SECURITY SOLUTION PROPOSAL FOR DEATH STAR, INC.

By: Bhavik Shah (118547640) and Akshat Mehta (119229194)

ENPM686 – 0201, Final Project

1. Introduction

The Death Star, Incorporated is a defense-oriented engineering firm (in a galaxy far, far away), focused on developing planetary weaponry. The company is responsible for safeguarding highly sensitive data, and in the past year, it has experienced several security incidents that have compromised its security posture. These incidents include ransomware attacks, spear-phishing campaigns, and distributed denial-of-service (DDoS) attacks on its client login portal. The attacks have led to the loss of critical data, rendering some machines unrecoverable, and exposing the organization to reputational damage and financial losses.

To mitigate the risks associated with these security incidents, Emperor Palpatine, the head of Death Star, Inc., has tasked us with developing a comprehensive security solution that would prevent further attacks, detect undetected attacks, and tolerate them. Our proposed solution should cover both Linux and Windows workstations used by the organization, enable secure communication between the networks, enable secure connectivity between mainframe and work-from-stations laptops, and protect the web server that serves as the hosting platform for selling products and offering customer support.

This paper proposes a security solution that involves the deployment of a next-generation firewall, intrusion detection, and prevention system, security information and event management (SIEM) system, web application firewall, and employee security awareness training programs. The proposed solution aims to enhance the confidentiality, integrity, and availability of sensitive data held by Death Star, Inc.

The paper first reviews the recent security incidents that have affected Death Star, Inc., and analyzes the current state of its security infrastructure. It then presents a detailed proposal for the security solution, which includes the benefits of each component of the proposed solution. Furthermore, the paper outlines an implementation plan for the proposed solution, with a focus on the costs and resources required to implement the solution. Finally, the paper concludes with a recommendation for future security measures to be adopted by Death Star, Inc. down the line annually with budget allocation.

2. Overview of Security Incidents

Over the past 365 days, Death Star, Inc. has suffered several security incidents that have impacted the organization’s data and operations. These incidents have demonstrated the vulnerability of the company’s security infrastructure, highlighting the need for a more comprehensive and robust security solution.

2.1 Spear-Phishing Campaigns

Various units within the organization fell victim to spear-phishing campaigns. Spear phishing is a targeted form of phishing that uses personalized messages to deceive the recipient into clicking

on a malicious link or downloading a malicious attachment. These attacks are often difficult to detect because they are tailored to the specific recipient and are designed to bypass traditional security measures.

Spear phishing campaigns are a common tactic used by attackers to gain access to an organization's system. Once inside the network, attackers can steal sensitive data or install malware that can be used to compromise other systems. The success of these attacks relies heavily on social engineering techniques, such as the creation of convincing fake emails that appear to come from a trusted source.

In our opinion, the rebel forces might have sent out an email with a malicious link. They have targeted several Death Star, Inc. employees and they only needed one of them to click the link present in the email. The rebel forces would have included a link to a worm that was downloaded on the Death Star, Inc.'s server, which then infected the servers with ransomware.

2.2 Ransomware Attacks

Several workstations within the organization were compromised by rebels with ransomware. Ransomware is a type of malware that encrypts data and demands payment in exchange for the decryption key. Of the five machines that were compromised, three were deemed unrecoverable. The loss of data on these machines could have had significant implications for the organization's operations and the confidentiality of its sensitive data. This might have also resulted in significant financial losses and can even lead to bankruptcy in extreme cases.

Ransomware attacks are a common tactic used by cybercriminals to extort money from organizations. Attackers like the rebel forces often use social engineering techniques, such as phishing, to gain access to an organization's systems. Once inside the network, they use malware to encrypt data and demand payment for the decryption key. Preventing ransomware attacks requires a multi-layered approach to security. In addition to thinking about prevention, Death Star, Inc. should also have a robust incident response plan in place to enable them to quickly detect and respond to a ransomware attack.

In our opinion, the rebel forces might have gained access to Death Star, Inc.'s systems through the series of phishing attacks launched by them. They might have sent out packaged malware through the phishing campaign, which was opened by one of Death Star, Inc.'s employees and gained access to the network. We have reason to believe that the malware might have been a worm as it traveled to 4 other workstations and infected them with the ransomware. There is a chance that even though the ransomware did not spread to other systems, the worm might have, giving access to the rebel forces to Death Star, Inc.'s network.

2.3 DDoS Attack

We discovered that the organization's client login portal had been under DDoS attacks intermittently for several months. A distributed denial-of-service (DDoS) attack is a type of

cyber-attack in which an attacker floods a network with traffic in an attempt to overload it and disrupt its operations.

DDoS attacks can be used to disrupt an organization's operations, causing significant financial losses and reputational damage. Attackers often use botnets to carry out these attacks, making it difficult to trace the source of the attack. Organizations can use various measures, such as web application firewalls and content delivery networks, to mitigate the impact of DDoS attacks.

2.4 Additional Risks

The use of laptops by personnel within the organization presents additional risks to the security of the organization's data. Laptops are often used outside of the organization's network, making them more vulnerable to cyber-attacks. When employees connect to the organization's network from their remote laptops, they might be accessing it from their personal network or even a public network. This can lead to attackers accessing sensitive data by performing a man-in-the-middle attack. Additionally, the use of personal devices, such as smartphones and tablets, to access the organization's system can increase the risk of unauthorized access to sensitive data.

3. Current State of the Death Star, Inc.'s Security Infrastructure

The Death Star, Inc.'s security infrastructure is currently inadequate, as evidenced by the recent security incidents that have impacted the organization. Several computers within the organization were compromised with ransomware, and various units fell victim to spear-phishing campaigns. We also discovered that the network had been attacked for months via DDoS attacks on the client login portal. Additionally, of the devices compromised with ransomware, three of the five machines were unrecoverable.

The company relies on a perimeter firewall that is only capable of layer 2 verification. While the firewall provides some protection, it is insufficient in preventing advanced attacks that can bypass traditional firewall protection. The firewall does not have the ability to inspect the contents of the network packets and identify potential threats. Furthermore, the company's web server, which serves as a platform for selling products and offering customer support, is also inadequately secure. The web server is hosted locally, and there are no measures in place to protect against web-based attacks such as SQL injection and cross-site scripting (XSS).

The company's data center consists of a primary and a failover mainframe, which houses the Linux computers used for scientific research and Windows computers for administrative tasks. The age of equipment makes it difficult to enable encryption, which is a critical security feature for protecting sensitive data. On top of that the computers are not segmented and communicate with each other through the same network. The design makes it easier for attackers to move laterally within the network, as they can pivot from one compromised machine to another. Additionally, the company has issued laptops to employees to enable increased work-from-starship capabilities, but there are no measures in place to secure these laptops against external threats such as malware infections.

The lack of an intrusion detection and prevention system (IDPS) and security information and event management (SIEM) system makes it difficult to detect and respond to security incidents. The absence of an IDPS means that the company is unable to identify and prevent potential threats. Similarly, the absence of a SIEM system means that the company is unable to collect and analyze security logs from its various systems, which can help in identifying and mitigating potential security threats.

In summary, Death Star, Inc.'s current security infrastructure is inadequate and leaves the company vulnerable to a range of security threats. The company's reliance on traditional firewall protection, the lack of measures to secure the web server, the absence of a network segmentation strategy, and the absence of an IDPS and SIEM system are significant vulnerabilities that must be addressed to prevent future security incidents.

Asset Name	Category	Description	Severity
Primary Data Center	Physical Asset	The primary data center for Death Star Inc. where all sensitive data regarding weapon plans, employee information, customer information, the web server for advertisement, and the customer portal	Critical
Failover Backup Mainframe	Physical Asset	The secondary mainframe stores the same data as the primary which is activated when the primary fails	Critical
Linux Workstations	Physical Asset	Workstations to perform scientific research	High
Windows Workstations	Physical Asset	Workstations to perform administrative functions	High
Perimeter Firewall	Physical Asset	The firewall that can scan till level 2	Critical
Work from Spaceship Laptops	Physical Asset	Laptops provided to employees so that they can work remotely - OS are Linux, Mac, Windows	High
OS on the systems	Software Asset	Linux, Mac, and Windows installed on the workstations and WFS laptops	High

Locally Hosted Webserver	Software Asset	Web servers where the advertisement and customer support software is hosted	High
Advertisement and sales Software	Software Asset	A web page to sell and advertise Death Star products	High
Customer Support Portal Software	Software Asset	Web page for customer support	High
Existing Antivirus and Antimalware Software	Software Asset	Any existing antivirus software installed on the system	High
LAN connected assets	Network Asset	Devices like workstations and mainframes are connected via LAN in DeathStar Inc.	High
WAN connected assets	Network Asset	Devices like routers, firewalls, network monitoring and management tools, and ISP	Critical
Sensitive Data related to weaponry and research	Data Asset	All the plans, blueprints, and research performed for the products and weapons	Critical
Customer Information	Data Asset	Details of clients who have purchased from DeathStar Inc in the past	High
Employee Information	Data Asset	Employee details like names, addresses, family details, phone numbers, bank details, tax details	High

4. Proposed Security Solutions

4.1 Local Deployment Plan

4.1.1 Hiring Dedicated Security Staff

Hiring dedicated security staff for Death Star Inc is crucial to ensure that the company's security needs are met. A dedicated security team can provide a range of benefits, such

as increased security expertise, regular security maintenance, timely incident response, compliance, and training and awareness. It is recommended that the company hire at least two full-time security administrators with relevant security certifications, such as CISSP, CISM, or CompTIA Security+.

4.1.2 Upgrade IT infrastructure

Upgrading the IT infrastructure is a critical step in improving the overall security posture of Death Star, Inc. As noted, the current on-premises data center is using outdated equipment that cannot be encrypted, which makes the data stored in the data center vulnerable to attacks. Upgrading the infrastructure will help to address this vulnerability by replacing outdated equipment with modern equipment that supports encryption.

4.1.3 Network Upgrade and Management

The network upgrade and management plan is a crucial aspect of enhancing the security of Death Star Inc. It involves upgrading the company's network infrastructure to ensure that it can handle the traffic generated by employees and customers while also remaining secure.

The first step is to design a secure network that is resilient to attacks, breaches, and other malicious activities. This can involve segmenting the network traffic to ensure that sensitive information is kept separate from other less critical data. By doing this, Death Star Inc can minimize the risk of unauthorized access to sensitive information.

Additionally, implementing access control policies will further strengthen the security of the network. Access control policies help to ensure that only authorized personnel can access the network and its resources. Hardware upgrades will also be required, especially in the case of networking equipment. To enable secure communication between the Linux and Windows networks, there is a need to upgrade network hardware and software, including switches and routers. The new network should be based on a new topology with network segmentation, to prevent attackers from compromising the entire network in case of a breach. The routers should also be updated with the latest software to ensure that all vulnerabilities are patched.

The network upgrade and management plan is essential for solving several security problems. First, it helps to prevent unauthorized access to sensitive information by implementing access control policies and network segmentation. Secondly, it helps to detect any suspicious activities on the network, enabling Death Star Inc to take immediate action to prevent any potential breaches.

4.1.4 XDR Infrastructure

XDR (Extended Detection and Response) infrastructure can provide a holistic approach to threat detection and response by combining multiple security solutions into one platform. The integration of EDR, NDR, and SIEM tools can help Death Star, Inc. detect, investigate, and respond to security incidents in real time. Sophos Central Intercept X Advanced with XDR is recommended as it provides deep learning anti-malware, anti-exploit technology, and advanced threat detection capabilities. The solution is cloud-based and can be easily managed by the dedicated security staff.

Endpoint Detection and Response (EDR) tools can help Death Star, Inc. monitor and respond to security incidents on individual devices, such as laptops and mobile phones, by analyzing endpoint activities for suspicious behavior and taking action to contain and remediate potential threats. Network Detection and Response (NDR) tools can monitor network traffic and detect potential threats such as malware, phishing attempts, and other malicious activities. SIEM tools can collect and analyze security event data from across the IT environment to identify potential threats and prioritize them based on risk.

The XDR infrastructure can help solve several problems for Death Star, Inc., including:

1. Improved threat detection and response: XDR infrastructure can provide a more comprehensive view of the security posture of the organization by monitoring and correlating security events from multiple sources, leading to faster and more effective threat detection and response.

2. Increased visibility: XDR infrastructure can provide a single pane of glass view of the security environment, making it easier to identify potential security incidents and prioritize them for remediation.

3. Centralized Security Management: The XDR solution will provide a centralized view of the organization's security posture, making it easier to manage and respond to security incidents.

4. Real-Time Threat Intelligence: The XDR solution will provide real-time threat intelligence, enabling the organization to respond quickly to emerging threats.

4.1.5 Firewall Upgrade

Upgrading the firewall is an essential part of the proposed security solution. The current firewall is only capable of layer 2 verification, which is not enough to protect against modern-day cyber threats. Therefore, Death Star, Inc. needs to invest in a modern firewall with advanced security features.

The proposed firewall is Sophos XGS 3100 with XStream protection. Sophos XGS 3100 is a next-generation firewall that provides comprehensive protection against advanced threats, malware, and zero-day attacks. The firewall comes with advanced security

features such as Intrusion Prevention System (IPS), Application Control, Web Filtering, and Advanced Threat Protection.

The XStream protection is a real-time deep packet inspection technology that provides protection against advanced threats such as ransomware, zero-day exploits, and malware. The technology uses machine learning and behavioral analysis to identify and block malicious traffic in real time, thereby reducing the risk of a successful cyber attack.

In addition to the advanced security features, the Sophos XGS 3100 also provides easy-to-use management and reporting tools. The firewall can be managed through a web-based console that provides a central point of control for all security policies. The console provides real-time visibility into network traffic, allowing security administrators to monitor and respond to security events quickly.

The proposed firewall upgrade will provide Death Star, Inc. with advanced security features that are essential in today's cyber threat landscape. The firewall will provide comprehensive protection against advanced threats, malware, and zero-day attacks. It will also provide real-time visibility into network traffic, allowing security administrators to monitor and respond to security events quickly.

4.1.6 Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security measure that requires users to provide two or more forms of authentication to access a system or application. MFA is an effective way to protect against stolen or weak passwords, as it adds an extra layer of security by requiring additional information that only the authorized user should have.

To implement MFA in Death Star, Inc., the company should adopt Google Authenticator, a widely used MFA solution. Google Authenticator is a free app that generates a unique code every 30 seconds on the user's mobile device. This code, in combination with the user's password, is required for access to any system or application.

To maintain security, it is important to periodically review and audit MFA settings. Administrators should regularly monitor the logs of MFA authentication attempts to identify any suspicious activity, such as repeated login failures, unauthorized access attempts, or other anomalies.

4.1.7 VPN Services

To provide secure connectivity for remote workers and protect the company's sensitive data, a Virtual Private Network (VPN) will be implemented. The VPN will allow remote workers to securely connect to the company's network as if they were physically present in the office. This will ensure that sensitive data is protected even when employees are working from outside the office.

The VPN solution chosen for Death Star, Inc. is Cisco AnyConnect VPN. AnyConnect provides secure remote access to the company's network and can be installed on a variety of platforms, including Windows, Mac, and Linux. AnyConnect also supports multi-factor authentication, which will be implemented for additional security.

To ensure that the VPN solution is secure, all traffic between the employee's laptop and the company's network will be encrypted using SSL/TLS. This will prevent any potential eavesdropping or man-in-the-middle attacks. Additionally, access to the VPN will be restricted to authorized employees only.

Regular audits will be conducted to ensure that the VPN solution is functioning as expected and that all security measures are in place. This will include reviewing logs and monitoring access to the VPN server.

4.1.8 Employee Training and Awareness

Employee training and awareness are essential components of any security program. No matter how much money is spent on hardware, software, and security personnel, employees who are not properly trained and aware of security risks can be the weak link in an organization's security posture.

To address this issue, Death Star, Inc. should implement a quarterly employee training and awareness program that covers a variety of security-related topics. The training should be mandatory for all employees and should cover both general security best practices and specific policies and procedures implemented by the company.

The training should cover a range of topics including:

1. Password Security: Employees should be trained on the importance of creating strong passwords and regularly changing them. They should also be educated on the risks of using the same password for multiple accounts and the importance of using a password manager to securely store passwords.

2. Phishing Awareness: Employees should be trained to recognize phishing emails and other social engineering attacks, such as phone calls or text messages. They should be taught how to identify suspicious emails and how to report them to the IT department.

3. Data Protection: Employees should be educated on the importance of protecting sensitive company data. They should be taught how to properly handle confidential information, such as encrypting files and using secure methods to transfer data.

4. Device Security: Employees should be trained on how to secure their devices, including laptops, smartphones, and tablets. This should include best practices for securing devices both in and out of the office.

5. Incident Reporting: Employees should be taught how to report security incidents to the IT department. This should include reporting procedures for lost or stolen devices, suspicious emails, and other potential security breaches.

The training should be delivered in a variety of formats, including online courses, live seminars, and written materials. The training should be interactive, engaging, and designed to hold employees' attention.

To ensure that employees are retaining the information presented in the training, regular assessments and quizzes should be given. Employees who do not pass the assessments should be required to retake the training.

Finally, to reinforce the importance of security best practices, the company should consider offering incentives for employees who demonstrate a strong commitment to security. This could include recognition programs or bonuses for employees who report potential security incidents or successfully complete the training and assessment modules.

4.2 Cloud Deployment Plan

Through the cloud deployment proposal, we aim to migrate the mainframes and server to the cloud without spending an excessive amount of money on it. The proposal for majority part of the solution remains the same as the local deployment solution and so we would like Death Star, Inc. management to focus on the components where differences arise between both solutions.

4.2.1 Cloud Upgrade

Cloud migration is the process of moving an organization's data, applications, and infrastructure to cloud-based services. Moving to the cloud can offer several benefits such as scalability, cost savings, increased flexibility, and better security. In the case of Death Star, Inc., migrating the mainframe to AWS S3 cloud storage and the server to AWS EC2 instances can significantly improve the security posture of the organization. Here are some of the benefits of migrating to the cloud:

1. Improved Security: AWS provides numerous security features such as firewalls, encryption, access controls, and monitoring tools that can help protect the organization's data and infrastructure. Additionally, AWS regularly updates its security features and adheres to strict compliance standards.

2. Scalability: AWS allows for elastic scalability, which means that the resources can be quickly scaled up or down depending on the organization's needs. This can help reduce costs and provide better performance.

3. Cost Savings: By moving to the cloud, Death Star, Inc. can reduce the costs associated with maintaining an on-premises infrastructure such as hardware maintenance, electricity, and cooling costs. Additionally, AWS provides a pay-as-you-go model, which means that the organization only pays for the resources it uses.

4. High Availability: AWS offers high availability and redundancy features such as multi-region deployment, auto-scaling, and load balancing. These features ensure that the organization's resources are always available and can provide better uptime.

Cloud upgrades can also address various security loopholes such as data breaches and unauthorized access to the cloud infrastructure. By implementing the latest cloud security measures and services, Death Star, Inc. can protect its cloud infrastructure from potential cyber threats.

4.2.2 IAM System

Identity and Access Management (IAM) is an important component of any modern cybersecurity strategy. It refers to the set of policies, technologies, and practices used to manage digital identities and control access to resources within an organization's IT infrastructure. In the context of Death Star, Inc., implementing IAM through AWS can help improve security by providing centralized control over user access to cloud resources.

AWS offers a wide range of IAM features that can be leveraged to control user access to AWS resources. The first step is to create a new IAM user for each employee that requires access to the AWS console or resources. IAM users can be granted permission to access specific AWS services and resources using policies that are managed centrally.

One important feature of AWS IAM is the ability to create IAM roles. An IAM role is like an IAM user, but it is intended to be assumed by other AWS services or applications. Another important aspect of AWS IAM is the ability to set up multi-factor authentication (MFA) for user accounts. This is an additional layer of security that requires users to provide a second form of authentication, such as a security token or biometric data, before gaining access to AWS resources.

4.2.3 Firewall Upgrade

To enhance the security posture of Death Star, Inc., the firewall needs to be updated to a more robust and sophisticated solution capable of detecting and preventing advanced threats. The current perimeter firewall used by the organization only offers Layer 2 verification and lacks the ability to perform deep packet inspection, which can lead to undetected threats entering the network.

A more advanced firewall solution that provides full packet inspection capabilities is the AWS network and web application firewall. This solution offers an application-aware firewall that can detect and prevent common web-based attacks such as SQL injection, cross-site scripting, and cross-site request forgery.

The AWS network and web application firewall also provide intrusion detection and prevention capabilities, which enables the firewall to automatically block traffic from known malicious sources, as well as traffic that violates specific security policies.

The AWS network and web application firewall is also capable of providing granular controls to manage traffic flows between different network segments within the organization. This feature enables the organization to segment its network into smaller, more secure zones, limiting the ability of attackers to move laterally across the network.

Moreover, the AWS network and web application firewall can provide centralized visibility and management of security policies, making it easier for security administrators to manage and enforce security policies across the entire network.

5. Implementation Plan and Cost Estimate for Proposed Solutions

5.1 Implementation Plan and Cost Estimate for Local Deployment Proposal

The implementation plan for the proposed local deployment security solution involves a step-by-step process of upgrading the security infrastructure of The Death Star, Inc. to prevent future security incidents. The implementation plan will include the deployment of new security hardware and software, the implementation of new security policies, and employee training programs.

The first step in implementing the proposed security solution is hiring at least two full-time security administrators. The security administrators will be responsible for monitoring the security infrastructure, analyzing security alerts, and responding to security incidents. They will also be responsible for developing security policies, managing security configurations, and implementing security controls. These administrators will also be responsible for overseeing the day-to-day operations of the security infrastructure, including the implementation and maintenance of various security systems, as well as ensuring that all employees are trained on proper security practices.

One of the first tasks in the equipment upgrade process is to patch all operating systems (OS) and software applications to their latest versions. This will involve upgrading Windows and Linux operating systems on all devices, as well as ensuring that all software applications are running the latest available version. It is also important to remove any legacy software that is no longer being used to prevent attackers from exploiting known vulnerabilities in outdated software. Another critical task is to upgrade outdated workstations. As noted in the scenario, several computers in the organization were compromised, and three of them were unrecoverable. It is therefore essential to upgrade all workstations to the latest models with updated hardware specifications, such as the latest CPU, RAM, and storage devices. Additionally, all workstations must be equipped with updated anti-virus software with real-time monitoring capabilities.

The network topology will be changed to include network segmentation, which will help isolate potential security incidents. The router software will also be updated to include the latest security features. The next-generation firewall, specifically the Sophos XGS 3100 with XStream protection, will be deployed to monitor network traffic and prevent unauthorized access.

In the next phase, the installation of an XDR solution, specifically Sophos Central Intercept X Advanced with XDR will take place. With that we will secure the critical components of Death Star, Inc. After that, we will work on nuanced implementations like Google MFA and Cisco AnyConnect VPNs on every single device being used by the organization. Finally, we will hire a 3rd party organization that specializes in employee awareness and training programs to bring awareness about cybersecurity to the employees of Death Star, Inc.

The implementation plan will be executed in a phased approach, starting with the most critical systems first. The security administrators will work closely with Order 66 Consulting to ensure that the plan is executed effectively and with minimal disruption to the business operations of Death Star, Inc.

	Description	**Cost ($/year)**
Infrastructure Upgrade		
Network Infrastructure	Upgrade of routers and WAN devices	50,000 (one time cost)
Workstation and Laptop Upgrades	Upgrade and Patches on all devices	100,000 (one time cost)

Personnel Hire Salary	Salary for dedicated security staff	150,000
Security Solutions Upgrade		
MFA	Google Authenticator	Free
XDR Security Solution	Sophos Central Intercept X Advanced with XDR	180,000
Firewall Solution	Sophos XGS 3100 with XStream protection	9,978
VPN	Cisco AnyConnect VPN	4,018
Miscellaneous		
Periodical Security Assessment	Conduct assessments on quarterly level	18,000
Employee Training and Awareness Program	Training session for employees	2,000-12,000
Total		513,996 - 523,996

5.2 Implementation Plan and Cost Estimate for Cloud Deployment Proposal

To begin the implementation of the cloud deployment plan, we will start by hiring 2 dedicated security administrators. In addition to their responsibilities as mentioned above, they will also help carry out the migration of the web server and mainframes to the cloud.

The next step will be to migrate Death Star, Inc.'s web server to an AWS EC2 instance. To implement this solution, the first step is to select an appropriate AWS EC2 instance type based on the organization's requirements, such as the expected traffic load, memory, CPU, and storage requirements. Once the instance type is selected, the next step is to create an EC2 instance in the AWS console and install the necessary software, such as the web server software and any required dependencies. Post that, the organization should transfer the website data from the current on-premises server to the new EC2 instance. Additionally, it is important to configure the new EC2 instance's security settings, such as setting up firewall rules, restricting access, and enabling SSL/TLS encryption. Finally, to ensure high availability and fault tolerance, the organization can configure the AWS Elastic Load Balancer (ELB) to distribute traffic among multiple EC2 instances and configure auto-scaling to automatically adjust the number of EC2 instances based on demand.

The next step is to migrate the mainframes to cloud storage so that Death Star, Inc. can reduce its reliance on outdated and potentially vulnerable hardware and software. If Death Star, Inc. management decides to go forward with this plan, Order 66 Consulting will help devise a detailed migration plan that will outline the steps involved in migrating the mainframes to the cloud, including data transfer, the configuration of the cloud environment, and testing. The next step will be to transfer the data from the mainframes to the cloud environment and configure the storage settings to meet the company's needs. This will include configuring access controls, encryption, and backup and recovery options. Once the migration is complete and the mainframes are fully operational in the cloud environment, the old hardware will be decommissioned and securely disposed of.

The company's perimeter firewall will be upgraded to an AWS web application and network firewall. This will provide enhanced protection against web-based threats, such as SQL injection and cross-site scripting (XSS) attacks.

Overall, the implementation of the proposed cloud solution will require a significant investment of time and resources. However, the benefits of enhanced security and protection of sensitive data make this investment necessary. The implementation plan will be carried out in stages to minimize disruption to the company's operations, and ongoing monitoring and maintenance will be provided to ensure that the company's security posture remains strong over time.

	Description	**Cost ($/year)**
Infrastructure Upgrade		
Network Infrastructure	Upgrade of routers and WAN devices	50,000 (one time cost)

Workstation and Laptop Upgrades	Upgrade and Patches on all devices	100,000 (one time cost)
Webserver on Cloud	Host webserver on AWS EC2	5,630
Mainframes on cloud	Host mainframe and backup on cloud	2,338
Personnel Hire Salary	Salary for dedicated security staff	150,000
Security Solutions Upgrade		
MFA	Google Authenticator	Free
XDR Security Solution	Sophos Central Intercept X Advanced with XDR	180,000
Firewall Solution	AWS Web Application and Network Firewall	7,325
VPN	Cisco AnyConnect VPN	4,018
Miscellaneous		
Periodical Security Assessment	Conduct assessments on quarterly level	18,000
Employee Training and Awareness Program	Training session for employees	2,000-12,000

Total	569,311 - 579,311

6. Recommendation

After evaluating the current state of security at The Death Star, Inc. and considering the proposed security solutions, we recommend moving forward with a cloud deployment solution. While both the local security deployment and cloud migration deployment plans offer improvements to the current security infrastructure, a cloud deployment solution provides several advantages that make it the superior option.

One of the main advantages of a cloud deployment solution is the cost savings it offers. As noted in the cost and resources required section, a complete upgrade of the mainframes would be extremely expensive, costing millions of dollars. With a cloud deployment solution, the company can avoid these costs and instead pay for only the resources they need, reducing overall expenses. Additionally, the remaining budget of $100,000 can be used to speed up the cloud deployment process.

Another advantage of a cloud deployment solution is scalability. Cloud providers offer the ability to quickly scale up or down as needed, allowing The Death Star, Inc. to easily adjust to changes in demand. This is particularly important for a company like The Death Star, Inc., which has varying computing needs for its scientific research and administrative tasks.

A cloud deployment solution also offers improved disaster recovery and business continuity. With cloud deployment, data is stored off-site and can be quickly recovered in the event of a disaster, providing better protection against data loss. Additionally, because the data is stored off-site, employees can access it from anywhere with an internet connection, ensuring that business can continue as usual even in the event of an office closure or other disruption.

While a cloud deployment solution may take longer to implement than a local security deployment solution, the benefits it offers make it the superior choice. With the budget and resources available, we believe that a cloud deployment solution is the best option for The Death Star, Inc. to improve its security infrastructure.

In conclusion, we recommend that The Death Star, Inc. move forward with a cloud deployment solution. This solution provides cost savings, scalability, and improved disaster recovery and business continuity, making it the superior choice for enhancing the company's security infrastructure. We also recommend that the company continues to evaluate and implement additional security measures as needed to ensure ongoing protection of its sensitive data.

7. Future Pipeline Projects Proposal

While the proposed security solution is comprehensive, it is essential for The Death Star, Inc. to continue evolving its security posture to stay ahead of the ever-changing threat landscape. Therefore, this section outlines the recommended pipeline projects for the next five years.

7.1 Year 1: Business Continuity and Disaster Recovery Plan

Year 1 of the proposed security pipeline involves the development and implementation of a business continuity and disaster recovery plan (BCDR). A comprehensive BCDR plan is crucial for ensuring that Death Star, Inc. can recover from any type of disruption, whether it be a natural disaster or a cyber-attack. This plan should outline the procedures and protocols for restoring critical business functions and infrastructure after a disaster or disruption. It should also include measures to ensure that sensitive data is protected and recoverable in the event of data loss or corruption.

To develop a BCDR plan, Death Star, Inc. should begin by conducting a risk assessment and business impact analysis. This will help identify potential threats and vulnerabilities to the organization and determine the criticality of various business functions and systems. With this information, the organization can create a plan that outlines the necessary steps for restoring essential business functions and infrastructure in the event of a disruption or disaster. This plan should also include regular testing and updating to ensure that it remains effective over time. By implementing a BCDR plan, Death Star, Inc. can minimize the impact of any potential disruptions and ensure business continuity in the face of adversity.

7.2 Year 2: Insider Threat Program

The second year should focus on developing an insider threat program to monitor and prevent unauthorized access or exfiltration of sensitive information. Insider threats are a significant risk for organizations, and Death Star Inc is no exception. The company has sensitive information that should not be accessed or exfiltrated by unauthorized individuals. An insider threat program aims to identify and prevent insider threats from causing harm to the organization. The program will also help identify the root cause of an insider threat and mitigate the impact of such a threat. The insider threat program should be comprehensive and cover all aspects of the organization, including IT infrastructure, personnel, and processes.

To develop an insider threat program, the organization should first identify the critical assets that need to be protected. The organization should identify the types of data that are most sensitive, the employees who have access to that data, and the systems used to store or transmit the data. Once the critical assets are identified, the organization should establish policies and procedures to control access to those assets. The policies should define who has access to the assets and how that access is granted or revoked. The policies should also define the acceptable use of the assets and the consequences of unauthorized access or misuse of the assets. The organization should also implement technical controls such as access controls,

monitoring, and auditing to detect and prevent insider threats. Finally, the organization should train its employees on the policies and procedures and the consequences of violating them. By developing an insider threat program, Death Star Inc can significantly reduce the risk of insider threats and protect its critical assets.

7.3 Year 3: Security Operations Center and Dedicated Security Staffing

In the third year, The Death Star, Inc. should invest in developing a dedicated security operations center (SOC) and employee dedicated security staffing. Having a SOC in place will provide Death Star, Inc. with a dedicated team of security professionals who can detect, analyze, and respond to threats in real time. The SOC will use a variety of technologies and tools to monitor the organization's network, including intrusion detection systems (IDS), security information and event management (SIEM) systems, and advanced threat intelligence feeds.

The SOC team will work together to identify and mitigate security incidents and will also be responsible for developing and maintaining incident response plans. The SOC will collaborate with other teams across the organization, such as the IT department and management, to ensure a cohesive security strategy. In addition to developing a SOC, it is also recommended to hire dedicated security staff. These security professionals will work closely with the SOC to monitor the organization's IT infrastructure and ensure that security incidents are identified and resolved in a timely manner. The security staff will also be responsible for implementing security policies, procedures, and best practices across the organization, including training employees on security awareness and maintaining security compliance. Hiring dedicated security staff will help to ensure that security incidents are identified and resolved quickly, reducing the risk of damage to Death Star, Inc.'s reputation, financial stability, and customer trust.

7.4 Year 4: Formal Encryption Program

In the fourth year of our security pipeline proposal, Death Star Inc. will focus on developing and implementing a formal encryption program. This program will ensure that sensitive information is protected both at rest and in transit. Encryption is a critical component of any security program and is particularly important for protecting sensitive data from external threats such as cybercriminals, nation-states, and hacktivists. The formal encryption program will ensure that all sensitive data is encrypted using strong, industry-standard encryption algorithms such as AES or RSA.

To implement the encryption program, Death Star Inc. will need to evaluate its existing infrastructure and applications to identify any potential gaps or vulnerabilities. This assessment will help them determine which systems and applications need to be upgraded or replaced to support the new encryption program. They may need to invest in new hardware or software to support encryption, such as hardware security modules (HSMs) or data encryption software. The company will also need to ensure that all employees are trained on how to properly use encryption to protect sensitive data and that they understand the importance of keeping their encryption keys secure. By implementing a formal encryption program, Death Star Inc. will

significantly reduce the risk of data breaches and protect its sensitive information from unauthorized access or theft.

7.5 Year 5: Data Loss Prevention Program

In the fifth year, The Death Star, Inc. should develop and implement a formal data loss prevention (DLP) program to prevent unauthorized exfiltration of sensitive information. The DLP program should identify sensitive information and monitor all outbound communications, including email and file transfers, to prevent unauthorized exfiltration. The program should also include policies and procedures for reporting and responding to incidents involving the exfiltration of sensitive information.

The proposed pipeline projects for Death Star, Inc. recommended by Order 66 Consulting, provide a clear roadmap for evolving the company's security posture. While these projects require additional investment, they are essential for protecting the sensitive information held by the company. Order 66 Consulting can help implement these projects, and The Death Star, Inc. should review and update its existing cybersecurity program to ensure that it remains effective and relevant in today's threat landscape.

8. References

1. NIST. (n.d.). Framework for Improving Critical Infrastructure Cybersecurity. In https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
2. CISA. (n.d.). *CRR Supplemental Resource Guide*. https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-AM.pdf
3. NIST. (n.d.-b). *IT Asset Management* (No. 1800–5). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.1800-5.pdf
4. *Cisco AnyConnect Plus - license - 250 users - AC-PLS-P-250-S - Firewalls - CDW.com*. (n.d.). CDW.com. https://www.cdw.com/product/cisco-anyconnect-plus-license-250-users/3564987?pfm=srh
5. Sophos. (2023, May 9). *Endpoint Protection with Sophos Intercept X*. SOPHOS. https://www.sophos.com/en-us/products/endpoint-antivirus

6. *CrowdStrike Falcon vs SentinelOne Singularity vs Sophos Intercept X | TrustRadius*. (n.d.). TrustRadius. https://www.trustradius.com/compare-products/crowdstrike-falcon-vs-sentinelone-singularity-vs-sophos-intercept-x#pricing
7. Sophos. (2023b, May 9). *Sophos Next-Gen Firewall Features*. SOPHOS. https://www.sophos.com/en-us/products/next-gen-firewall/features
8. *Sophos XGS 3100 | EnterpriseAV*. (n.d.). https://www.enterpriseav.com/XGS-3100.asp#standard
9. *AWS Pricing Calculator*. (n.d.). https://calculator.aws/#/addService