Protecting workloads in the cloud from Ransomware

Temi Adebambo
AWS Solutions Architecture
Considerations for cloud workloads

1. Alignment with security framework
2. Vulnerability Management in the Cloud
3. Multi-Account Structure
4. Disaster Recovery
5. Automation of Security Guardrails
1.1 Align to a standardized security framework

NIST Cybersecurity Framework

**Identify**
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Assessment Strategy
- Supply Chain Risk Management

**Protect**
- Access Control
- Awareness and Training
- Data Security
- Information Protection
  - Processes and Procedures
- Maintenance
- Protective Technology

**Detect**
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

**Respond**
- Response Planning
- Communications Analysis
- Mitigation Improvements

**Recover**
- Recovery Planning
- Improvements
- Communications
1.2 Utilize Cloud Services to mitigate ransomware

- Identify
- Protect
- Detect
- Respond
- Recover

AWS Services:
- AWS Systems Manager
- AWS Config
- AWS Security Hub
- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector
- Amazon CloudWatch
- AWS Lambda
- AWS Systems Manager
- AWS Key Management Service
- AWS Secrets Manager
- AWS Shield
- AWS Firewall Manager
- AWS Identity and Access Management (IAM)
- AWS IoT Device Defender
- AWS Single Sign-On
- AWS WAF
- AWS CloudWatch
- AWS Shield
- AWS Secret Manager
- AWS Firewall Manager
- CloudEndure Disaster Recovery
- AWS Backup
- AWS Console

Diagram shows a cycle of Identify → Protect → Detect → Respond → Recover.
2. Vulnerability Management

Unpatched vulnerabilities are one of the most common ways ransomware infects an organization’s environment.

- **Build and distribute Golden Images** Use an automated factory to build images conforming to your standards, test their compliance to required policies, probe for known vulnerabilities, and distribute them across your organization for use.

- **Allow only approved Golden AMIs** Approved AMIs can then be distributed to your organization and tools. Service Control Policies (SCPs) can be used to apply controls ensuring that new compute resources can only be started using the approved versions of the AMI.

- **Monitor configuration changes for compliance** AWS Config rules can be used to monitor compliance to these policies, for example, automatically highlighting older resources that are out of compliance when old AMIs are decommissioned or new vulnerabilities found.

- **Use your AMI pipeline for patch management** The AMI pipeline can be used to roll out patches with new versions of the Golden AMI. This strategy aligns with infrastructure as code best practices and provides a secure auditable trail for your compute resources.
3.1 Establish a multi-account structure
3.2 Utilize Virtual Private Clouds

Segmenting VPCs into isolated components, either by security groups and network access control lists (ACL) so that only necessary traffic is available can reduce ransomware’s ability to spread indiscriminately across AWS environments.
4. Disaster recovery processes

- Develop High Availability architectures
- Leverage infrastructure as code to restore data quickly
- Build detailed playbooks to test them periodically
- Store backups and images in an isolated account with minimal access
- Use different encryption keys for different sets of data
5. Automate security guardrails and response

1. All findings automatically send to CloudWatch events, and
2. Security Hub user can select findings in the console and take a custom action on them. These findings are sent to CloudWatch decorated with a custom action ID.

3. User creates Amazon CloudWatch Events rules to look for certain findings associated with a custom action ID or findings with specific characteristics.

4. The rule defines a target, typically a Lambda function, Step Function, or Automation document.

5. The target could be a chat, ticketing, on-call management, SOAR platform, or custom remediation playbook.

AWS Security Hub

Event

Amazon CloudWatch

Rule

Lambda function

Automation document

AWS Step Function

Custom Remediation
Thank you!