****

**NORTHEASTERN UNIVERSITY  
ITC 6520 Fall 2022**

**Section 01**

**Network Protection & Cloud Security Project**

**By Group 3:**

[**Abhishek Vijayakumar**](https://northeastern.instructure.com/groups/118526/users/170316)**,**

[**Fanta Sow**](https://northeastern.instructure.com/groups/118526/users/63451)**,**

**Nsikak-Abasi Una**

**YAHOO CYBERSECURITY PLAN**

**PURPOSE**

A cybersecurity plan is one of the essential mechanisms an organization must show its customers and partners as it shows trust and data privacy. Due to the gravity of the security incident that occurred. In September 2016, Yahoo released the first information on the Yahoo cyberattack. 500 million users' data were stolen by hackers in late 2014. There were eight million UK-based accounts in all. Yahoo was informed of the intrusion but was not aware of the extent of the hack. In July 2016, Yahoo learned that 200 million customer accounts were up for sale on a darknet market website while investigating another data breach. Info Armor, a private security firm, claimed that a select group of hackers grabbed Yahoo's information. These hackers are contractors who work for the highest bidder. The hacking group, according to Info Armor, was called "Group E." They undoubtedly have an Eastern European base of operations, broke into Yahoo, and took data for three private agreements. The third purchase was a "state-sponsored actor" looking for information on U.S. government and military personnel, while the other two buyers were clandestine spammers.

# Yahoo planned to move its on-premises data centers to the cloud. Still, it neglected to set up efficient risk assessment procedures before doing so, leaving its information open to attacks and breaches. This strategy aims to comprehend what transpired to permit such a significant data breach. The majority of NIST CSF control failures were caused by a lack of:

# least privilege,

# vulnerability management,

# security event monitoring, and

# security principles.

**SCOPE**

The question of data security is now frankly topical among SMEs and groups and professionals in the sector, hosting or online service providers, and software publishers in SaaS mode. At a time when data theft from Yahoo! (500 million hacked accounts) is made public – more than two years later (which makes it scandalous), it may be useful to recall certain legal rules.

Yahoo indeed makes sure that its customer’s data is kept protected by so many rules and policies that tried to apply over the years since the incident. They decided to give the users options about their accounts and how they want them protected. They decide how they want their data used and who should access it as well.

**Expected Result**

The project will provide a general overview of the concepts, practices, and strategies Yahoo's management must develop to prevent data breach occurrences and compliance problems. A set of technical controls can be implemented to encourage a corporation to use suitable security measures and abide by confidentiality regulations.

**Plan Framework**

Most people agree that the NIST Cybersecurity Framework is the complete collection of industry best practices and controls available. It is beneficial to select a framework that is frequently employed in the sector and offers mitigation guidelines for security issues. As a result, we are utilizing the Cybersecurity Framework, which was developed by the National Institute of Standards and Technology (NIST). There are five primary tasks of the NIST CSF, which are identification, protection, detection, response, and recovery. These encompass every aspect of cybersecurity, making the system's risk-based strategy for securing a business comprehensively.

Selecting an industry-standard, agnostic framework that offers a guideline for mitigating cyber threats is more effective due to the variety of breaches. It was decided to use the Framework from the National Institute of Standards and Technology (NIST Cybersecurity), version 1.1. To support this effort and the use of the NIST Cybersecurity Framework, regulatory considerations required under US governance instruments and best practices were investigated.

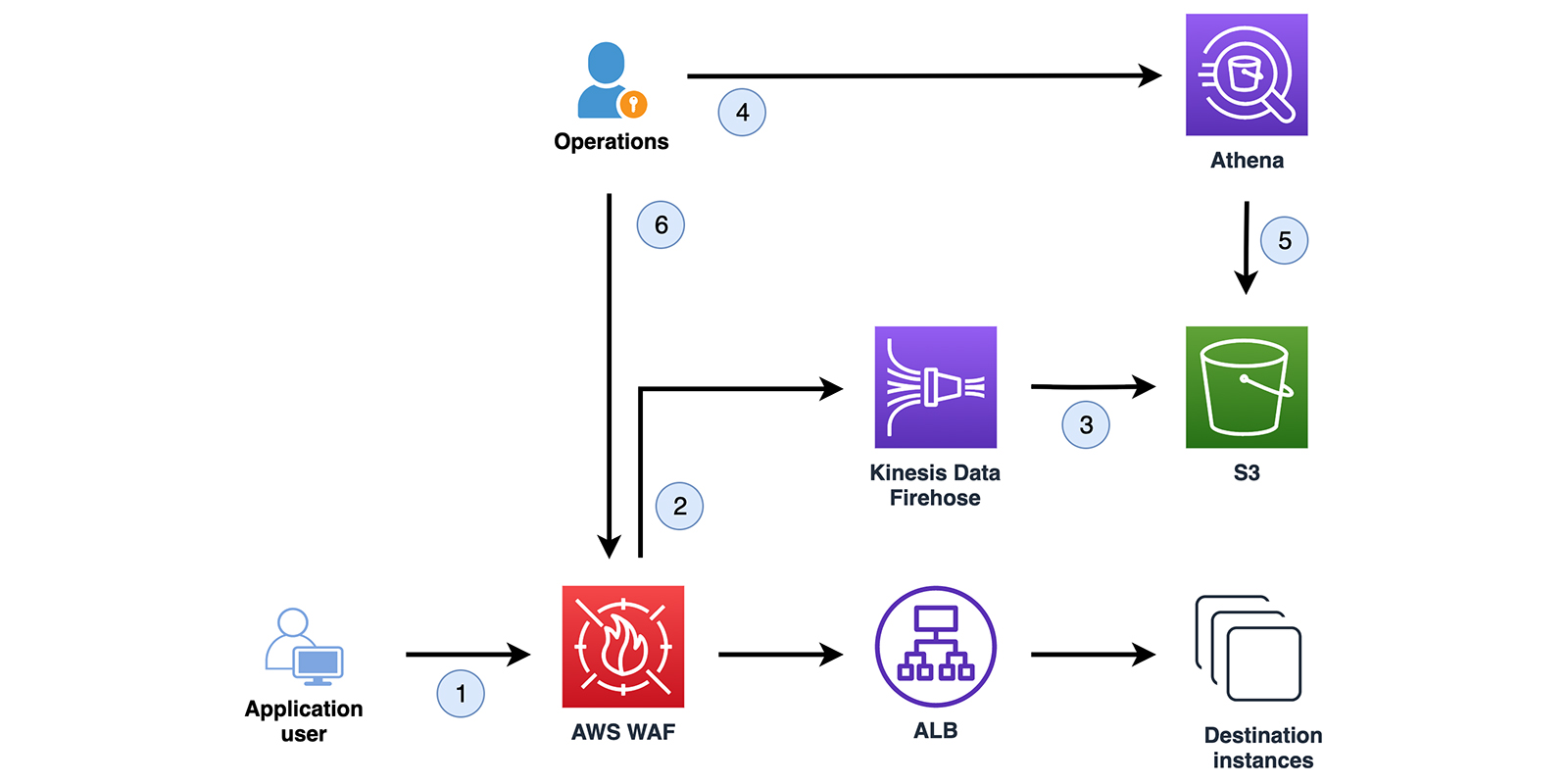
This project will use the NIST Cybersecurity Framework (CSF) to prevent and mitigate data breaches in Yahoo. The framework includes:

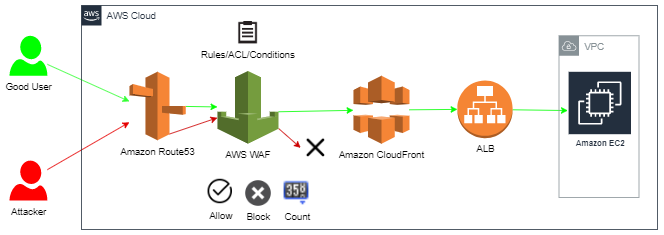
1. **IDENTIFY**: this function will help Yahoo know how to manage cybersecurity risk to systems, people, capabilities, data, and assets, as this is the foundation for the effective use of the framework. Using AWS as our cloud provider, there is a shared security responsibility. AWS offers risk information to enable Yahoo to incorporate controls in its NIST framework. The following category and subcategories have been identified as being critical to addressing Yahoo’s data breach.
   1. **Risk assessment**: the intent of this category is for Yahoo to understand the cybersecurity risk surrounding data breaches: organizational operations (including image, reputation, mission, or functions), individuals, and corporate assets.
      1. **ID.RA-3** Threats, both internal and external, are identified and documented:

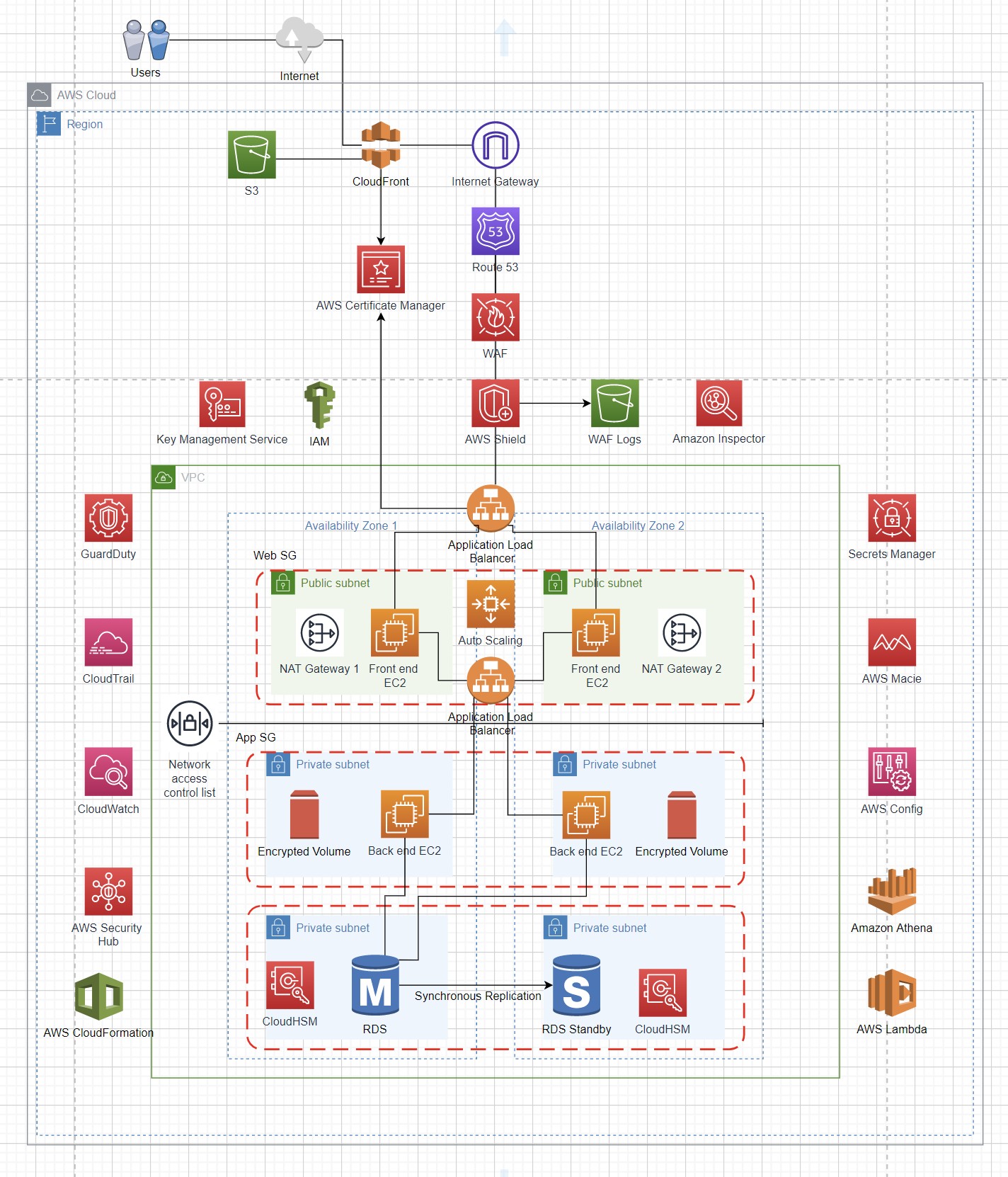
* Assess document, review, disseminates & update supply chain risks associated with data breaches.
* Utilize all source intelligence to assist in risk analysis.
* Determine the targeted/current data breach environment on an ongoing basis to enable Yahoo’s information security operations to be up to date with a response procedure.
* Employ advanced analytics capabilities and automation to predict and identify risks, e.g. Automated Threat Discovery and Response
  1. **Risk management strategy**: the intent of this category is for Yahoo to establish its organization’s constraints, assumptions, priorities, and risk tolerances used for supporting operational risk decisions.
     1. **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders:
        + Develops a robust strategy to address the identified data breach risks
        + Implements, reviews, and updates the developed strategy consistently across Yahoo.

1. **PROTECT**: this function will support Yahoo's ability to reduce or control the impact of a potential cybersecurity event and develop and implement the necessary protections to ensure the delivery of vital services. Using AWS as our cloud provider, there is a shared security responsibility. AWS offers Identity and Access Management (IAM) service that Yahoo can use to assign access roles, encryption services such as Amazon Elastic Block Store (EBS), key management service, and integrity checks with CloudWatch & CloudTrail. AWS also offers user identities, authentication standards, and access rights with services like Single Sign-On (SSO), Multi-Factor Authentication, Cognito, etc. The following category and subcategories have been identified as being critical to addressing Yahoo’s data breach.
   1. **Identity Management and Access Control**: the intent of this category is for Yahoo to limit access to associated facilities and physical & logical assets to authorized users, processes, and devices.
      1. **PR.AC-4:** Access permissions are managed, duties are separated, and the principles of least privilege are incorporated
         * Yahoo will develop and disseminate a policy document that addresses access control and identity management.
         * Define system authorization access to support the separation of duties
         * Employ the principle of least privilege, which authorizes access for users necessary to accomplish assigned organizational tasks.
         * Use multifactor authentication for access to privileged accounts
         * Automatically terminate a user session after a defined condition
   2. **Data Security**: the intent of this category is for Yahoo to protect the integrity, availability of information, and confidentiality of information and data.
      1. **PR.DS-1:** Data-at-rest is protected
         * Data at rest must be encrypted
         * Critical information is backed up properly
         * The network protocol must be secured
      2. **PR.DS-2:** Data-in-transit is protected
         * Implement and manage network devices to prevent hackers from exploiting vulnerable network services and access points.
         * Provide a trusted communication path for communications between systems and users
         * Communication channels must be secured and encrypted when migrating data.
         * Utilize cryptographic safeguards to avoid unwanted data disclosure while transmission is taking place
      3. **PR.DS-5:** Protections against data leaks are implemented
         * Data will be classified according to value, data, criticality, and sensitivity to Yahoo
         * Provide security awareness training to employees and third-party vendors on identifying data leaks like insider threat
         * Monitor Yahoo systems to indicate potential data leaks and detect attacks
         * Design and configure networks to restrict and monitor traffic between trusted and untrusted connections
2. **DETECT:** This function will assist Yahoo in creating and putting into practice the proper cybersecurity event detection procedures. The Detect Function makes cybersecurity events quickly discoverable.
   1. **Security Continuous Monitoring**: the intent of this category is monitoring assets and information system, identifying cybersecurity events, and verifying the effectiveness of protective measures.
      1. **DE.CM-1:** the network is monitored to detect potential cybersecurity events
         * Develop and implement a continuous monitoring strategy
         * Execution of vulnerability management plan.
         * Regular audits of the vulnerability management plan should be conducted.
         * Determine and record the different sorts of system modifications that are configuration-controlled.
         * The configuration of network environments and virtual instances must limit and track traffic between trustworthy and untrusted connections.
         * Include security in the development process and ensure that customers use security features.
         * Establish a relationship between the frequency of scanning and the amount of time needed for repair.
         * The vulnerability management plan needs to undergo routine audits.
         * To maximize opportunities, collaborate with other departments, including the data, security, and remediation teams.
         * Establish enterprise strategic goals for tracking the performance and health of the entire organization.
         * Participate in imperatives for vulnerability management with management and stakeholders.
3. **RESPONSE:** this function will help Yahoo develop and implement appropriate activities to act regarding a detected incident. Management buy-in and the existence of a documented incident response plan are essential. But having the right tools to help prepare for and respond to security incidents is not insignificant. Given the information they provide, the analyzes they perform, and the reports they can create, these tools should be implemented long before incidents occur.
   1. **Response Planning:** the intent of this category is for Yahoo to execute and maintain response procedures and processes to the detected cybersecurity incidents.
      1. **RS.RP-1:** Response planning is executed
         * Activity featuring ongoing learning and advancements to discover how to protect the organization's best
         * Having essential elements ready to be used, such as a Mission statement, documentation of roles and responsibilities, etc.
   2. **Analysis:** the intent of this category is for Yahoo to analyze the detected cybersecurity incident to ensure adequate response and support.
      1. **RS.AN-3:** Forensics are performed
         * Analysis of the response and support recovery activities.
         * Retains and engagement of an external forensics firm for incidents requiring forensic investigation
   3. **Mitigation:** the intent of this category is for Yahoo to prevent the escalation of the detected cybersecurity incident, mitigate the effects and provide resolution.
      1. **RS.MI-2:** Incidents are mitigated
         * Execution of the plan during or after the incident
         * Incidents are contained
         * Proper communication with stakeholders
4. **RECOVER:** this function will assist Yahoo in creating and carrying out the necessary procedures to maintain resilience plans and restore any capabilities or services damaged due to a cybersecurity incident. The three Framework Categories that will be useful for Yahoo according to the NIST are:
   1. **Communications:** the intent of this category is for Yahoo to coordinate restoration processes with internal and external stakeholders.
      1. **RC.CO-1:** Public relations are managed
         * Personnel knows their roles and order of operations when a response is needed.
         * The VP of marketing and communications manages official messages during incidents.
   2. **Recovery Planning:** the intent of this category is for Yahoo to execute and maintain response procedures and processes, so the systems and assets affected by the incidents are restored.
      1. **RC.RP-1:** A recovery plan is executed during or after an event
         * The CISO makes sure that the recovery plan is applied when an official response is called for.
         * Activity featuring ongoing learning and advancements to discover how to protect the organization best is set up.
   3. **Improvements:** the intent of this category is for Yahoo to improve its recovery procedures by incorporating the lessons learned.
      1. **RC.IM-1:** Recovery plans incorporate lessons learned
         * After an incident response, the CISO guides the incident response team through a meeting to discuss the lessons learned.
         * Lessons learned will be used to address better future security events.

**HIGH-LEVEL AWS ARCHITECTURE**







**CLOUD SERVICES**

For the Yahoo project, we would be securing our assets on the AWS cloud, which supports every pillar in the NIST Framework. As a leading provider in the cloud industry, AWS has the following services, which will be incorporated into the plan framework.

1. **IDENTIFY**:
   1. **AWS Identify and Access Management (IAM):** This service enables access roles for users and services based on business roles. To prioritize automated tasks, tags for services and data might contain predetermined risk assessments and stop-gates that let a human user examine the data and choose which course the system should take. Improving identification and access management was where we started (IAM). Organization-wide access to all systems, including the cloud, was provisioned and de-provisioned using federated authentication within a centralized system. We can use AWS Single Sign-On (AWS SSO), direct federation to IAM, or Active Directory integration to gain access to AWS.
2. **PROTECT**:
   1. **AWS Shield**: this is a managed Distributed Denial of Solution (DDoS) prevention service (AWS). Since AWS Shield offers always-on monitoring and automated inline mitigations that reduce application downtime and latency, there is no need to get in touch with AWS Support to take advantage of DDoS protection.
   2. **Amazon Macie**: this service is used to detect, categorize, label, and apply rules to data stored in Amazon S3.
   3. **AWS Key Management Service (KMS**): cryptographic keys are created, managed, and controlled using this service in your applications and several AWS services. The hardware security modules used by AWS KMS to safeguard your keys have either been certified under FIPS 140-2 or are in the process of being validated. You can obtain logs of all key usage from AWS KMS and CloudTrail to meet regulatory and compliance obligations.
   4. **AWS Certificate Manager**: this is a service that makes it simple to produce, manage, and deploy public and private SSL/TLS certificates. SSL/TLS certificates encrypt network traffic, validate the legitimacy of private network resources, and authenticate websites on the Internet.
   5. **AWS Secrets Manager**: this is a service that safeguards the secrets required to access applications, services, and IT resources. The service enables simple rotation, administration, and retrieval of database credentials, API keys, and other secrets across their entire lifetime. By using the Secrets Manager APIs, users and programs can retrieve secrets without having to hardcode sensitive data in plain text.
3. **DETECT**: to gather the data required to react to unforeseen changes or incidents; we used the detect controls. Security intelligence and event monitoring systems like **CloudWatch** are coupled with tools like **Amazon GuardDuty** and **AWS Config**, enabling the response to issues with both manual and automatic remediations. When a security incident is discovered, it's critical to act promptly and appropriately to reduce the damage to your company. A robust incident response process combines automated processes with human involvement steps. The automated response and remediation solutions offered by **AWS Security Hub** give a general overview of the incident response automation development process. Custom certificates and alternative domain names are only a couple of the extra capabilities offered by the secure and dependable. **AWS Inspector** is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It reveals technical errors that can inform risk stances and management methods.
4. **RESPONSE**: the security posture is strengthened by collecting and analyzing log data, allowing quicker detection and investigation of potential attacks. It might be challenging to manually process enormous amounts of data and derive insights from them. AWS services like **AWS Systems Manager**, **Amazon CloudWatch**, **Amazon Simple Storage Service (S3)**, **Amazon Athena**, and **Amazon Quick Sight** can all be used securely to gather and store logs without requiring direct access to instances or data. In this manner, you can react to dangers and implement the necessary safeguards. Additionally, **Amazon Detective** can be used to identify and resolve any potential security problems. It develops an interactive website using statistical analysis.
5. **RECOVER**: an architecture with several availability zones and autoscaling may result in the replacement of unhealthy instances with fresh or backup resources. It is possible to automate recovery in a disaster using **AWS Lambda** and **CloudFormation**. Long-term data protection and the creation of new EBS volumes are both possible with **EBS** snapshots. The crucial data backup will be created using it. You can utilize **Amazon RDS** standby for automatic failover with no data loss and no need for human intervention. The S3 bucket's versioning feature could be enabled as an additional recovery option. Data would be shielded from the effects of updating or deleting. We can retrieve the data and return it to the required version.

**CONCLUSION**

In summary, every organization needs to develop and implement the NIST Cybersecurity framework, as it provides the foundation for a highly secured system. AWS is a leading cloud provider that offers several services and controls which will enable Yahoo to execute the identify, protect, detect, response, and recover functions in the NIST framework.

**REFERENCES**

* Cloud Security, Identity, and Compliance Products – Amazon Web Services (AWS). (n.d.). Retrieved from Amazon Web Services, Inc. website: <https://aws.amazon.com/products/security/?nc=sn&loc=2>
* *NIST Cybersecurity Framework (CSF) Aligning to the NIST CSF in the AWS Cloud*. (2019). Retrieved from <https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf>
* NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity*, *1.1*(1.1). <https://doi.org/10.6028/nist.cswp.04162018>
* RA-3 RISK ASSESSMENT | NIST Controls and PCF. (n.d.-b). Retrieved from docs.pivotal.io website: <https://docs.pivotal.io/nist/ra/ra-3.html>
* NIST. (2020b). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, *5*. <https://doi.org/10.6028/nist.sp.800-53r5>
* PM-9: Risk Management Strategy - CSF Tools. (2020b, August 13). Retrieved from csf.tools website: <https://csf.tools/reference/nist-sp-800-53/r4/pm/pm-9/>
* PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties - CSF Tools. (2020b, August 13). Retrieved from csf.tools website: <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ac/pr-ac-4/>
* PR.DS-1: Data-at-rest is protected - CSF Tools. (2020b, August 13). Retrieved from csf.tools website: <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ds/pr-ds-1/>
* PR.DS-2: Data-in-transit is protected - CSF Tools. (2020b, August 13). Retrieved from csf.tools website: <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ds/pr-ds-2/>
* PR.DS-5: Protections against data leaks are implemented - CSF Tools. (2020b, August 13). Retrieved from csf.tools website: <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ds/pr-ds-5/>
* nicole.keller@nist.gov. (2018, February 1). Recover. Retrieved from NIST website: <https://www.nist.gov/cyberframework/recover>
* nicole.keller@nist.gov. (2018b, February 1). Respond. Retrieved from NIST website: <https://www.nist.gov/cyberframework/respond>