Active Directory Security Assessment
Statement of Work Proposal

Purpose

County of Monterey ("Monterey", or "Company") is a county located on the Pacific coast of the U.S. state of California. Monterey reached out to Trimarc Security, LLC ("Trimarc", or "Contractor") regarding concerns with their Active Directory environment.

About Trimarc

Trimarc focuses on Active Directory (AD) security meaning we are uniquely positioned to assess enterprise Active Directory and Windows platform security. Trimarc develops defensive strategies to combat evolving attack techniques with focus on "defense in depth" defensive layers within the enterprise – while any single defense may fail, there are other compensating factors that provide additional detection and/or mitigation for that area. Our mission is to identify ways to better help protect organizations from modern threats not effectively stopped by traditional security measures. Successful defense is based on an approach involving three primary components: Detection, Mitigation, and Prevention.

Trimarc fields security personnel who have worked in operations (most of whom were systems administrators and/or systems engineers for over 10 years) and have shifted their focus & vision to security. Trimarc maintains a highly technical group of Subject Matter Experts (SMEs) that cover Active Directory, Microsoft Windows, Exchange, Azure Active Directory, Office 365, and Exchange Online. This blend of expertise means Trimarc is able to more quickly and effectively identify security issues by "connecting the dots" across systems.

Trimarc provides leading expertise in security solutions including strategy, architecture, tactical implementations, and long-term maintenance. In addition, we perform renowned security research that helps drive the implementation of effective protection measures for organizations reliant on Microsoft technologies.

We work with a wide range of customers from government to private companies to educational institutions and have evaluated their Active Directory security posture and provided valuable security recommendations and solutions. We have also helped organizations implement these recommendations.

Scope of Work

Trimarc and Monterey have entered into or will enter into a consulting agreement ("Agreement") pursuant to the terms and conditions of which will perform services as described in this Statement of

Work ("SOW"). Trimarc will conduct an "As Is" assessment and deliver a clear suggested roadmap to address short-term and long-term actions for desired "To Be" state as determined in conjunction with Monterey.
Services include the following:

- An Active Directory Security Assessment of the production Active Directory environment which includes one (1) Active Directory forest and one (1) domain that is about 20 years old with approximately 5,000 users and 6 Domain Controllers (including 1 Read-Only Domain Controller).

Note that all domains in the forest will be assessed as part of this effort and needs to be scoped properly. If the domain number here doesn't match the total number of domains in the forest, please let Trimarc know ASAP. We are unable to only assess specific domains in the forest.
Additional forests are not in scope.

Trimarc will only ever have user-level rights and will not elevate the rights of the assessment account(s) to that of a privileged administrator. Trimarc does not make modifications to the customer environment and only performs "read-only" computer system and Active Directory queries.

Technical Tasks

Task #1: Active Directory Security Assessment of the Production AD Environment

This task involves the review and assessment of one (1) Active Directory forest and one (1) domain. The forest is assessed, and the data is analyzed and reviewed. The final report is created which describes the environment along with any issues and recommendations.

Trimarc performs an Active Directory Security Assessment (ADSA) at the customer's site (or remotely, as appropriate) in order to assess known security configuration issues. The ADSA involves document review, discussions with staff, running scripts and tools, and/or manual review of the Active Directory (AD) configuration and settings. The assessment process has four (4) primary phases: 1) gathering data from the environment; 2) processing the data & interpreting the results; 3) completing the assessment report; and 4) a wrap-up session to field questions/answers based on assessment report for project closure.

Trimarc approaches this process as a partner and provides security guidance that helps improve the Active Directory security posture. This interactive assessment is meant to help answer questions about current and future project plans relating to AD security to support both short-term and long-term planning.

ADSA Benefits

- A snapshot of the Active Directory security configuration as a point in time.
- Identification of the most common and effective attack vectors and how best to detect, mitigate, and prevent them.
- Tailored recommendations focused on leveraging existing technology investments to improve the enterprise security posture.

- Active Directory security best practices customized to align with business process and requirements and minimize impact.
- As part of the report's executive summary, the top security issues are highlighted and described, along with the suggested methods to mitigate/resolve the issues.
- All discovered issues are detailed in the report along with effective impact and recommended remediation.
- The final section of the document summarizes all of the identified issues along with mitigation/resolution recommendations which can be used to develop a plan of action.

Key Security Assessment Components

- Active Directory forest and domain configuration. This includes evaluating the current Domain and Forest functional levels and identification of security enhancements in the current and higher levels.
- Active Directory security misconfigurations are highlighted and recommended remediation/mitigation is provided specific to the environment (with the understanding that often these issues can't be fully resolved in the near term).
- Active Directory trust configuration and security.
- Active Directory administration groups. This includes Enterprise Admins, Administrators, Domain Admins, custom delegation groups, and others as identified. Groups with logon rights to Domain Controllers are scrutinized and membership is expanded to gain a complete picture of the Active Directory administrators.
- Custom security groups with privileged access to Active Directory are discovered and their access rights identified.
- Group Policy security configuration for the domain and Domain Controllers.
- Permissions for all Group Policy Objects (GPOs) are reviewed and issues with the delegation of GPOs are noted along with recommended remediation.
- Service Accounts with elevated permissions. Identification of Kerberos enabled services and their associated service accounts. Special focus on service accounts with domain-level admin rights.
- Domain Controller management review including Operating System versions, backup, and FSMO role holder locations.
- Security software and tools. This involves identifying the security components and their purpose and this information is used to identify potential gaps in defenses an attacker could leverage.
- Active Directory organizational unit (OU) permissions with a focus on top-level domain OUs. Additional Active Directory object permissions are reviewed to identify potential "backdoor" access which is not obvious based on group membership.
- Identify Domain Controller auditing configuration and determine what event IDs will flow to the central logging system (SIEM/Splunk). Provide recommendations for Domain Controller auditing and what specific event IDs should be sent to the central logging system in order to detect attacker activity.
- Provide broad recommendations for all Windows system auditing (specific event IDs) that should be forwarded to the central logging system (SIEM/Splunk).
- Administrative and security review of Azure Active Directory integration components such as Azure AD Connect (if applicable).

Scoping Notes

This is not a penetration test or "Red Team" review. No attack activity will be performed on the network. If a follow-on penetration test or Red Team review is requested, that can be scoped separately.

In Scope: Production forest Domain Controller and Active Directory security configuration.

Out of Scope: Review of workstation and member server's security configuration. Other Active Directory forests.

Data on workstations and servers stored in Active Directory will be used to baseline system security configuration as an aggregate (total number sorted by OS version, Kerberos services, etc); individual workstations and servers will not be assessed. With that stated, the security posture of workstations as a whole will be discussed with focus on how attackers leverage access to one to expand access to others.

Note: Each Active Directory forest is its own AD environment and is assessed as such. Any connections to the environment via trust is noted and explored to identify the security impact. Each task listed here will be assessed separately and will have a separate deliverable specific to the AD environment assessed.

Deliverable: Technical document that describes current Active Directory security configuration of the AD environment, identifies areas of concern, and provides short and long-term recommendations to improve AD security.

AD Security Assessment vs Pentest/Red Team Engagement

While a penetration test ("pentest") or Red Team typically identifies two to three escalation paths and demonstrates exploitation, Trimarc maps out as many potential escalation paths we can (often five to twelve) that an attacker could leverage to escalate rights in Active Directory. We use a custom, proprietary PowerShell script that interrogates Active Directory; scans and evaluates security rights, roles, and permissions; and provides information and input used to generate the assessment report. This report captures the AD configuration, identifies findings and associated recommendations, and provides an actionable list of recommendations that are prioritized based on criticality. Furthermore, since we focus on Active Directory security and have created this engagement based on Microsoft and industry best practices as well as our own research, we go into more depth on what the issues are and more importantly, how to mitigate them.

Trimarc's assessment engagement is a fairly comprehensive review of the Active Directory security posture and maps the identified issues to actionable steps to resolve these issues. In comparison, penetration testing and Red Team reports tend to focus on the how and why the attack worked with some remediation information and typically include a recommendation like "disable Lan Manager ('LM') and Network Lan Manager ('NTLM') authentication on all Windows computers."

The following italicized content is a sample of how Trimarc will present recommendations in this engagement:

> *"The authentication levels supported and configured in the enterprise greatly affect the security posture since using weaker security authentication protocols such as LM and NTLM can expose account passwords.*
>
> *The group policy setting has several options:*
>
> - *Send LM & NTLM responses: Clients use LM and NTLM authentication and never use NTLMv2 session security; domain controllers accept LM, NTLM, and NTLMv2 authentication.*
> - *Send LM & NTLM - use NTLMv2 session security if negotiated: Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.*
> - *[Default] Send NTLM response only: Clients use NTLM authentication only and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.*
> - *Send NTLMv2 response only: Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.*
> - *Send NTLMv2 response only\refuse LM: Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).*
> - *Send NTLMv2 response only\refuse LM & NTLM: Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers refuse LM and NTLM (accept only NTLMv2 authentication).*
>
> *The first two options should never be set since it enables weaker security authentication by default. The goal is to move up the levels to eventually configure this setting to be "Send NTLMv2 response only\refuse LM & NTLM."*
>
> *There is no group policy linked to the Domain Controllers OU and it does not have the LAN Manager authentication level set.*
>
> *Recommendation:*
> *The Domain Controllers should have a group policy that sets authentication to at least "Send NTLMv2 response only\refuse LM", with the goal of ultimately configuring this setting to "Send NTLMv2 response only\refuse LM & NTLM".*
> *The challenge in this environment is the population of non-Windows computers and devices which may not support NTLMv2. Non-Windows devices have different support capability depending on OS and vendor. Ensure the vendor supports NTLMv2 before disabling NTLMv1 (note that this is often the case when disabling SMBv1, especially with devices such as NetApp)."*

Furthermore, Trimarc's Active Directory Security Assessment (ADSA) offering provides insight into potential security issues in the environment and how to mitigate them.
The following "Highlights" and "Critical Findings" are provided as a reference.

Example of Pentest Report Findings Highlights

1. *Found an unpatched SQL server, compromised the box and dumped hashes, which includes the SQL service account which is a member of Domain Admins.*
2. *Kerberoasted the default domain Administrator account and cracked the password.*

Example of Trimarc ADSA Report Critical Findings

1. *5 service accounts are members of Domain Admins. After reviewing these accounts and what they are used for, none of these require AD admin rights. This includes a SQL Service account that is a member of Domain Admins which could be compromised on the SQL server to compromise the AD forest.*
2. *Default domain Administrator account (RID 500) has a Kerberos service principal name (SPN) and a password that is >5 years old. This account could have its password cracked offline using a Kerberos attack method called "Kerberoasting". The Kerberos SPN should be removed from this account and the password changed.*
3. *3 GPOs are linked to the Servers OU and the Domain Controllers OU which means Server Admins can escalate to Domain Admin since members of Server Admins have modify rights to these 3 GPOs. The settings in these GPOs that need to apply to Domain Controllers should be configured in a DC specific GPO and the existing ones unlinked from the Domain Controllers OU.*
4. *1 Service account is delegated rights on the domain root, that enables an attacker with control of this account to request all password hashes in the domain (DCSync). Based on the account configuration, these rights should not be required.*
5. *Domain Users have the ability to logon to the Domain Controllers which is configured in the Default Domain Controllers Policy GPO.*
6. *The KRBTGT password has never been changed. Since the associated password hash is in every backup since the Active Directory forest was created, this account's password should be changed due to risk of potential "Golden Ticket".*
7. *Server Operators contains a group which has regular user accounts as members. This group has elevated rights on Domain Controllers.*
8. *Local Administrator passwords on all workstations are the same. When workstations are built, the standard local Administrator password is set to the organization default. Compromise of one workstation would result in compromise of all workstations and potentially Active Directory.*

The ADSA Assessment Report

The final report provides key information on the AD environment, is specific to the environment, and is typically around 200 pages (including appendices). The document includes a summary which can be shown to management and summarizes what was discovered along with the potential impact. The primary report sections each include findings and recommendations which are all captured in the final section. The findings section of the report is a summary of the AD environment issues and recommendations which simplifies the remediation process. Furthermore, this section includes a table highlighting the most critical findings and recommended remediation actions, levels of criticality, and estimated level of effort (all of which are specific to the environment assessed) and is often used to generate a remediation project plan. Report data detail is included in an appendix and referenced from each of the relevant sections. Recommendations for domain and Domain Controller security settings are provided along with recommended event log auditing configuration at the end of the document.
For multi-forest engagements, the primary production forest report will include the detail that is common across forests such as the administration model and process.

Our key differentiator is that we provide a report specific to the customer environment. Furthermore, the issues we look for are based on Trimarc's Active Directory security research, some of which is not public knowledge.

In order to gather the information required to create the report, Trimarc uses a proprietary PowerShell script which is continuously updated and refined to better gather data from each customer environment we work in. The assessment report template document and the Trimarc assessment PowerShell script, including changes, updates, and modifications made during Trimarc's work for the Company, are Trimarc's intellectual property and are subject to the provisions in the Agreement between Trimarc and the Company relating to confidential information and the license contained in the Agreement. Upon payment in full, a license to the Company is provided to use the Report for internal remediation processes and, subject to a non-transferable license of Trimarc's Intellectual Property contained in the Report, may use the completed Report and Trimarc's proprietary Intellectual property for its internal management purposes (such as remediation of any identified issues and improving security of the environment) relating to the system(s) that are subject to the assessment, but the Company may not assign the Report to third parties or use it or permit its use in a manner inconsistent with the ownership rights and the license described herein and in the Agreement. In the event the Company desires that a third party perform any remediation or changes to the systems, the Company shall obtain Trimarc's prior consent, which may be conditioned on such third-party providing undertakings to Trimarc regarding the use of Trimarc's proprietary and confidential information.
Trimarc Intellectual Property Contract Language is provided in Appendix A of this document.

A sample outline of the final assessment report is included in Appendix B: Sample Active Directory Security Assessment Report Outline.

Place of Performance

The assessment will be performed remotely from Trimarc office location(s).
Remote work requires a remote connection to a computer (or virtual machine) on the internal network and a regular Active Directory user account.

Period of Performance

Remote Engagement:
For the remote assessment engagement, the Period of Performance is expected to be approximately six (6) weeks (starting when Trimarc has started gathering data in the environment) which includes the remote assessment and development of the detailed final deliverable with observations and recommendations. When the work will be performed remotely, Trimarc will schedule calls with Monterey to discuss interim findings and recommendations as appropriate.

Once the final report document is completed, Trimarc will schedule a conference call to review the document.

Dates will be determined at a later date as agreed upon by Monterey and Trimarc. No date is guaranteed without a signed contract.

Note that the computer(s) and account(s) need to be available when Trimarc starts performing the work. If all listed pre-requisites aren't in place prior to the Trimarc team arriving, the work may be rescheduled/repriced or Trimarc will perform a "best effort" assessment of the environment.

Monterey will provide key requested details of "As Is" AD infrastructure to support the SOW, access to required staff, access to required systems and/or information, and appropriate workspace. Any delays to these dependencies may increase the total amount of time required for delivery and will incur additional fees.

Deliverables

Deliverable	Estimated Delivery Date
Active Directory Security Assessment Report	25 business days after work begins.

ADSA Requirements

The Active Directory Security Assessment is a mix of requested information, running PowerShell scripts and reviewing Active Directory information from the AD GUI tools, and documenting findings.

The estimated delivery date described above and elsewhere in this SOW as well as the cost of the Services assume that Company will fully cooperate in a timely manner with Trimarc. Company will provide key requested details of "As Is" AD infrastructure to support the SOW, access to required staff, access to information, required systems and/or information, and appropriate workspace. information, access to required Company staff and employees, access to required systems and/or information, and appropriate workspace, all as may be requested by Trimarc. all as described in the SOW or as requested by Trimarc. Any delays to these dependencies may increase the total amount of time required for delivery and will incur additional fees.

ADSA Assessment Computer

For multiple forests, we require 1 domain-joined computer in each forest.

1 domain-joined computer is required for this assessment with network connectivity to all Domain Controllers in the forest being assessed.

In order to perform the AD Security assessment Trimarc uses the customer's domain-joined Windows computer with the following:

- 12GB RAM.
- If the computer system is virtual, the virtual system and its drive needs to persist during the engagement.

- Windows 10 or Windows Server 2012R2/2016/2019 with the US English language configured (United States region).
- Microsoft Office 2013 (Microsoft Office 2016 preferred) with Excel installed and fully licensed for the engagement period. The assessment tool generates Excel files that are provided with the final report and if Excel isn't installed Trimarc may not be able to provide this data.
- 7zip archive utility installed (for creating AES encrypted archive files).
- PowerShell v5.x with full PowerShell language and capability.
- Active Directory Remote Server Administration Tools (RSAT) which includes Active Directory Users and Computers, Active Directory Domains and Trusts, etc.
- The Group Policy Management Console installed which enables Trimarc to review GPOs.
- Active Directory PowerShell module (typically installed with the AD RSAT component).
- Group Policy PowerShell module.
- Local administrative rights on the assessment computer(s) is preferred so we can more quickly resolve dependency issues.
- The assessment computer(s) needs to be able to run the assessment tools overnight. Trimarc often works in AD environments where the assessment tool takes more than 8 hours to gather the necessary data. If we are unable to leave the computer on overnight we cannot ensure successful collection of data for this engagement.
- Persistent storage on the assessment computer for the entire engagement (any storage that resets overnight will wipe out the progress logged during that session).
- Internet access (specifically access to the Trimarc secure portal site).
- For a remote engagement, remote access for Trimarc to perform the assessment (via VPN, VMware Horizon, or similar).

Trimarc utilizes a custom, proprietary assessment tool (which leverages PowerShell) to gather information about the AD environment (read-only) which leverages the Active Directory and Group Policy PowerShell modules. The Active Directory Remote Server Administration Tools (RSAT) is also required on this system to review the AD configuration by looking at the AD GUI tools.

ADSA Assessment Account

AD user account is required with view access to all organizational units (OUs) and objects. The AD user account only needs to be a regular user account, no elevated privileges are needed for the assessment account(s). If any OUs or objects such as GPOs have more restrictive permissions than the AD default, please add these accounts to a group that has read access.

Note that the computers and accounts need to be available when Trimarc starts performing the work. If all listed pre-requisites aren't in place prior to the Trimarc team arriving, the work may be rescheduled/repriced or Trimarc will perform a "best effort" assessment of the AD environment.

Cost

ADSA Remote Assessment:

The total cost for a remote assessment is $42,250 includes all labor based upon the tasks and

deliverables identified above as in scope.
Remote work requires a remote connection to a computer (or virtual machine) on the internal network and a regular Active Directory user account.
If a remote assessment is selected and travel is later requested, that travel will be invoiced separately.

This quote expires on April 15, 2021.
Please note that we are usually booked 3 to 6 months out and are unable to hold a "next available" date until we have a signed SOW.

Termination

This Scope of Work shall terminate immediately and automatically upon the earlier of: (i) thirty (30) days prior written notice from either party, (ii) the expiration of the Consulting Period, or (iii) written notice from either party to the other that this Agreement is being terminated for "cause" (as defined herein). "Cause" shall mean that the Trimarc or the Company has committed an act of gross misconduct, gross insubordination, embezzlement, fraud, misappropriation of funds or trade secrets, or any felony or any material violation of state or federal law or that either party has committed a material breach of this Agreement. In any case, upon termination: (x) for cause based on conduct of Trimarc, no additional consideration will be due or payable to Trimarc and for cause based on conduct of the Company, Trimarc shall be paid for all work done and shall be entitled to be paid the balance of Trimarc's fee for Services; or as provided in Section (i) of the first sentence of this Section, Trimarc shall be paid for all work done to the date of such termination, and (y) this Scope of Work shall cease to have any force or effect, except that in all events, the parties' obligations to maintain confidential or proprietary information, the parties' warranties, indemnification obligations, and limitation of liability shall survive.

Payment

An Invoice will be submitted for payment after completion and delivery of the deliverable(s) identified in the Deliverables section above. Payment terms are Net30 and payment should be received within 30 days.

Purchase Order (PO) number for the engagement (as appropriate): ______________________

Email address to which Trimarc should send the invoice: ______________________________

IN WITNESS WHEREOF, the parties hereto, agree that this Statement of Work sets forth, as of the date signed below by an authorized representative, the work that Trimarc will perform for Company, subject to the terms and conditions contained in the Agreement between Company and Trimarc.

County of Monterey	Trimarc Security, LLC
Signature :	**Signature:** DocuSigned by: Sean Metcalf 7E5DEF0DA20B48D...
Name :	**Name:** Sean Metcalf
Title :	**Title:** CEO
Date :	**Date:** 3/18/2021

Appendix A: Trimarc Intellectual Property Contract Language

Trimarc Property Rights

General.
Contractor will perform the Services described in the SOWs, which may involve assessing the security of the COMPANY's and its affiliates' Active Directory environment and/or providing security consulting services to the COMPANY. In both assessment and consulting work, which will include meetings with COMPANY staff and review of COMPANY materials, Trimarc ("Trimarc" or "Contractor") uses proprietary tools, including the assessment report template and script(s)/program(s). Through access to COMPANY's system, the script creates data files which Contractor uses to complete its security assessment report template (each, a "Report"). The Report will be delivered to COMPANY. In the course of doing its on-site work, Contractor may make modifications or updates to its tools, template, script, and programs. The Report will be based on and will include COMPANY's information ("COMPANY Content") and Contractor's script, template and other tools and programs. The script, the template, and any other tools and programs used by Contractor, together with any changes to any thereof, whether before, during, or after, the assessment and the consulting period, are proprietary and confidential information of Contractor, subject to the confidentiality provisions of the Agreement. Contractor also provides access to teaching and training materials ("Training Materials") which are copyrighted, some or all of which may be delivered to COMPANY. As described below, and subject to full payment, Trimarc will grant to COMPANY a non-revocable perpetual license to use the Report and the Training Materials for Company's internal use only.

Title to Certain Property.
All COMPANY Content, and any materials (whether original or duplicates and whether in tangible or intangible form) including, without limitation, equipment purchase agreements, file or data base materials in whatever form, books, manuals, sales literature, equipment price lists, COMPANY's training materials, client record cards, client files, correspondence, documents, contracts, orders, messages, memoranda, notes, agreements, invoices, receipts, lists, software listings or printouts, all programmer generated materials including any materials cataloged on the COMPANY's storage media, documentation of tests conducted by Contractor, specifications, models, computer programs, the Report(s), and records of any kind in the possession or control of Contractor which in any way relate or pertain to COMPANY's business, including the business of subsidiaries or affiliates of COMPANY, whether furnished to Contractor by COMPANY or prepared, compiled or acquired by Contractor during its consulting relationship with COMPANY (the "Materials"), shall be the sole property of COMPANY. Notwithstanding the generality of the foregoing, the term "Materials" as described in the preceding sentence does not and shall not include (i) Contractor's Training Materials, some or all of which may be copyrighted by Contractor, provided however, if applicable, that Training Materials used by Contractor and distributed to the employees or contractors of COMPANY or its affiliates who participate in any training provided by Contractor may be retained by COMPANY, and (ii) the Technical Elements (defined below), even if Technical Elements are contained in the Report or other materials delivered to COMPANY. "Technical Elements" means the (i) data, modules, components, designs, utilities, subsets,

objects, program listings, software, tools, models, methodologies, programs, templates, scripts, systems, analysis frameworks, leading or best practices, and specifications (including all of the foregoing owned or developed by Contractor prior to, independently from, or during the assessment or consulting activities under, the Agreement); (ii) Contractor's script, programs, tools, security assessment report template); and (iii) any updates, modifications, or improvements Contractor makes to its script, programs, tools, and template, and any offensive or defensive techniques Contractor creates, develops, acquires, or conceives during the course of its work for COMPANY. At any time upon request of COMPANY, and in any event promptly upon termination of the Agreement, Contractor shall deliver to COMPANY all Materials that are the sole property of COMPANY and shall destroy any copies in Contractor's possession.

Title to Certain Intangible Property.

Unless otherwise specifically agreed to in an SOW, the work to be delivered to COMPANY under any SOW, including the Reports ("Deliverables") may include Technical Elements. The Technical Elements are and shall be owned by Contractor and Contractor retains all rights thereto. All such Technical Elements shall remain intellectual property of Contractor and shall remain Contractor's Confidential Information subject to the provisions and restrictions set forth above in the Scope of Work (regarding termination). Subject to full payment, Contractor hereby grants COMPANY a perpetual, worldwide, non-transferable (except to affiliates), royalty-free license in the Technical Elements as are integrated into any Deliverables solely for the internal management purposes of COMPANY with respect to the system(s) which were the subject of the assessment and to the Training Materials solely for internal management use of the COMPANY and its affiliates. Without limiting the generality of the foregoing, COMPANY agrees that it will not modify, reverse engineer, decompile, create other works from, or disassemble any software programs contained in the Contractor's Confidential Information or the Report(s) without the prior written consent of the Contractor. For the avoidance of doubt, COMPANY will not own or have any rights in the Technical Elements, except by virtue of this license.

Appendix B: Sample Active Directory Security Assessment Report Outline

Note: This is a rough outline of what might be included. Included content varies based on environment configuration and security posture.

- Executive Summary
  - Overview
  - Purpose and Scope
  - Mitigations already in place
  - Most significant findings
  - Assessment Limitations
  - Document Structure

- Active Directory Security Assessment Findings & Recommendations
  - Potential Attack Paths
  - Top Recommended Remediation Items

- Existing Active Directory Architecture Configuration
  - Overview
  - Forest & Domain Configuration
  - Forest Read-Only Domain Controllers
  - DNS
  - Forest Partition Backup
  - Trusts
  - Authentication
  - Accounts
  - OUs

- Active Directory Administration, Privileged Groups, Permissions, & Rights
  - Administrative Accounts
    - Active Directory Administration
    - Active Directory Administrative Account Protection
    - Default Domain Administrator Account
    - KRBTGT Domain Kerberos Service Account

- Local Administrator Account Management
- Inactive Privileged Accounts
- Computer Accounts that are Members of Potential Admin Groups
- Kerberos Delegation

- Active Directory Delegated Permissions & Rights
    - Domain Permissions
    - Custom OU Permissions
    - OUs with Non-Standard Owner
    - AD Object Security Permissions
    - AdminSDHolder Permissions
    - Custom GPO Permissions
    - Credentials in SYSVOL
    - Exchange Active Directory Permissions
- Privileged Groups
    - Highest Privileged Accounts and Group Membership
    - Forest Administration Groups
    - AD Administration Groups
    - Domain Administration Groups
    - Default Privileged Built-in Accounts and Groups
    - Custom Privileged Groups

* Security Controls, Monitoring, and Group Policy Configuration
    * Secure Administrative Host and Configuration
    * User Logon Scripts
    * Azure Active Directory Integration
    * Group Policy Configuration
        * Domain Password Policy
        * Domain-Linked Group Policies
        * Domain Audit Policy Configuration
        * OUs with Blocked Inheritance
        * GPOs Managing Local Groups
        * Group Policies linked to Active Directory Sites
* Domain Controller Security
    * Security Overview

  - Domain Controller Patching & Security Updates
  - Domain Controller Configuration
  - Flexible Single Master Operators (FSMOs) Configuration
  - Directory Services Restore Mode Password Management
  - Domain Controller Group Policy Configuration
    - Group Policies linked to the Domain Controller OU
    - Audit Policy Configuration
    - User Rights Assignment Policy Configuration
    - Security Options Policy Configuration
  - Domain Controller Configuration
    - Installed Software
    - Services and Agents
    - Scheduled Tasks
  - Domain Controller Shares & Permissions
  - Read-Only Domain Controllers
    - Read-only Domain Controllers Group Membership
    - RODC Administration
    - RODC Password Replication Policy
    - RODC Password Revealed Users
  - Domain Controller Internet Access Configuration

- Appendix: Active Directory Overview

- Appendix: Recommended Configuration References
  - Security Event Auditing
  - Recommended Domain Controller Group Policy Security Settings
  - Recommended Windows Server Group Policy Settings
  - Recommended Windows Workstation Group Policy Settings

- Appendix: Trimarc Security Recommendations
  - Standard Recommendations
  - Reducing Service Account Rights in Active Directory
  - Delegating Rights with Role Groups
  - Securing and Preventing Lateral Movement with a Host-Based Firewall

  - Securing Administration Recommendations
  - Hardening Active Directory Administration
  - Domain Controller System Encryption
  - Application Whitelisting Deployment Roadmap Recommendations
  - PowerShell Security Recommendations
  - Active Directory Lab Environment Recommendations
  - Recommended Enhanced Security for all Windows Systems
  - Active Directory Security Best Practices
  - Microsoft Active Directory Security Reference Documents
  - Active Directory Security Reference Articles

- Appendix: Resources & References

Appendix C: Sample Microsoft Cloud Security Assessment Report Outline

Note: This is a rough outline of what might be included. Included content varies based on environment configuration and security posture.

Sample Microsoft Cloud Security Assessment (MCSA) report outline

1. Introduction
    - a. Overview
    - b. Document Structure

2. Assessment Findings & Recommendations
    - a. Existing Mitigations
    - b. Most Significant Findings
    - c. Microsoft Cloud Security Posture
    - d. Recommended Remediation items

3. Microsoft Cloud Tenant Architecture
    - a. Office 365 Tenant Information
    - b. Tenant DNS Configuration
    - c. Office 365 Subscriptions
    - d. Azure AD Connect
    - e. Azure AD Accounts
    - f. Azure AD Service Principals
    - g. Azure AD Groups
    - h. Azure AD Devices

4. Microsoft Cloud Administration, Privileged Groups, Permissions, & Rights
    - a. Microsoft Cloud Administration
    - b. “Break Glass” Cloud Administrator Account
    - c. Privileged Roles & Accounts
    - d. Privileged Identity Management (PIM)
    - e. Azure AD Admin Groups
    - f. Azure AD Applications & Permissions

5. Exchange Online Configuration
    - a. Exchange Configuration
    - b. Exchange Domains
    - c. Exchange Role Group Report
    - d. Exchange Mailbox Configuration
        - i. Exchange Mailbox Auditing Configuration
        - ii. Exchange Mailbox Non-Standard Permissions
        - iii. Exchange Mailbox Non-Standard Owners
    - e. Exchange Apps/Add-Ins
    - f. Exchange Transport Rules

Trimarc Security, LLC
1775 I St NW
Suite #1150
Washington, DC 20006
Phone: (202) 587-2735
Email: info@TrimarcSecurity.com
Web: TrimarcSecurity.com