CSCY 1030

August 21, 2023

Professor: Mohammed Alani

By: Aman Toor

**PHEONIX Project Case**

August 22, 2023, on the behalf of the WizardSpyder consulting group I, Aman Toor have been assigned with the clearance on the behalf of the USA and CANADIAN secret services in the consultation of the design and implementation for the Ethyon Corporations operation with both Government. The following report is confidential and is only accessible to those involved and authorized users and personals. The following document will aim to suggest and incorporate Architectural and networking proposals as well as the system model that I as a security consultant propose for the growth and goal of this active project.

Project Pheonix has been Classified as top secret by the US and Canadian Government, the operation is involved in nano programable aerosol that is deployed over land as a counterattack for viral attack from foreign and terror-based attacks. The Governments have required that Ethyon corporation keep the Pheonix project Top secret from the employee that are not involved in the Project. Simply put that all non-Pheonix activities are to be segregated from access of any Pheonix approved infrastructure. The location of the operation is set to be based in Las Vegas, Nevada. As per agreement with all three party’s requirement and, the proposed architecture and security will all be fulfilled in the best befitting way to accommodate each party. The accommodation and guidelines are as stated in bulletin points below.

A diagram of different types of computer systems

Description automatically generated with medium confidence**- Requirements/Guidelines-**

1. Security Model Selection
2. Architecture
3. Access Control
4. Staff Capability
5. Physical and Network Security
6. Data Exchange
7. Least Privilege Enforcement
8. Risk Management
9. Data Reporting
10. Defense in Depth
11. Controls Selection

The guideline showcased above will represent the outline of the report and my implementations and best fit suggestions for each category including a detailed brief explanation for the authorized users or personals reading this report for project phoenix. The above diagram is not a final view of the project’s architecture but rather a visual view of how it will possibly look.

Implementing a security model for Project Phoenix will provide researchers and staff with access to valuable information based on their authorization level. When configuring a security model, it's best to aim towards an open design architecture. The entirety of this architecture will be focused on the principles of open design planning, implying that all implementations will be based on pre-existing design concepts rather than building new design structures from the ground up. Recalling back to the selection of a security model, after reviewing the requirements from all three parties and their operational needs, the most suitable choice is the Bell-Lapadula model. The model of choice allows for the enforcement of confidentiality by preventing unauthorized users access information at a higher authorized security level. The key advantage lies in the "No Read Up" and "Write Up" policies. The "No Read Up" policy, also known as the Simple Security Policy, prevents unauthorized or lower-level personals from accessing highly classified data. This separation effectively isolates Ethyon employees involved in other operations from accessing Project Phoenix data, this allows for a clear distinction between different projects and their associated personnel as well as keeping project phoenix's Top secret within the organizations structure. The "Write Up" policy, often referred to as the Star Property, restricts high-level personnel from modifying lower-level data, effectively preventing any potential cross-contamination between the data of the different operations.

A diagram of two people

Description automatically generated

To assure that confidentiality and integrity is maintained with the system architecture of this operations life span, Enforcing the principle of least privilege is crucial in maintaining a secure and controlled environment for data access and manipulation. This approach can provide individuals with the minimum level of access needed to perform their daily tasks, reducing the risk of unauthorized personals. To implement this system effectively, strengthening access controls will involve around the evaluation of each individual personals work and tasks. Evaluating each personals work will allow for precise assignment of permissions, limiting their access to data and systems to the bare essentials. This approach also provides for the confidentiality and integrity of the phoenix project, as cross contamination will be much easier to prevent just as no read up and write down policies provide security. Additionally, Key management can be a critical concept for this strategy. Utilizing strong encryption protocols can be employed to safeguard sensitive information, and accessing decryption keys will be controlled through strict authorization mechanisms to prevent unauthorized personals. By following the least privilege policy and employing strong key management practices, the system will ensure that only authorized personals can access specific information. This approach will also help in mitigating the risk of unauthorized data leaks and attacks.

With the approach of utilizing the least privilege policy with key management, this design will require a staff trained to maintain the security and continues effectiveness of this system. With the increase of permission given by the USA and Canadian Secret Services, Project Phoenix has increased in numbers. The operation has now received 50 researchers and 40 support staff to operate, bringing a total of 90 authorized personals to sustain the system and its security. To ensure all staff capability, all personals involved as support staff in the operation of project will be required to undergo an assessment. This assessment will involve in the comprehensive review of skills, knowledge and experience of personnel who will be responsible for the implementing and maintaining the security measures. The assessment will also allow for identifying for any training needed or gaps in skills that may need addressing. This assessment will not be given alone to the support staff but also to the researchers, who will undergo a workshop class regarding work site security and maintaining the security of their credentials and authorization. This workshop will primarily focus on show casing how to protect their credentials, preventing phishing emails, maintain safety of encryption key and other attacks to look out for and how to prevent. The workshop will also be available to other personals and will be required to be held either between once a month or bi-monthly (every two months). With a well-prepared team, the operation can confidently navigate the security architecture, guaranteeing the integrity and confidentiality of project Phoenix's sensitive information.

The Affects that an assessment of all employees in project phoenix will also help to assign access controls to staff and researchers. Allowing determination based on experience, skills, and knowledge to assign access controls. With the assessments for operation staff, it will allow for determination of administrators, server technicians, Human resources, finance, as well as scheduled pen testers for vulnerabilities. With the determination of position and roll we can then begin assigning access controls needed for their position and tasks need to complete, allowing us to assign the bare minimum access to information and data they need. This will also follow for researchers and categorizing them by their skills and knowledge, providing them access control levels based on their bare minimum requirements.

It is also crucial to handle both physical and network security issues when protecting project Phoenix data and assets. Implementing a strong actively detect vulnerabilities culture within the operation can be ideal, this will prevent unapproved access or theft, and put measures in place to prevent these threats by assessing potential physical dangers to lab and data facilities. Restrictive access areas with biometric verification, surveillance cameras for ongoing oversight, and safe document storage should all be part of physical security protocols. Physical security is further improved by implementing a guest access policy that requests prior authorization and allows only restricted access to specific places with the company of a prior authorized personal within the project phoenix's staff.

A multi-layered strategy is crucial for network security. To protect against external cyber threats, a strong firewall system will be installed at the network's perimeter together with intrusion detection and prevention technologies. Data protection will further be increased by encryption methods like TLS (Transport Layer Security) for data transfer and end-to-end encryption for private communications. This method of encryption and end-to-end encryption communication can also be met with the Canadian governments request for information sharing between Project phoenix's lab in Nevada, with Ethyons lab located in Halifax, Canada. To find and fix potential network vulnerabilities, regular security audits, vulnerability assessments, and penetration testing should be carried out.

Moreover, putting in place an access control policy that upholds the least privilege will allow for only authorized workers to have access to sensitive information and systems. Two-factor authentication (2FA), which adds an additional layer of authentication, can be implemented for access to sensitive systems. Regular security awareness training for employees reduces the likelihood of social engineering attacks by fostering a security-conscious culture.

A strong security culture will also allow for project Phoenix to be protected by the integrated strategy that combines physical security protocols, visitor access restrictions, multi-layered network security measures, and access control policies. This strategy ensures the project's confidentiality, integrity, and availability while also protecting it from illegal physical access and cyber threats.

adhering to a data exchange strategy is mandatory for upholding confidentiality while enabling effective collaboration. Given the project phoenix's connection to both the Canadian and US governments, a clear design and planned approach for information sharing is important. To ensure quick and secure communication, distinct communication channels will be established for each government communication. These channels will be strengthened by encryption protocols, such as TSL, to safeguard data during transit.

In alignment with the least privilege policy, dedicated systems will be set up for each government, guaranteeing a clear segregation of data and minimizing any risk of leaked data sharing. Canada and the USA will have separate access points, each with unique authentication mechanisms to ascertain authorized entry. The data exchange process will be meticulously documented, and access will be granted only to individuals with the requisite security clearances, allowing for the operation's commitment to safeguarding sensitive information. The Utilization of TSL will allow for encryption of data during exchange as it is more secure and stronger than that of SSL and the use of an installed client for communication. TSL will also allow for one-way authentication which will come in handy for communication between Halifax lab and Nevada lab.

By adopting these measures, Project Phoenix can connect the gap between security protocols and seamless collaboration. This implementation would also enable the two governments to receive identical weekly progress reports at a timely matter while upholding the highest standards of confidentiality and data protection. This approach will help to secure the system’s security architecture, ensuring the project's success through a strong encryption protocol and integrated security framework.

Through intensive analysis and reconnaissance, potential risk areas can be identified, including physical breaches, data loss, and cyberthreats. Each risk will be thoroughly assessed, considering its likelihood of happening and potential effects on the safety and success of the project.

The possibility of a data breach during transmission may materialize, for example, in the context of data accessing through SSH port also known as port 22. To counter act this breach possibility encrypting and disabling access through remote access this port will help sustain the confidentiality of the data. Similar to this, the possibility of unauthorized individuals physically entering sensitive locations might be extremely dangerous. To address and reduce this danger, strict access control mechanisms combining biometric verification, security cameras, and regulated entry points can be put in place.

However, some risks may be deemed to have a low likelihood and impact. For instance, since it wouldn't significantly impair the project's overall security or objectives, the risk of minor software bugs affecting non-critical systems may be acknowledged and monitored till the next available staff is able to review and repair the bug.

This approach to risk management ensures that funds are wisely spent to address the most essential vulnerabilities while keeping a close watch on less serious threats. By adopting this approach, allows for Project Phoenix to maintain its goal of protecting sensitive information and guarantee the effective realization of its goals while striking a balance between proactive risk mitigation and risk acceptance.

Project phoenix is delicate, thus implementing a in depth defense system is crucial. By applying several layers of security measures will allow for increase in system defense, as well as reduced risks through the implementation of multiple layers for attackers to attack through. Project phoenix can protect against a range of potential risks by implementing multiple security controls at different levels, such as network, application, and physical access.

For instance, a in Depth Defense strategy for network security might involve installing firewalls at network perimeters, intrusion detection systems to watch over network traffic, and endpoint protection on individual devices. There are also suggestions for Access control procedures, security patrols, and surveillance cameras for physical security measures. By implementing these controls in a layered security system, you can be sure that even if one layer is compromised, the remaining levels will still be in place, lowering the risks of attackers. By thoughtfully implementing suggestions and ideas of security measures in dept for individual layers throughout project phoenix's system, it will provide for staff with a wider understanding of where attackers may appear from. This design also goes to show the operations’ commitment to the safeguarding of its assets and data.

Throughout the design and implementation suggestion for project phoenix a security control must be put in place. Through analyzing the operations goals, focus and criteria the best security control is Saltzer and Schroeder’s Principles. This security control accounts for all requirements provided by the USA and CANADIAN secret services following for, Separate privilege, least privilege, Fail-safe Default, and Open Design concepts. Although the ISO/IEC 19249 principle allows for layering it can be utilized through the use of defense in depth already implementation of layering.

To summarize this report, this concludes my design and implementation of a system architecture to assure the growth of project Phoenix. Through this report I’ve included system model suggestions, networking encryption protocols, implementation of systems to allow communication between both governments and as well as defense protocols and suggestions on implementing a strong reliable security culture among the staff. The aim of this report is to suggest and provide insight on implementation methods and fulfilling the requirement criteria of the USA and Canadian secret service, as a consultation on behalf of WizardSpyder.