**Security Introduction**

**Cybersecurity** is concerned with protecting networks/devices/systems/digital information from Unauthorized Access, Malicious Modification/Theft/Destruction and Disruption of Intended use.

* Confidentiality: Is the data protected to prevent unauthorized access?
* Integrity: Are measures in place to ensure data hasn’t been modified & that it’s correct/authentic?
* Availability: Can Users access the data when they need?

**Attackers** are people with malicious intent to compromise a system.

**Vulnerability** is weakness/s in the system the attacker exploits.

**Threats** are events that potentially negatively impact a system.

**Breaches** are attacks that compromise a system.

|  |  |  |
| --- | --- | --- |
| **Threat Type** | **Description** | **CIA Attribute** |
| **Malware** | Malicious Software which Disrupts System Operations to Gain Access/Data to it. i.e. – *Spyware, virus* | Confidentiality (*spyware*)  Integrity (*virus*)  Availability (*virus/worm*) |
| **Ransomware** | Malicious Code Restricting Computers Access to Data until Ransom Paid. | Availability. |
| **Denial of Service (DoS)** | Attack Preventing Users from System Access. | Availability |
| **Man-in-the-Middle (MitM)** | Intercepting Communication between 2 Parties & Impersonates/Modifies Communication, | Confidentiality  Integrity |
| **Phishing** | Masquerades as Legitimate Person/Business using Emails/Websites to get Personal Info. | Confidentiality |
| **Social Engineering** | Human Interaction Manipulates someone into Revealing Sensitive Info/Break Security Procedure for System Access/Information. | Confidentiality |

**Security Controls** are mechanisms to reduce/eliminate a vulnerability.

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Type** | **i.e. - Physical** | **i.e. - Administrative** | **i.e. – Technical** |
| Preventative | Card-Readers for Building Access. | Employees Policy to Swipe Cards. | Collect Data from Card Readers. |
| Detective | Airport Metal Detectors. | Report when System Changed. | Antivirus Regularly Runs Scans. |
| Corrective | Back-Up Generator for Blackout. | Continuity Plan to Continue Ops during a Blackout | Antivirus Removes Malware when detected. |

**Security Lifecycle Prevention Introduction**

The Key Steps of the Security Lifecycle are Prevention, Detection, Response and Analysis.

|  |  |
| --- | --- |
| **Prevention Tasks** (*AWS System Manager Inventory*) | * Identifying Assets (*Network Devices/Servers/Apps/Services*) and how they’re Protected (*Network/Host/App/Data Assessments*). *Nmap, Arp, ping*. * Assessing Asset Vulnerability. * Implementing Countermeasures (*Network/System Hardening, Data Controls, Identity Management, etc*). * Aided by the [Common Vulnerabilities/Exposures Website](https://cve.mitre.org/). |
| **Prevention Strategy** | Different Levels of Défense (*Perimeter, Network, Endpoint, Application, Data*). |
| **Prevention Measures** | * Network Discovery Hardening (*Close Unused Ports, Block Network Explore Protocols, Up-to-date Asset Inventory of Authorised Users*). * Network Security Architecture (*Firewalls, Intrusion Prevention System, Network Segmentation*) * Host-Level Controls (*Regular OS Updates/Patches, Remove Unused Apps, Monitor/Control Config Changes*) * Data Security Controls (*Encrypt Data in-Transit/rest, Digital Certificates, Data Integrity Checking Tools, Role-Based Access Control*) * Identity Management (*Principle of Least Privilege, Password Strength Policy, Authentication/Authorization/Accounting Principles*). |

**Security Lifecycle Prevention: Network Hardening**

**Network Hardening** works within the Layered Security Prevention Strategy to Protect the Network and is achieved through *Network Discovery and Architecture Security Hardening*.

**Network Security Threats** are attempts to Expose/Alter/Disable/Gain Unauthorized Access to Steal Data/Perform Malicious Activity. They Discover Network Information & Exploit Weaknesses.

|  |  |
| --- | --- |
| **Network Security Threat Types** | |
| Network Mapping | Exposes Network Topology (Devices/Hosts present) through *ping/traceroute/nmap* |
| Port Scanning | Exposes Protocols & Services through *nmap* |
| Traffic Sniffing | Exposes Information Travelling within Network & Read Unencrypted Data with *Wireshark (Show Packet Size/Source/Destination. MAC address & Protocol)*. |

**Network Discovery Hardening** keeps Attackers off the Network with the help of the Amazon Inspector through the following means:

|  |  |
| --- | --- |
| *Restricting Protocols (ICMP/SNP).* | *Disabling NICs Promiscuous Mode.* |
| *Use Switches not Hubs.* | *Encrypt Sensitive Data on Transit.* |
| *Record Traffic Entering Network.* | *Watch for Unknown IP Addresses* |
| *Monitor for Sequentially-Scanned Ports.* | *Limit Remote Administration Protocols.* |
| *Limit Possible Remote Administration Locations.* | *AAA Policy to Limit Network Device Access.* |

**Network Architecture Hardening** increases network security through Design Improvements.

|  |  |
| --- | --- |
| *Add Network Firewalls* | *Intrusion Prevention Systems.* |
| *Create Private Subnets.* | *Use Network Access Control Lists.* |

**Network Firewalls** work as Protection Mechanisms to Filter Incoming/Outgoing Traffic, capable of being a Hardware/Software Device. Only allows certain packets/users.

* Deny all traffic, then permit only needed traffic.
* Block Network Control Device Traffic unless it’s from a Trusted Network.
* Place the Firewall as close to the Traffic Source as Possible.
* Use Firewalls to Create Network Zones with differing Levels of Security

|  |  |
| --- | --- |
| **Network Zones & Security Levels** | |
| **Internet** | Uncontrolled & Unsecure Area |
| **Perimeter** | Partially-Controlled & Secured by 1 Firewall, Serves as Buffer between two zones with differing Trust Levels. |
| **Internal/Intranet** | Fully Controlled secured by 2 Firewalls. |

**Security Groups** used within AWS function like Built-In Firewalls for Instances & are associated with Network Interfaces. They’re stateful and Define Allow Rules (Inbound/Outbound Traffic Rules) that Determine Instance Access.

The **Network Access Control List (ACL)** acts like a firewall within the AWS Cloud to protect a subnet, it’s stateless and typically implemented on switch/router to control Inbound/Outbound Traffic.

*Network ACLs protect the Subnet Level, Security Groups protect the Instance Level.*

The **Intrusion Prevention System (IPS)** is software/hardware actively Protects a Network against threats using different types of Threat Detection Methods (*Anomaly/Signature-based Detection*). It’s usually placed behind a network terminal.

* Anomaly-Based Detection: Comparing Current Traffic Patterns against Established Baselines for deviation.
* Signature-Based Detection: Monitoring/Analysing Traffic for Known Attack Patterns.

**Subnets** are Network Segmentation which applies differing security controls to different parts of a network, creating smaller logical networks, each with a contiguous subset of the larger network’s IP address

* Classless Inter-Domain Routing (CIDR) Notation is used to specify subnet IP address ranges, it’s shorthand for describing network size.

**Security Lifecycle Prevention: System Hardening**

**System Hardening** is securing computing systems to prevent attacks. *Comprehensive solutions to this issue should cover the following facets:*

|  |  |  |
| --- | --- | --- |
| *Remove Unused Apps* | *Suspend Rarely-Used Apps* | *Run Updates/Patches* |
| *Monitor Systems - AWS SSM* | *Protect Server Access* | *Prevent Config File Changes* |
| *Prevent Unapproved Apps* | *Turn on Antivirus/Firewalls* | *Secure File Systems* |
| *Using Alerts* | *Controlling Downloads* | *Limit Admin Access* |
| *Use Dedicated Roles* | *Restrict Physical Access* | *Limit Removable Media* |

|  |  |
| --- | --- |
| **Authentication** | Validates you are who you claim to be. |
| **Authorization** | Verifies you have permission to access the resource. |
| **Accounting** | Gathers usage & other information for auditing/billing. |

**Security Baselines** define the expected system conditions, providing a starting point for determining what/how to secure and regularly updates to reflect system changes including enhancements.

**Application Hardening** involves updating/implementing security measures to protect standard/third-party apps installed on your server

|  |  |
| --- | --- |
| **Application Hardening Examples** | |
| Patch Standard/3rd Party Apps Automatically | Software-Based Data Encryption |
| Application Firewalls | CPUs with Intel Software Guard Extensions |
| Antivirus/Malware/Spyware Protection Apps | Specific Apps Manage/Encrypt Passwords |

|  |  |
| --- | --- |
| **AWS Security Tools** | |
| **AWS Trusted Advisor** | Provides Recommendations for following AWS best practices, evaluating accounts with checks. |
| **Amazon Guard Duty** | Threat Detection Service continuously monitoring AWS accounts/workloads for malicious activity & reporting back. |
| **AWS Shield** | DDoS Protection Service that Safeguards Applications on AWS. |
| **AWS CloudTrail** | Auditing/Security-Monitoring/Operations Troubleshooting by tracking User Activity and API Usage. |

I'm interested in the DevSpecOps Role as I'm currently working towards my AWS Solutions Architect Certificate, however during this training I'm also learning quite alot of Devops which has me interested in this role.

What I lack in experience I can more than make up for in enthusiasm and work ethic, and would greatly appreciate you giving a recently-graduated retraining student a chance within your company.

**Security Lifecycle Prevention: Data Security**

**Cryptography** is a discipline which provides data security, confidentiality and data integrity.

**Encryption** is the process of using a Code (Cipher) to render data unreadable for another party. It contains algorithms to encrypt & decrypt data.

The **Key** is a series of numbers/letters the algorithm uses to encrypt/decrypt data reserved for the key owners. AWS Cloud HSM can generate/use keys on the AWS Cloud, and you create/manage cryptographic keys over a range of services with AWS Key Management Service (AWS KMS)

**Data Integrity** ensures data remains accurate/consistent when used/travelling across a network and is determined using a **Hash Mechanism** (*one-way encryption creating a file signature*).

**Hashing** pertains to one-way encryption by generating a unique hash value/message digest from file contents. Recipients use the hash value to verify data hasn’t changed during transit.

|  |  |
| --- | --- |
| **Data at Rest Encryption** | |
| File System Encryption | Windows New Technology File System (NFTS) can encrypt several files. |
| Drive Encryption | Encrypt an Entire Drive using BitLocker/VeraCrypt. |
| **Data in Motion Encryption** | |
| SSL/TLS | Secures Data travelling across the wire (https). |
| Kerberos | Encrypts Communications between Two Devices. |
| IP Security (IPsec) | Integral Component of IPv6 and used with IPv4 for Logical Connection between Devices by providing identification for each securing a VPN. |
| IM/Secure Email | Secures Messages Sent using Secure/Multipurpose Internet Mail Extensions (S/*MIME*) and Pretty Good Privacy (*PGP*) |

|  |  |
| --- | --- |
| **Types of Encryptions** | |
| **Symmetric** | Uses the same key to encrypt/decrypt data shared between sender/receiver. *AES, IDEA, Two Fish, TLS & SSL* |
| **Asymmetric** | Uses Private & Public key pair to encrypt/decrypt data, much more complex & slower than symmetric but has more key management capabilities. *RSA, DH, ElGamal, TLS, SSL, SSH.* |
| **Hybrid** | Uses both symmetric & asymmetric encryption on either sides. *TLS, SSL* |

**Permissions** are used to allow subjects explicit resource access to objects, there are two types:

* Discretionary: Based on Identity, aided by the AWS Identity and Access Management. *Decentralized Access, ACLs, ACEs, Auditing, Dynamic Access Control.*
* Role-Based: Based on Assigned Role. *Efficient with high numbers, customizable, mostly used in commercial sector.*

**Security Lifecycle Prevention: Public Key Infrastructure**

**Public Key Infrastructure (PKI)** is a collection of technologies used to apply cryptography principles based on the practical implementation of keys. They provide *confidentiality, integrity, nonrepudiation, authenticity and management of trust/relationships.*

**Trust** is achieved through exchanging public keys, verifying each part and preventing rogue systems from interfering.

**Public Keys** are possessed by the sender & receiver, ensuring trust throughout the entire hierarchy.

**Certificate Authorities (CAs)** issue certificates to entities ensuring website security.

* A diagram of a computer

  Description automatically generatedRoot CAs are the hierarchal peak, initializing it, storing root CA keys, kept isolated & offline.
* Subordinate CAs are registration authorities that verify/validate entity requests, issuing certificates.
* Certificate Practices Statement (CPS) defines practices, standards and algorithms the Cas use.
* Certificate Policy defines rules CA customers must follow

|  |  |  |
| --- | --- | --- |
| **Characteristics** | **Internal CA** | **External CA** |
| **Configuration** | Organization/Company | 3rd Party |
| **Trust Level** | Only within Org/Company | Every Entity |
| **Admin Effort** | More Effort | Less Effort |
| **Additional Info** | Free Cost | No Direct Access Granted |

AWS Cloud provides an Internal CA in the form of the AWS Certificate Manager (ACM), you no longer manually purchase/upload and renew SSL/TL.S certificates.

* Protect/Secure Websites & Internal Resources
* Help Meet Compliance Requirements.
* Improve Uptime.

**Obtaining a Digital Certificate** for an External CA, you must submit a Certificate Signing Request (CSR), The process works as follows:

1. Use Open-Source/Vendor-Specific Tools to create a CSR.
2. Create CSR File on Server, Providing Details about Organization.
3. Send CSR File to the CA.
4. Receive Digital Certificate from CA.
5. Install Certificate on Server

A certificate with text and a ribbon

Description automatically generated The **Certificate Revocation List (CRL)** is a document maintained by the Issuing Certificate Authority which holds expired and revoked certificates.

* Must be accessible, especially for Internal CAs.
* Requires Large Administrative Efforts for Multiple CRLs.
* Online Certificate Status Protocol (OCSP) for Enterprise Environment.

**Security Lifecycle Prevention: Identity Management**

**Identity Management** is the active administration of subjects, objects & their relationship regarding accessing permissions, ensuring identities receive appropriate accesses and that systems remain scalable in access-granting.

**Identification/Authentication/Authorization/Accounting (IAAA) Principles** are primarily used as common security steps enforced on user login.

* Identification: Something user must prove.
* Authentication: Something that can be verified/validated. *Multi-factor Authentication*.
* Authorization: Specific access according to role/level.
* Accounting: Way to track users with a log.

|  |  |  |
| --- | --- | --- |
| **Authentication Factors** | | |
| *Smart Card* | *Certificate* | *Token* |
| *USB Key* | *Key* | *Virtual Card* |
| *Transaction Authorization No.* | *Smart Phone* | *Two-Factor Authentication* |
| *Fingerprint Reader* | *Hand Geometry* | *Retina Scanner* |
| *Facial Recognition* | *Iris Recognition* | *Signature Analysis* |

There’s also **Personally Identifiable Information (PII)** which is information such as *passport number, name, date of birth etc.*

**Password Policies** define rules for how passwords are created/maintained *i.e. – At least one capital letter and special character, to prevent Dictionary Attacks.*

**Password Managers** operate over a Centralized Authentication System requiring extra login steps, password resets and manages services used with specific credentials. *Stores on a Local System*.

**Single Sign-On** synchronises passwords between two independent systems which aren’t in a trust relationship & belong to different directory structures.

**Federated Users** are forms of SSO where one account is used and verified by multiple services.

**AWS SSO** is a Cloud-Based Service used to centrally manage SSO Access to all AWS accounts, user permissions & AWS Organizations.

* One-click access to AWS Accounts & Cloud Applications.
* Create/Manage Users/Groups.
* Compatible with Common Cloud Applications.
* Compatible with existing AWS IAM roles, users & policies.

**Amazon Cognito** provides User Management, Authentication and Authorization for Web/Mobile Apps, containing the following:

* User Pools providing sing-up/in options for users.
* Identity Pools granting access to AWS Services.

*AWS IAM is primarily concerned with authentication, authorization and ensuring the services required are available*

**AWS Identity and Access Management (IAM)**

**AWS IAM** centrally manages authentication & access to AWS resources, creates users/roles/groups and applies policies to control entities access to AWS resources. *Uses Authentication & Authorization.*

* IAM Users are entities representing persons/apps created within AWS providing a way to interact with it, they have no default security credentials.
* IAM Groups are collections of users without any default group. They can’t be nested but users can belong to multiple groups and specify permissions for an entire group defined with IAM policies.
* IAM Roles are used to delegate access to AWS resources providing temporary access with permissions defined using IAM policies and attached to the role instead of a user/group.
* IAM Permissions are checked if allowed through looking for explicit deny/allow policies, reverting to the implicit deny if neither exist.
* IAM Policy is a formal statement for one/more permissions, attached to one or more entities authorizing actions it performs. *A single entity can have multiple policies.*

*A screenshot of a computer

Description automatically generated*

|  |  |
| --- | --- |
| **IAM Features** | |
| **IAM user** | Entity in AWS to represent person/app interacting with resources. |
| **IAM Account Root User** | Entity with complete access to all AWS Services. |
| **Identity Federation** | Trust System which authenticates users & conveys info to authorize their resource access. |

|  |  |
| --- | --- |
| **Security Credentials** | |
| **Email & Password** | Associated with AWS (root) account. |
| **IAM Username & Password** | Access AWS Management Console. |
| **Access/Secret Access Keys** | AWS CLI & Programmatic requests i.e. – *APIs/SDKs* |
| **Multi-Factor Authentication** | Provides Extra Security Layer, enabled for Root & IAM Users. |
| **Key Pairs** | Specific AWS Services only, such as EC2. |

**Security Lifecycle Detection**

**Malware** is designed to harm computer systems through interrupting a CIA (Confidentiality /Integrity / Availability) element. *Worms, Viruses, Bots, Backdoors, Rootkits, Spyware, Adware, Ransomware through emails, untrusted websites & removable media.*

**Antivirus Software** is specialized in preventing/detecting/removing Malware, built into the OS/3rd Party using malware signature definitions to scan memory for matches & remove it.

**Intrusion Detection System (IDS)** is hardware/software which detects security threats & generates alerts using two different types of threat detection mechanisms.

* Anomaly-Based Detection: Compares current traffic pattern/system activity to established baseline for any deviations.
* Signature-Based Detection: Monitors/Analyses traffic for known attack patterns.
* **Network-Based IDS** monitors network traffic, detects threats and raises alerts installed on the network.
* **Host-Based IDS** monitors logs/critical files on the server, detects threats & raises alerts installed on the server.

**Amazon GuardDuty Detection Mechanism**

1. Activate GuardDuty monitoring all AWS Accounts.
2. Continuously analyses AWS workloads/resources for potential threats using machine learning, anomaly detection & integrated threat intelligence
3. Reviews findings, integrating into event management/workflow systems initiating AWS Lambda for automated remediation/prevention.

**AWS CloudTrail**

**CloudTrail** provides auditing, security monitoring and operational troubleshooting for AWS. It delivers log files to user-specified S3 Buckets.

|  |  |
| --- | --- |
| *Monitor User/Resource Activity.* | *Simplified Compliance.* |
| *Always On.* | *Security Automation.* |
| *Analysis & Troubleshooting.* |  |

|  |  |
| --- | --- |
| **Best Practices** | |
| *Turn of CloudTrail Log File Integrity Validation.* | *Aggregate Log Files to Single S3 Bucket.* |
| *Ensure CloudTrail enables globally across AWS.* | *Restrict CloudTrail S3 Bucket Access.* |
| *Integrate with CloudWatch* |  |

**To Find your Log Files:**

1. Open Amazon S3 Console.
2. Choose Bucket specified during creation.
3. Navigate through Object Hierarchy until you find it.

**AWS CONFIG**

**AWS Config** is used for assessing/auditing/evaluating AWS Resources, providing resource inventory, configuration history and change notifications, evaluating changes against user-defined security prevention & compliance rules.

|  |  |
| --- | --- |
| *Compliance Auditing* | *Security Analysis* |
| *Resource Change Tracking* | *Troubleshooting* |
| *Discover New/Deleted Resources* | *Record Config Changes Constantly* |

**How AWS Config works:**

1. AWS Config records, normalizes & stores changes to S3 bucket.
2. Automatically evaluates changes against user-defined AWS Configuration Rules.
3. Sends Configuration & Rule Compliance Change Notification to Amazon SNS Topic.
4. Users receive Notification through SNS Alerts.

**Security Lifecycle Response**

**Event Responses** cover questions asked in case of a damaging event.

The **Business Continuity Plan** lists several disaster scenarios & actions to keep the business running (not activated during outage).

The **Disaster Recovery Plan** strategizes business recovery from disaster/unplanned incidents, and features the following parts:

* Primary Goal: Restore Functionality Quickly & with Minimum Impact.
* Security Goal: Don’t lower Control Level/Safeguards in place.
* Follow-on Goal: Threat/Exploit/Disaster Prevention.

|  |  |
| --- | --- |
| **Disaster Recovery Plan Key Parameters** | |
| **Recovery Time Objective (RTO)** | Maximum acceptable days between service interruption & restoration. |
| **Recovery Point Objective (RPO)** | Maximum acceptable time since last data recovery point, showing how much data lost/retrieved. |
| **Work Recovery Time (WRT)** | Recovering/Restoring Data, Testing Processes, Making Systems Live for Production. |
| **Maximum Tolerable Downtime (MTD)** | Total time system can be disrupted after disaster without caused unacceptable consequences from break in business continuity. *MTD = RTO + WRT.* |

There are various **Disaster Recovery Options** including *Backup, Replication (Snapshot/Continuous) or Pilot Light.*

A graph of recovery options

Description automatically generatedThe **Event Investigation Process** works through the following stages:

1. Event Occurs.
2. Investigate Event.
3. Respond & Remediate.
4. Notify Dependent Stakeholders.
5. Act to Prevent Event Reoccurrence.

**Security Lifecycle Analysis**

**Types of Security Tests include**

External Vulnerability Assessment: System vulnerabilities evaluated with little knowledge of infrastructure/components by 3rd party.

External Penetration Test: 3rd party with little system knowledge actively tries to break into it in controlled manner.

Internal Performance/App Review: Tester with some/full system knowledge validates effectiveness of controls in place, applications and platforms.

**Root Cause Analysis (RCA)** is used to identify security breach origins through the following steps:

1. Describe the issue that happened & what led to it.
2. Return to baseline situation & evaluate each event leading up to the issue.
3. Analyse events & understand link between them, identifying which most likely caused the issue (*event correlation*).
4. Create visual representation of the sequence of events from origin to final problem.

**Risk Assessment** assesses and ranks the likelihood of a threat occurring against a particular asset & the impact that’d have through the following five steps:

|  |  |
| --- | --- |
| **Risk Response Strategies** | |
| **Risk Avoidance** | Stop Doing Risky Activity. |
| **Risk Transference** | Assign Risk Responsibility to another party. |
| **Risk Mitigation** | Implement Control to reduce risk. |
| **Risk Acceptance** | Do nothing to reduce risk, monitor and plan response. |

1. Identify Threats.
2. Identify Vulnerabilities.
3. Determine Likelihood.
4. Determine Impact.
5. Determine Risk.

**Monitoring & Logging** are tools that help security analysis through providing data used to identify/resolve security problems and includes the following benefits:

*Logs provide data both in forms of input & output which are monitored for changes/exceptions/other significant events, records produced are logs for further analysis.*

|  |  |  |
| --- | --- | --- |
| *More effective IT governance* | *Regulatory Compliance* | *SLA Performance Validation & Compliance* |
| *Better Management Oversight* | *More Effective Change Control* | *Support Corporate Information Security* |
| *More Consistent Problem Identification & Resolution* |  |  |

|  |  |
| --- | --- |
| **Monitoring Types** | |
| **Location** | Onsite, Remote, Internal/External, Outsourced. |
| **Resource** | System, Network, Database, Physical, Employee. |
| **Usage** | Usage/Consumption, Location, Access restrictions. |

**Metrics** measure security program success, capable of being both positive and negative i.e. – *Attack No. stopped, IDs created/revoked, money saved, etc.*

**Acceptable Use Policy (AUP)** defines how employees/users are monitored on a company’s network i.e. – *at work, remotely, on mobile devices.*

|  |  |
| --- | --- |
| **AWS Monitoring Services** | |
| **Amazon CloudWatch** | Monitors Resources & Apps in AWS Cloud/On-Premises. |
| **AWS Config** | Records & Evaluates AWS Configurations. |
| **Amazon Managed Service for Prometheus** | Provides Highly Available, Secure & Managed Container Monitoring. |
| **Amazon GuardDuty** | Protects AWS Accounts with Intelligent Threat Detection. |
| **Amazon Macie** | Fully-Managed Data Security/Privacy Service using Machine Learning & Pattern Matching to find/protect sensitive AWS data. |
| **AWS Logging Services** | |
| **AWS CloudTrail** | Tracks User Activity & API usage. |
| **AWS Config** | Records/Evaluates AWS Configuration Resources. |
| **Amazon VPC** | Flow Logs Capture Information about IP Traffic. |

**Monitoring as a Service (MaaS)** includes Amazon CloudWatch, its entire infrastructure is deployed in the cloud providing anytime/anywhere access to monitoring information i.e. – *Routers/Switches/Firewalls/Printers/Cameras etc.*

**Logging Policy** is defined to identify what/how will be logged/managed, ensuring both logging policy & infrastructure support cohesive/integrated enterprise solution.

**AWS Trusted Advisor**

**Trusted Advisor** provides best practices/checks in the following five categories.

|  |  |
| --- | --- |
| **Cost Optimization** | Save money with AWS through reducing unused/idle resources or making commitments to reserved capacity. |
| **Performance** | Improved through checking Service Limits, ensuring you take advantage of provisioned throughput & monitoring for overutilized instances. |
| **Security** | Improved through closing gaps, activating different AWS Security Features & Examining Permissions. |
| **Fault Tolerance** | Increase Availability/Redundancy through Automatic Scaling, Health Checks, Multiple Availability Zones & Back-up Capacities. |
| **Service Limits** | Check Service Usage which is > 80% of Service Limit. |

*Trusted Advisor Provides Checks for the following services:*

|  |  |
| --- | --- |
| **AWS IAM** | Checks for Existence of at least one IAM user, discourages root access use. |
| **MFA on root** | Checks Root Account & warns if MFA not activated. |
| **Security Groups** | Specific Ports Unrestricted, checks rules allowed unrestricted access to certain ports. |
| **Amazon S3 Bucket Permissions** | Checks buckets with open access permissions/that allow access to any authenticated AWS user. |
| **Amazon EBS Public Snapshots** | Checks perm setting for EBS Volume Snapshots & alerts if any public. |
| **Amazon RDS Public Snapshots** | Check perm settings for RDS database snapshots & alerts if any public. |

**Security Best Practices**

*While the AWS is responsible for security of the cloud & services, you’re responsible for the security IN the cloud.* The tasks listed below require signing in with AWS Root User Credentials:

|  |  |  |
| --- | --- | --- |
| *Change Account Settings* | *Restore AWS IAM User Perms* | *Change/Cancel AWS Support Plan* |
| *Activate IAM Access* | *View Certain Tax Invoices* | *Close AWS Account* |
| *Register as Seller* | *Configure S3 Bucket* | *Edit/Delete S3 Bucket* |

**Best Practices are as follows:**

1. Stop using AWS Account Root User as soon as possible.
2. Require MFA for all AWS Account Users.
3. Activate AWS CloudTrail as soon as possible.
4. Activate Billing Report i.e. – *AWS Cost & Usage Report.*

**AWS Compliance Program**

**Security Compliance** ensures Security Controls meet regulatory/contractual requirements. Both of the following two goals create company policies to support/enforce regulatory compliance

* **Regulations** often mandate security controls & vary between differing localities/jurisdictions/cultures.
* **Companies** include examples such as *SLA & PLA.*

**External Authorities** can be Governments/Laws (Mandatory), Open Standards (Recommended) and Best Practices (Optional).

**Payment Card Industry Data Security Standard**is an International Regulated Requirement Set which maintains a secure environment for payment card transactions.

**Health Insurance Portability & Accountability Act of 1996 (HIPPAA)** modernizes handling of healthcare info & stipulates how its protected addressing limitations on insurance coverage (consists of 5 tiles).

**General Data Protection Regulation (GDPR)** is regulations set created to provide EU citizens enhanced control over personal/private data.

**Personal Information Protection & Electronic Documents Act (PIPEDA)** is the Canadian federal privacy law regulating the private sector’s’ collect/usage and disclosure of clients personal info.

**Russian Federal Law on Personal Data** states the individual must provide consent, can revoke said consent and the transfer of personal data outside the Russian fed requires good enough protection in destined location.

***The United States Includes the Following Compliance Requirements:***

* Dodd-Frank Wall Street Reform & Consumer Protection Act
* Gramm-Leach-Bliley Act (GLBA)
* Family Educational Rights & Privacy Act (FERPA)
* Federal Information Security Management Act (FISMA)
* Financial Industry Regulatory Authority (FINRA)
* Sarbanes Oxley Act (SOX)

**The AWS Risk & Compliance program** provides info about AWS Controls assisting customers in documenting their security compliance framework, and consists of the following three components:

|  |  |
| --- | --- |
| **AWS Business Risk Management** | Concerns monitoring of key AWS functional areas. |
| **AWS Control Environment & Automation** | Concerns integrating security & compliance reqs during design/development of each AWS Service. |
| **AWS Certification & Attestations** | Concerns regularly undergone independent 3rd party attestation audits providing assurance control activities operate as intended. |

**AWS Customers** are responsible for maintaining adequate governance over entire IT control environment through the following means:

1. Understand their required compliance objectives/requirements.
2. Establish control environment which meets objectives/requirements.
3. Understand validation required based on organizations risk tolerance.
4. Verify operating effectiveness of control environment.

**AWS Security Resources**

**AWS Account Teams** serve as the first point of contact guiding your deployment. They point you towards the right resources to resolve security issues.

Support plans are available with the following tiers:

|  |  |
| --- | --- |
| **Support Plan Tiers** | |
| **Basic Support Plan** | *Customer Service, Communities, Trusted Advisor & Persona Health Dashboard* |
| **Developer Support Plan** | For users using AWS Services for testing, have email access to cloud support associates during business hours (General Hours <= 24 hrs, System Impaired <=12 hrs) |
| **Business Support Plan** | For users/businesses with AWS Production workloads, with 24/7 available support (phone/chat/email) through (Production System Impaired <=4 hrs, Production System Down <= 1hr in addition to dev perks) |
| **Enterprise Support Plan** | For Business-Critical Workloads, support time < 15 mins, 24/7 support through phone/email/chat. |

**The AWS Partner Network** is a group of cloud software/service vendors with hundreds of certified APN Partners worldwide.

**AWS Advisories/Bulletins** provide information on current vulnerabilities/threats (report abuse/vulnerabilities, conduct pen tests).