and without adequate logging facilities in place incident response would be diminished.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- **Ensure S3 buckets are configured in accordance with platform best practices to include enabling logging, encryption, secure transport, and MFA delete.**

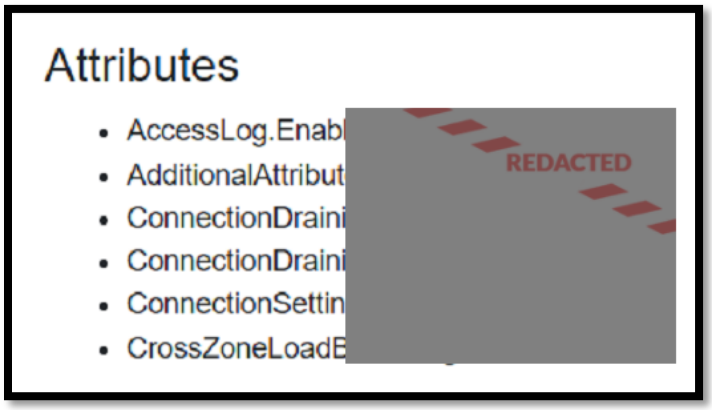
Reference(s):
https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.html
https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html

Affected Endpoint(s):
[REDACTED]

Elastic Load Balancer (ELB) Access Logging Not Enabled
QoD: 100% | Attack Risk: Moderate | Compliance Risk: Moderate | Remediation Effort: Intermediate

Summary:
ELB access logging was found to be disabled. ELB access logging captures information related to requests sent to associated load balancers. Integrating these logs with an existing SIEM can enhance overall awareness of going traffic patterns and support change management processes.

Risk Detection Result(s):

4. 

Risk Mitigation Recommendation(s):
- **Set AccessLog.Enabled to true for all ELB instances.**

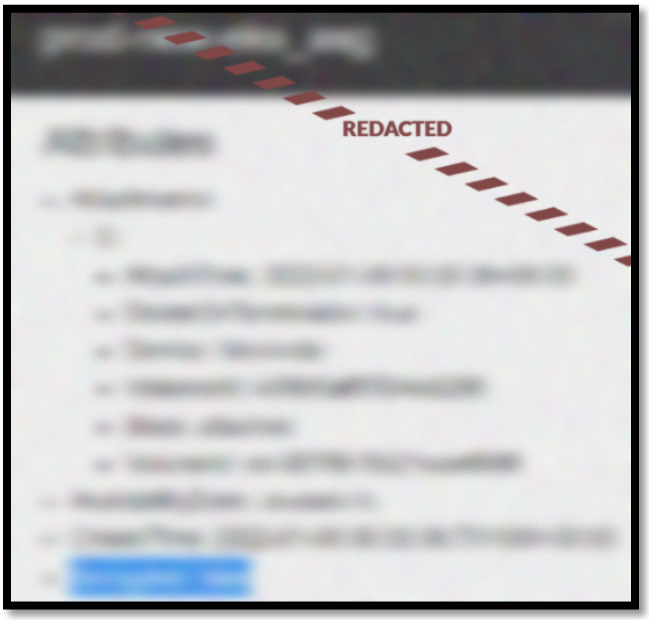
Reference(s):
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection.html

Affected Endpoint(s):
[REDACTED]

EBS Volumes Without Encryption at Rest or In-Transit
QoD: 100% | Attack Risk: Low | Compliance Risk: Low | Remediation Effort: Intermediate

Summary:
EBS volumes were found to have encryption disabled. Enabling this setting would ensure data is encrypted both at rest and in transit.

Risk Detection Result(s):



Risk Mitigation Recommendation(s):

- **Ensure encryption is enabled for EBS volumes.**

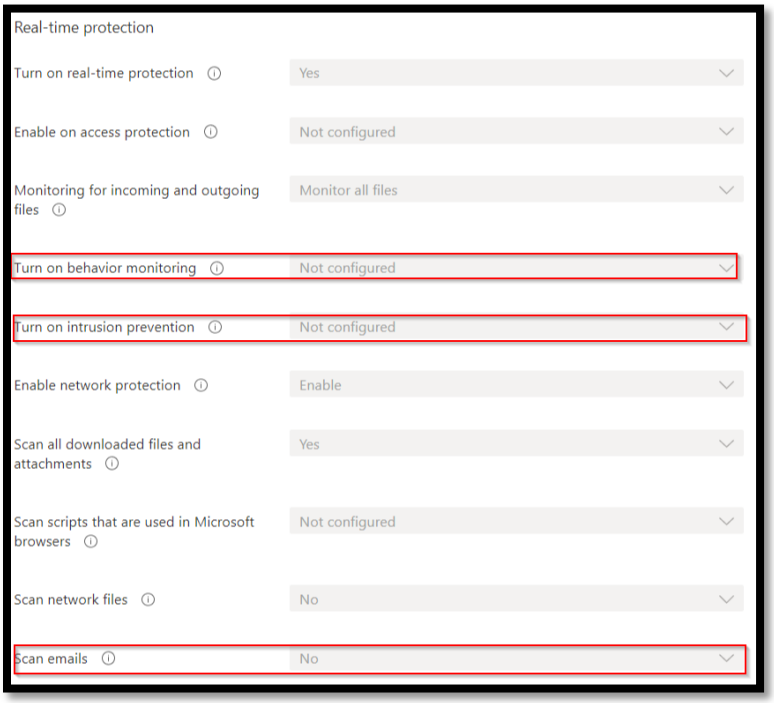
Reference(s):
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

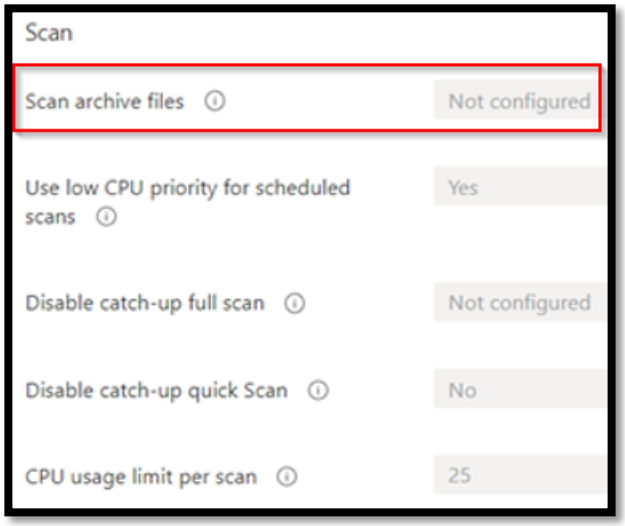
Affected Endpoint(s):
See Appendix B for list of unencrypted EBS volumes

Miscellaneous Endpoint Security Hardening Recommendations
QoD: 100% | Attack Risk: Low | Compliance Risk: Low | Remediation Effort: Low

Summary:
Endpoint security controls were identified as having behavior monitoring, intrusion prevention, email scanning, archive file scanning not configured or disabled. These features can all reduce the attack surface of the Office 365 environment.

Risk Detection Result(s):





Risk Mitigation Recommendation(s):

- **Configuring these options in accordance with platform best practices will further harden endpoints from a security standpoint.**

Reference(s):
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-real-time-protection-microsoft-defender-antivirus?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mde-p1-setup-configuration?view=o365-worldwide

Conclusion

This report reflects an evaluation of [CLIENT]'s environment within the limited scope provided in the Rules of Engagement (RoE). This included all cloud infrastructure (AWS and Azure), networking infrastructure, Office 365, written policies and procedures, and active directory analysis. When aggregated with previous provided external and internal network penetration testing reports, a holistic assessment of [CLIENT]'s security posture can be understood. Abacus Group makes a best effort to rank the severity of vulnerabilities; however, it is not possible for any assessment to guarantee that Low Risk issues cannot be used to significantly impact [CLIENT] information systems. All risk ratings in this report are a combination of industry standard ratings, as well as considerations for unique business risk as identified by Abacus Group. Special consideration should also be given to the fact that multiple low risk issues may compound into higher risk threats.

The most significant security vulnerabilities identified during this white box analysis were overly permissible file shares, inconsistent application of policies within both Azure and AWS, and a general lack of consistent logging for cloud-based infrastructure. Many of the risk findings detailed in this report are significant enough to warrant prioritized remediation, and the majority can be remediated both quickly and inexpensively.

Abacus Group security engineers found no indication of current or prior compromise. Furthermore, no external technical vulnerabilities were found to be significant enough for a malicious actor to gain access to the internal network. However, should a malicious actor compromise an employee account through social engineering, and gain access to the internal network, the information available to that malicious actor due to overly permissible file shares could have a substantial impact on the business and reputation of [CLIENT]. Once on the internal network, a malicious actor would have the ability to move laterally and would have a high likelihood of escalating to administrative privileges by exploiting current infrastructure and security controls.

Consolidated Risk Mitigation Recommendations

Priority 1:

- **Ensure MFA is universally enforced for all root and administrative accounts across the environment.**
- **Disable or constrain Kerberos delegation in order to minimize the potential for lateral movement should a malicious actor gain internal access to the environment.**
- **Upgrade unsupported operating systems and software to the latest feature releases. If that is unfeasible, consider additional network and domain segregation to isolate the most vulnerable systems.**
- **Reassess and adjust the permission level of standard users with regards to accessing file shares in accordance with the principle of least privilege.**

Priority 2:

- **Reassess the necessity of externally exposed [REDACTED] and restrict access to specified IP addresses if possible.**
- **Utilize global condition context keys or IAM role trust policies to limit the permissions that services have to specific resources and define who may assume roles.**
- **Enable LDAPServerIntegrity and LdapEnforceChannelBind to ensure LDAP traffic is properly encrypted.**
- **Standardize configuration of policies across AWS and Azure tenants to ensure consistency in password policy implementation, and that logging and encryption are in line with industry best practices.**
- **Ensure all domain controllers have been configured with Defender for Identity sensors to increase situational awareness.**
- **Configure and implement Microsoft 365 Compliance Manager, Microsoft Compliance Configuration Analyzer for Compliance Manager and Prowler (for AWS). Review Prowler results and Microsoft 365 Compliance CIS assessment dashboards on at least a quarterly cadence to ensure a consistent burn-down of security control gaps while also ensuring that new gaps do not appear from unintended regressions.**

It is important to note that the risk mitigation recommendations contained in this report reflect industry best practices and Abacus Group's limited knowledge of [CLIENT]'s infrastructure. Abacus Group does not warrant the compatibility or operational effectiveness of the risk mitigation recommendations provided in this report, as Abacus Group does not have any understanding of the nuances and caveats of [CLIENT]'s network. Abacus Group highly recommends that [CLIENT]'s technology department assesses the compatibility and operational effectiveness of the risk mitigation recommendations provided in this report, and uses a change management process to validate, plan and implement remediation changes in a UAT environment first.