# Project Part 1:

# Security Control Implementation and Optimization

Justin Langevin

8648380

Conestoga College

SECU74020:

Secure Enterprise Architecture

July 28, 2024

## Security Control Implementation and Optimization

### Access Control Implementation

The strategies for implementing Role-based access controls for different user groups are as follows:

- Role-Based Access Control (RBAC)
    - Defined Roles
        - System Administrator
            - Access to configurations and management of systems
                - Read, Write, Execute, Modify, Delete
                - Group Name: SysAdmins
        - Database Administrator (DBA)
            - Access to all database systems and data
                - Read, Write, Execute, Modify, Delete
                - Group Name: DBAdmins
        - Network Administrator
            - Access to network configurations and management.
                - Read, Write, Execute, Modify Delete
                - NetAdmins
        - Security Administrator
            - Access to security configuration and management
                - Read, Write, Execute, Modify Delete
                - Group Name: SecAdmins

- User Administrator
    - Access to user account management
        - Read, Write, Execute, Modify Delete
        - Group Name: UserAdmins

- Researcher
    - Permissions: Access to research databases, tools, and project files
        - Read, Write, Execute
        - Group Name: Researchers
- Developer
    - Permissions: Access to development environments, source code repositories, and testing platforms.
        - Read, Write Execute, Modify
        - Group Name: Developers
- Quality Assurance
    - Permissions: Access to testing environments, defect tracking systems
        - Read, Write, Execute
        - Group Name: QualityAssurance
- Manufacturing
    - Permissions: Access to manufacturing systems, schedules, and quality control data.
        - Read, Execute

      - Group Name: Manufacturing
  - Supply Chain
    - Permissions: Access to supply chain management systems, inventory, and logistics tools
      - Read, Write, Execute
      - Group Name: SupplyChain
  - Sales
    - Permissions: Access to customer relationship management (CRM), sales data, and marketing tools.
      - Read, Write
      - Group Name: Sales

- Access Control Lists (ACLs)
  - System Files and Settings:
    - SysAdmins
      - Read, Write, Execute, Modify, Delete
    - Developers
      - Read, Execute
    - Network Administrators
      - Read, Execute
    - Security Administrators
      - Read, Execute
    - Others

    - No Access

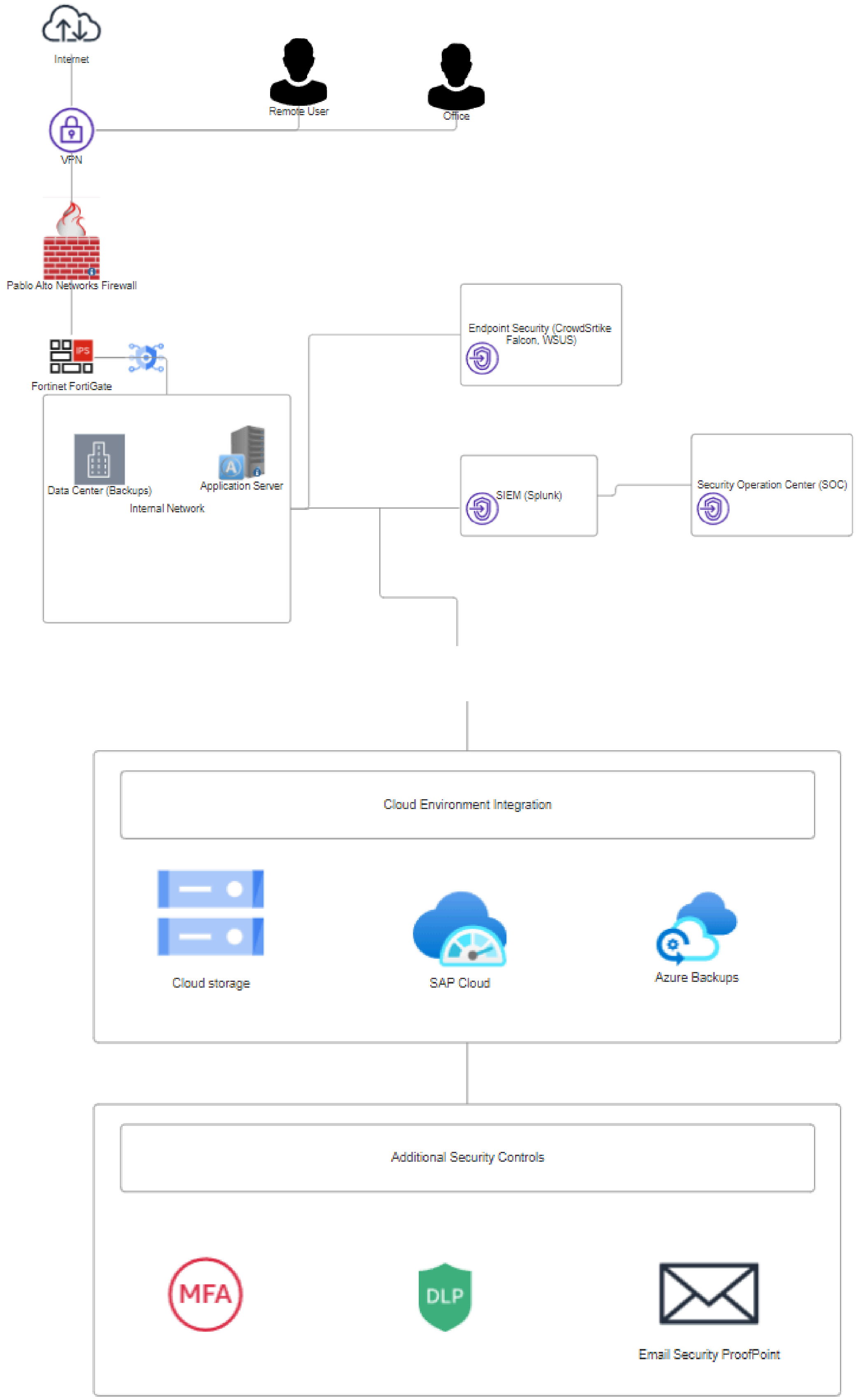
- Databases
  - DBAdmins
    - Read, Write, Execute, Modify, Delete
  - Developers
    - Read, Execute
  - Researchers
    - Read, Execute
  - Others
    - No Access
- Network Devices and Configurations
  - NetAdmins
    - Read, Write, Execute, Modify, Delete
  - SysAdmins
    - Read, Execute
  - Security Administrators
    - Read, Execute
  - Others
    - No Access
- Security Tools and Logs
  - SecAdmins
    - Read, Write, Execute, Modify, Delete
  - SysAdmins

    - Read, Execute
  - Others
    - No Access
- User Accounts and Group Policies
  - UserAdmins
    - Read, Write, Execute, Modify, Delete
  - SysAdmins
    - Read, Execute
  - Others
    - No Access
- Research Data and Projects Files
  - Researches
    - Read, Write, Execute
  - Developers
    - Read, Execute
  - Quality Assurance
    - Read Execute
  - Other
    - No Access
- Developement Enviroment and Source Code Repositories
  - Developers
    - Read, Write, Execute, Modify
  - SysAdmins

        - Read, Execute
    - Quality Assurance
        - Read, Execute
    - Others
        - No Access
- Testing Environments and Defect Tracking Systems
    - Quality Assurance
        - Read, Write, Execute
    - Developers
        - Read, Execute
    - SysAdmins
        - Read, Execute
    - Others
        - No Access
- Manufacturing Systems and Quality Control Data
    - Manufacturing
        - Read, Execute
    - SysAdmins
        - Read, Execute
    - Others
        - No Access
- Supply Chain Management Systems and Logistics Tools
    - SupplyChain

- Read, Write Execute
- SysAdmins
  - Read, Execute
- Others
  - No Access
- Customer relations ship systems, Sales Data and Marketing Tools
  - Sales:
    - Read, Write
  - SysAdmins
    - Read, Execute
  - Others
    - No Access

## Network Security Architecture Diagram


Internet
Remote User
Office
VPN
Pablo Alto Networks Firewall
IPS
Fortinet FortiGate
Endpoint Security (CrowdSrtike Falcon, WSUS)
Data Center (Backups)
Application Server
Internal Network
SIEM (Splunk)
Security Operation Center (SOC)
Cloud Environment Integration
Cloud storage
SAP Cloud
Azure Backups
Additional Security Controls
MFA
DLP
Email Security ProofPoint

**Endpoint Security Implementation Report**

Endpoint Security Solutions

1. Antivirus/Anti-Malware/Endpoint Detection and Response (EDR)
   - CrowdStrike Falcon Pro
   - $99.99 per device per year
   - Total Estimated Cost For 20,000 endpoints is $1,999,800 per year
2. Patch Management
   - Windows Server Update Services (WSUS)
   - WSUS is Free with Windows Server
   - Maintenance Cost: $90,000
   - Total Estimated Cost: $90,000
3. Multi-factor authentication (MFA)
   - OKTA
   - $3 per user per month
   - Total Estimated Cost for 20,000 users: $720,000 per year
4. Proofpoint (DLP and Email Security)
   - Email Security: $15 per user per year
   - DLP $5 per user per year
   - Total Estimated cost for 20,000 users: $400,000 per year

Grand Total Estimated Annual Cost: **$3,209,800**

**Deployment plan for Endpoint Security**

**Preparation Phase**

CrowdStrike Falcon Pro Deployment

- Register all the endpoints on the CrowdStrike Falcon management console.

WSUS Deployment

- Set up WSUS server and synchronize with the Microsoft Updates.

OKTA Deployment

- Set up the OKTA environment and integrate it with the enterprise directory.

Proofpoint Deployment

- Set up Proofpoint environment and integrate with email systems.

FortiGate Deployment

- Register all FortiGate devices with Fortinet support.

**Deployment phase**

CrowdStrike Falcon Pro Deployment

- Deploy the Falcon agent using deployment tools.

WSUS Deployment

- Configure the Group Policy to ensure the endpoints point to the WSUS server

OKTA Deployment

- Roll out MFA to different user groups in phases.

Proofpoint Deployment

- Deploy Proofpoint DLP and Email Security.

FortiGate Deployment

- Deploy FortiGate Devices around the network (data center, branch offices)

**Configuration**

CrowdStrike Falcon Pro Deployment

- Apply security policies based on endpoints

WSUS Deployment

- Define patching policies and schedules.

OKTA Deployment

- Roll out MFA to different user groups in phases.

Proofpoint Deployment

- Define DLP rules and email security policies.

FortiGate Deployment

- Set up firewall rules, NAT, VPN, and routing rules.
- Configure IDS IPS application control and web filtering.

**Monitoring and optimization phase.**

CrowdStrike Falcon Pro Deployment

- Aggregate logs into Splunk.

WSUS Deployment

- Monitor patch deployment and status and compliance reports.

OKTA Deployment

- Aggregate logs into Splunk.

Proofpoint Deployment

- Monitor DLP incidents and Email Security threats, all logs should be Aggregated logs into Splunk.

FortiGate Deployment

- Set up alerts for real-time monitoring.

Maintenance Phase

- Ensure proper patch management process is being followed as well as regular quarterly audits to ensure the optimization of the company endpoint security systems.

## References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

CISCO. (n.d.). *Networking, Cloud, and Cybersecurity Solutions*. Cisco. https://www.cisco.com/site/ca/en/index.html

CrowdStrike. (n.d.). *The CrowdStrike Falcon® platform*. Crowdstrike.com. https://www.crowdstrike.com/platform/

Fortinet. (2023). *Next-Generation Firewall (NGFW)*. Fortinet. https://www.fortinet.com/products/next-generation-firewall

ISO. (2023). *ISO/IEC 27001:2022(en)*. Iso.org. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

NIST. (2020). Security and privacy controls for information systems and organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

paloalto networks. (n.d.). *Global Cybersecurity Leader - Palo Alto Networks*. Www.paloaltonetworks.com. https://www.paloaltonetworks.com/

rockwell. (n.d.). *MES Solutions for Life Sciences | FactoryTalk | US*. Rockwell Automation. Retrieved July 25, 2024, from https://www.rockwellautomation.com/en-ca/products/software/factorytalk/operationsuite/mes/life-sciences.html

SAP. (n.d.). *MES: The Power of Real-Time Data*. SAP. https://www.sap.com/canada/products/scm/execution-mes/what-is-mes.html

SOLARWINDS. (n.d.). *What Is WSUS? Windows Server Update Services Guide - IT Glossary | SolarWinds*. Www.solarwinds.com. https://www.solarwinds.com/resources/it-glossary/wsus-windows-server-update-services