CyberArk DNA Scanner Requirements Analysis

# Executive Summary

This document outlines the requirements analysis for implementing CyberArk DNA (Discovery and Audit) scanner to replace/supplement BeyondTrust scanner for AWS server onboarding and privileged account discovery.

# 1. Current Situation Assessment

1.1 Existing BeyondTrust Issues

Problem: BeyondTrust scanner failing to onboard some AWS servers

Impact: Incomplete visibility of privileged accounts and potential security gaps

Business Need: Evaluate CyberArk DNA as alternative solution

1.2 Objectives

• Test CyberArk DNA scanner capabilities on AWS infrastructure

• Compare discovery results with BeyondTrust

• Determine if CyberArk provides better coverage for problematic servers

• Establish implementation requirements

# 2. CyberArk DNA Scanner Overview

2.1 What is CyberArk DNA?

CyberArk Discovery & Audit (DNA) is a powerful tool – available at no charge – that scans systems on your network to uncover accounts, credentials and misconfigurations that can create risk.

2.2 Key Capabilities

• Multi-platform Discovery: Windows, Linux, Unix, network devices

• Cloud Support: AWS, Azure, GCP - uncovers privileged access and control weaknesses across hybrid, cloud and DevOps environments

• Agentless Scanning: No software installation on target systems

• Dependency Mapping: Identifies service account relationships

• Risk Assessment: Identifies machines vulnerable to credential theft attacks and assess privileged access security risks

2.3 Discovery Capabilities

CyberArk DNA can locate privileged accounts on-premises, in the cloud and in DevOps environments, and identify all privileged credentials, such as passwords, SSH keys, passwords hashes, AWS access keys and more.

# 3. Technical Requirements Analysis

3.1 Infrastructure Requirements

3.1.1 CyberArk DNA Server Specifications

Operating System: Windows Server 2016/2019/2022 or RHEL 7/8

CPU: Minimum 4 cores, Recommended 8 cores

RAM: Minimum 8GB, Recommended 16GB

Storage: Minimum 100GB, Recommended 500GB (depending on environment size)

Network: 1 Gbps network interface

3.1.2 Database Requirements

Supported Databases:

• Microsoft SQL Server 2016/2019/2022

• Oracle 12c/19c

• PostgreSQL (specific versions)

Database Server: Separate server recommended for production

Storage: SSD recommended for database files

3.2 Network Requirements

3.2.1 Firewall Rules (Inbound to DNA Scanner)

- Admin Networks to DNA Scanner: 443 (HTTPS) - Web Console Access

- Admin Networks to DNA Scanner: 22 (SSH) - Linux Admin Access

- Admin Networks to DNA Scanner: 3389 (RDP) - Windows Admin Access

3.2.2 Firewall Rules (Outbound from DNA Scanner)

- DNA Scanner to Target Servers: 22 (SSH) - Linux/Unix Discovery

- DNA Scanner to Target Servers: 135, 445 (SMB) - Windows Discovery

- DNA Scanner to Target Servers: 1433 (TCP) - SQL Server Discovery

- DNA Scanner to Target Servers: 1521 (TCP) - Oracle Discovery

- DNA Scanner to Target Servers: 3306 (TCP) - MySQL Discovery

- DNA Scanner to Target Servers: 5432 (TCP) - PostgreSQL Discovery

- DNA Scanner to AWS API: 443 (HTTPS) - AWS Cloud Discovery

- DNA Scanner to DNS Servers: 53 (DNS) - Name Resolution

- DNA Scanner to License Server: 443 (HTTPS) - License Validation

3.2.3 AWS-Specific Network Requirements

- VPC Access: DNA scanner needs connectivity to target VPCs

- Security Groups: Configure appropriate security groups for target EC2 instances

- NACLs: Ensure Network ACLs allow required traffic

- Internet Gateway: Required for AWS API calls (can use NAT Gateway for private subnets)

3.3 AWS Permissions and Access Requirements

3.3.1 AWS IAM Role/User Permissions

DNA requires a license. The DNA license includes an expiration date, and limits the number of Windows machines and the number of Linux/Unix machines that can be scanned per scan.

Required AWS IAM permissions for cloud discovery:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"ec2:DescribeInstances",

"ec2:DescribeImages",

"ec2:DescribeKeyPairs",

"ec2:DescribeSecurityGroups",

"ec2:DescribeVpcs",

"ec2:DescribeSubnets",

"iam:ListUsers",

"iam:ListRoles",

"iam:GetUser",

"iam:GetRole",

"rds:DescribeDBInstances",

"rds:DescribeDBClusters"

],

"Resource": "\*"

}

]

}

3.3.2 Server-Level Access Requirements

Linux/Unix Servers:

• SSH access with sudo/root privileges

• Key-based authentication recommended

Windows Servers:

• Local admin privileges

• WMI access enabled

• Remote Registry service running

# 4. Implementation Plan

4.1 Phase 1: Environment Setup (Week 1-2)

- Provision DNA Scanner Server

- Install CyberArk DNA Software

- Network Configuration

4.2 Phase 2: AWS Integration (Week 2-3)

- AWS Access Configuration

- Target System Preparation

4.3 Phase 3: Discovery Testing (Week 3-4)

- Initial Discovery Scan

- Results Analysis

4.4 Phase 4: Production Readiness (Week 4-6)

- Performance Testing

- Documentation and Training

# 5. Resource Requirements

5.1 Personnel

- Technical Lead: 1 person (40 hours)

- System Administrator: 1 person (20 hours)

- Network Administrator: 1 person (10 hours)

- AWS Administrator: 1 person (15 hours)

5.2 Infrastructure Costs

- VM/EC2 Instance: ~$200-500/month (depending on size)

- Database Server: ~$300-800/month (if separate)

- Storage: ~$50-100/month

- Network Data Transfer: Variable based on usage

# 6. Success Criteria

6.1 Technical Success Metrics

- Successfully discover privileged accounts on problematic servers

- Achieve >95% discovery accuracy compared to manual verification

- Complete discovery scans within acceptable time windows

- Zero security incidents during testing

6.2 Business Success Metrics

- Improved coverage of AWS servers vs. BeyondTrust

- Reduced manual effort for privileged account management

- Enhanced security posture through better visibility

- Cost-effective solution compared to current state

# 7. Risk Assessment and Mitigation

7.1 Technical Risks

Risk | Impact | Probability | Mitigation

Network connectivity issues | High | Medium | Thorough firewall rule testing

AWS permission problems | High | Medium | Careful IAM policy configuration

Performance impact on targets | Medium | Low | Gradual rollout, monitoring

License limitations | Medium | Low | Verify license capacity

7.2 Security Considerations

- Credential Management

- Network Security

- Audit Logging

- Data Protection

# 8. Next Steps and Action Items

8.1 Immediate Actions Required

- Firewall Rules: Submit firewall rule requests to network team

- AWS Permissions: Coordinate with AWS team for IAM role creation

- VM Provisioning: Request VM/EC2 instance for DNA scanner

- Database Setup: Coordinate database provisioning if required

8.2 Dependencies

- Network team approval for firewall changes

- AWS team support for permissions and connectivity

- Security team approval for new scanning solution

- Management approval for resource allocation

# 9. Conclusion

CyberArk DNA scanner presents a viable alternative to address BeyondTrust limitations with AWS server discovery. The implementation requires careful planning around network connectivity, AWS permissions, and resource allocation. With proper setup and configuration, CyberArk DNA should provide improved visibility into privileged accounts across our AWS infrastructure.

Recommendation: Proceed with pilot implementation following the outlined plan, starting with firewall rule requests and infrastructure provisioning.

# 10. References and Supporting Documentation

10.1 Official CyberArk Resources

- CyberArk DNA Datasheet: https://www.cyberark.com/resources/product-datasheets/cyberark-dna-datasheet

- CyberArk Discovery & Audit Overview: https://www.cyberark.com/discovery-audit/

- CyberArk DNA Overview Video: https://www.cyberark.com/resources/videos/cyberark-dna-overview

- Official Documentation: https://docs.cyberark.com/privilege-cloud-standard/latest/en/content/privilege%20cloud/privcloud-assess-network.htm

- DNA Messages and Troubleshooting: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/MESSAGES/Discovery-and-Audit-DNA.htm

10.2 Community and Support Resources

- CyberArk Community - DNA Topic: https://community.cyberark.com/s/topic/0TO2J000000JPxzWAG/discovery-audit-dna

- DNA Installation Guides: https://community.cyberark.com/s/question/0D52J00008EpK11SAF/cyberark-dna-tools-manual-or-installation-guide

- Privileged Account Discovery Articles: https://community.cyberark.com/s/article/Discovering-Your-Privileged-OS-Accounts-with-DNA

10.3 Technical Documentation Sources

- AWS IAM Best Practices: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

- AWS VPC Security Groups: https://docs.aws.amazon.com/vpc/latest/userguide/VPC\_SecurityGroups.html

- CyberArk Installation Guides: https://www.scribd.com/document/452134215/CyberArk-DNA-Installation-Guide

- User Guide References: https://fliphtml5.com/jqrje/wntv/CyberArk\_DNA\_User\_Guide/

10.4 Industry Standards and Compliance

- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

- CIS Controls: https://www.cisecurity.org/controls/

- SANS Privileged Access Management: https://www.sans.org/white-papers/

10.5 Additional Reading

- CyberArk Security Services Program: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/11.3/en/Content/BestPractices/SecurityProgram-Phase1.htm

- Privileged Access Management Best Practices: Industry whitepapers and guides

- AWS Security Best Practices: https://aws.amazon.com/architecture/security-identity-compliance/

# 11. Document Control and Distribution

11.1 Document Version History

Version: 1.0

Date: [Current Date]

Author: [Your Name]

Changes: Initial draft for review

11.2 Distribution List

Manager: [Manager Name]

Technical Team: Surendra, David, Vengalatha

Network Team: [Network Admin Names]

AWS Team: [AWS Admin Names]

Security Team: [Security Team Names]

11.3 Document Classification

Classification: Internal Use

Retention Period: 3 years

Review Cycle: Quarterly or as needed