# Project Part 2

Justin Langevin

8648380

Conestoga College

SECU74020:

Secure Enterprise Architecture

August 11, 2024

**Asset Protection**
**Asset Inventory List**

| Asset Name | Type | Description | Location | Criticality | Sensitivity |
|---|---|---|---|---|---|
| NA-DC1-SERVER | Hardware | Main database which stores critical customer and business data | North America | High | High |
| NA-DC1-FIREWALL | Hardware | Network firewall for incoming and outgoing traffic | North America | High | Medium |
| NA-DC1-ROUTER | Hardware | Router for network connectivity | North America | High | Medium |
| NA-DC1-WSUS | Software | Windows Server Update Services for patch management | North America | Medium | Medium |
| NA-DC1-SAP | Software | SAP SCM system for supply chain management | North America | High | High |
| NA-DC1-VEEVA | Software | Veeva system for regulatory compliance | North America | High | High |
| NA-DC-DB | Data | Database containing drug formulas and patient clinical trial data | North America | High | High |

| | | | | | |
|---|---|---|---|---|---|
| NA-DC1-NETWORK | Network | Corporate network infrastructure | North America | High | Medium |
| GLOBAL-EMPLOYEES | Human | Employees | Global | High | High |
| NA-WAREHOUSE-1 | Hardware | Warehouse management system | North America | High | Medium |
| NA-MANUFACTURING-1 | Hardware | Manufacturing system for production control | North America | High | High |
| NA-PharmaSuite-1 | Software | The logistics system for tracking | North America | High | Medium |
| NA-DC1-IDS-IPS | Hardware | Intrusion Detection and Prevention System (Fortinet FortiGate) | North America | High | High |
| NA-DC1-CLOUD STORAGE | Data | Hybrid cloud storage for data (AZURE) | North America | High | High |
| NA-DC1-SIEM | Software | Security Information and Event Management (SIEM) (Splunk) | North America | High | High |
| NA-DC1-ENDPOINT | Software | Endpoint detection and response (EDR) solution (CrowdStrike Falcon) | North America | High | High |

**Asset Classification Report**

**Level of Criticality:**

- High: Downtime or break will cause a significant impact and financial loss
- Medium: Temporary downtime can be managed.
- Low: Minimal impact on the operations.

**Level of Sensitivity:**

- High: has sensitive data which requires the most secure protection.
- Medium: has important information that requires normal protection.
- Low: has nonsensitive information and needs minimal protection needs.

**Asset Protection Plan**

**Hardware**

- NA-DC1-SERVER
    - Protection Measures:
        - Physical Security (locks, movement sensors, cameras, etc)
        - Access Controls (RBAC)
        - Monitoring (SIEM, and Security teams)
        - Encryption(ensure data stored on the server is encrypted and in transit)
- NA-DC1-FIREWALL, NA-DC1-ROUTER, NA-DC1-IDS-IPS
    - Protection Measures:
        - Physical Security: (locks, movement sensors, cameras, etc)
        - Configuration Management: Regular updates and proper configuration.
        - Monitoring: Continuous SIEM monitoring and security teams.
- NA-WAREHOUSE-1, NA-MANUFACTURING-1, NA-LOGISTIC-1
    - Protection Measures:
        - Physical Security: (locks, movement sensors, cameras, etc)
        - Access Control (RBAC)
        - Inventory Control: inventory management systems to keep track of assets.

**Software**

- NA-DC1-WSUS, NA-DC1-SAP, NA-DC1-VEEVA, NA-DC1-SIEM, NA-DC1-ENDPOINT
    - Protection Measures:
        - Access Controls: RBAC and MFA.
        - Updates: Regular software updates and patch management.
        - Monitoring: SIEM monitoring and security reviews

**Data**

- NA-DC1-DB, NA-DC1-CLOUDSTORAGE

    - Protection Measures:
        - Encryption: Ensure data at rest and in transit (AES-256)
        - Access Controls: RBAC
        - Backups: ensure regular backups are securely stored.

**Network**

- NA-DC1-NETWORK
    - Protection Measures:
        - Firewalls: ensure they are correctly configured
        - Intrusion Detection and Prevention: use Fortinet FortiGate).
        - Network Segmentation: To limit access to critical areas.

**Human**

- NA-EMPLOYEES
    - Protection Measures:
        - Training: Regular security awareness training for employees.
        - Background Checks for all employees
        - Access Controls: Limit access based on roles and responsibilities (RBAC, Least Privilege)

## 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

Lenaerts-Bergmans, B. (2021, December 8). *What is a Supply Chain Attack? | CrowdStrike*. Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

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