Attack-Defense Use Cases in AWS

Protect your AWS environment with robust security measures

Unauthorized Access Attempts

Attack Vectors

Attackers may attempt to gain unauthorized access to AWS resources by exploiting weak credentials, misconfigured IAM roles, or through phishing attacks.

Weak Credentials | **Misconfigured IAM Roles** | **Phishing Attacks**

Defense Strategies

Implement Multi-Factor Authentication (MFA)
Add an extra layer of security for all users.

Use AWS Identity and Access Management (IAM)
Apply the principle of least privilege with fine-grained permissions.

Enable AWS CloudTrail
Log all API calls and monitor for suspicious activity.

Utilize AWS GuardDuty
Detect unauthorized access attempts and malicious activity.

Data Exfiltration

Attack Vectors

Attackers might exfiltrate sensitive data stored in S3 buckets, RDS instances, or other AWS storage services.

- S3 Buckets
- RDS Instances
- AWS Storage Services

Defense Strategies

Encrypt Data:
Use AWS Key Management Service (KMS) to encrypt data at rest and in transit.

- **S3 Bucket Policies:** Configure S3 bucket policies and access controls to restrict access.
- **AWS Macie:** Use Macie to identify and protect sensitive data stored in S3.
- **VPC Flow Logs:** Monitor VPC Flow Logs for unusual data transfer activities.

Distributed Denial of Service (DDoS) Attacks

Attack Vectors

DDoS attacks aim to overwhelm AWS resources, causing service disruptions.

Overwhelming AWS Resources | Causing Service Disruptions

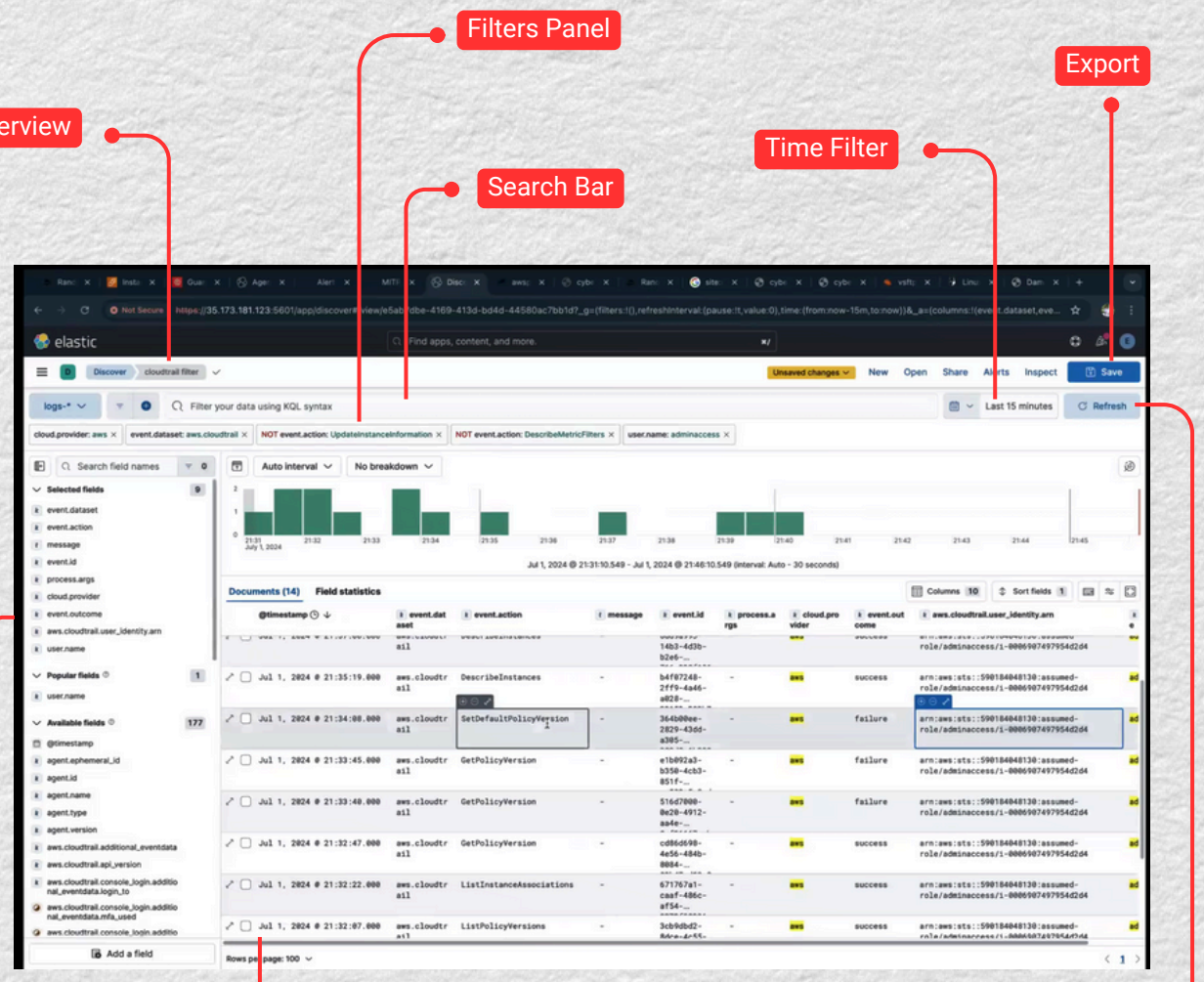
Defense Strategies

AWS Shield
- Protect against DDoS with Shield Advanced.
- Automatic detection and mitigation of attacks.

Amazon CloudFront
- Absorb and distribute traffic using CDN.
- Reduce latency and balance load efficiently.

Elastic Load Balancing
- Distribute incoming traffic across multiple instances.
- Ensure high availability and fault tolerance.

AWS WAF
- Block malicious web traffic using WAF.
- Customize and enforce web ACL rules.



Privilege Escalation

Attack Vectors

Attackers may exploit vulnerabilities to escalate privileges within the AWS environment.

Defense Strategies

IAM Policies

Ensure all IAM policies are up-to-date to prevent unauthorized privilege escalation.

AWS Config

Use AWS Config to monitor and enforce compliance with security best practices.

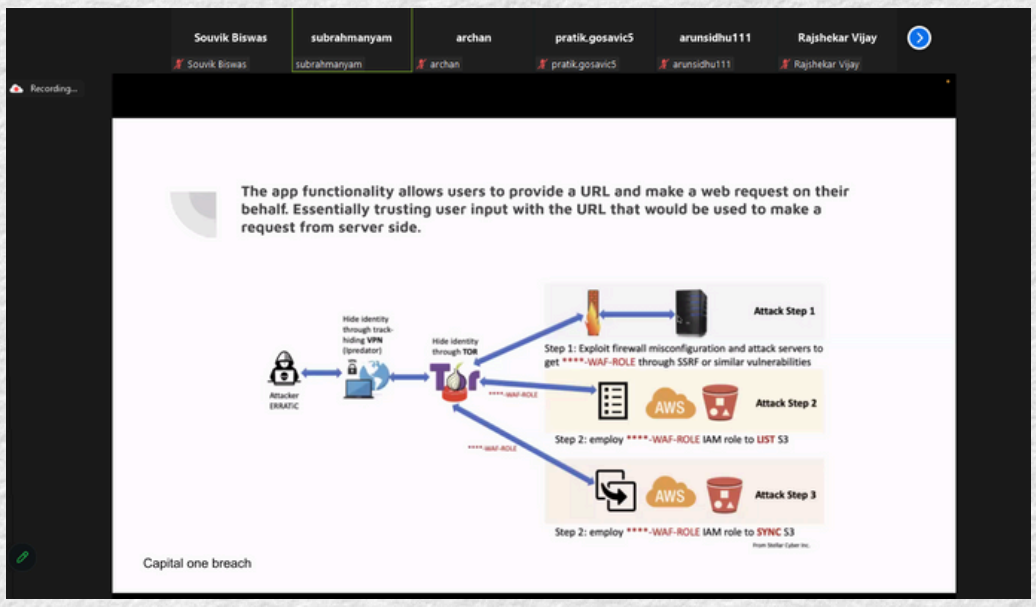
Security Groups

Apply restrictive security group rules to limit access and minimize attack surface.

AWS CloudTrail Insights

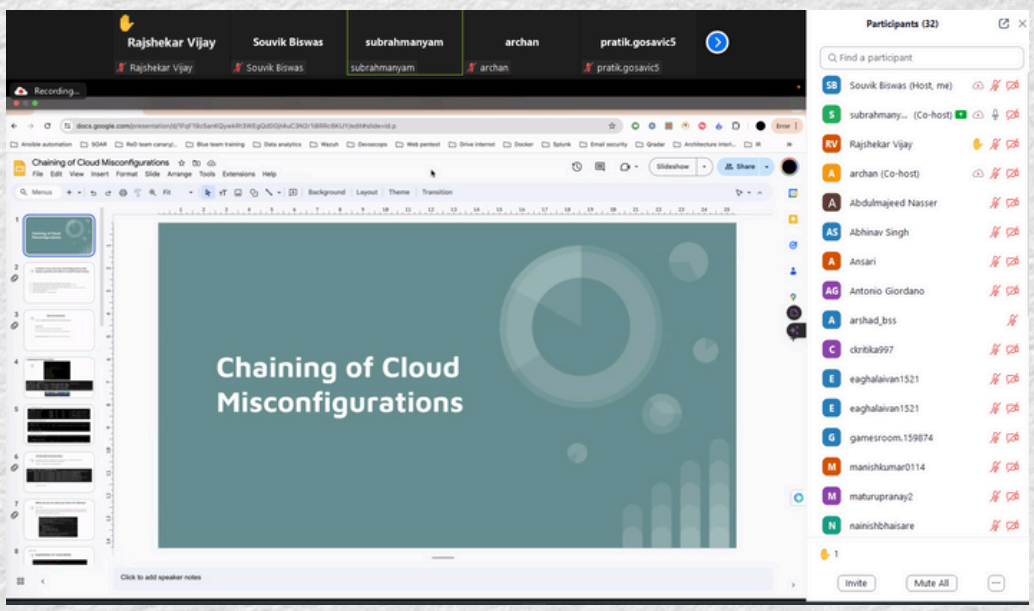
Enable CloudTrail Insights to automatically identify and alert on suspicious activity patterns.

Latest PCD Course on Attack and Defence on Cloud



Chaining of Cloud Misconfigurations

Chaining of Cloud Misconfigurations involves exploiting multiple cloud configuration errors to escalate privileges and gain unauthorized access.



Insecure APIs and Web Applications

Attack Vectors

Attackers can exploit vulnerabilities in APIs and web applications hosted on AWS.

Defense Strategies

Web Application Firewall

Protect web applications from common web exploits and malicious traffic by using AWS WAF. It filters and monitors HTTP requests to secure your applications.

Amazon API Gateway

Create, publish, and secure APIs using Amazon API Gateway. It provides robust features for API traffic management, authorization, and access control.

Static Code Analysis

Utilize tools like AWS CodeGuru for static code analysis. Identify vulnerabilities in code early in the development lifecycle to enhance application security.

Security Audits

Conduct regular security audits and penetration testing to identify and address vulnerabilities. Regular assessments help maintain application security and compliance.

Misconfigured Cloud Resources

Attack Vectors

Misconfigured resources can be exploited by attackers to gain unauthorized access or disrupt services.

Defense Strategies

1. **AWS Config Rules:** Implement AWS Config Rules to ensure compliance with security best practices.
2. **AWS Trusted Advisor:** Use Trusted Advisor to identify misconfigurations and optimize resources.
3. **Automated Remediation:** Set up automated remediation for non-compliant resources using AWS Systems Manager.

Insider Threats

Attack Vectors

Insiders with legitimate access might misuse their privileges to compromise data or services.

Defense Strategies

IAM Roles and Policies: Implement strict IAM roles and policies with the principle of least privilege.

CloudTrail and GuardDuty: Monitor user activities with CloudTrail and detect anomalies with GuardDuty.

AWS Security Hub: Use Security Hub to aggregate and prioritize security findings from multiple AWS services.

Employee Training: Conduct regular security awareness training for employees.