Raft meeting – 11/9 @2:30 pm

Meeting with Aaron Owens, Jose Ramirez – Both veterans, both recent joins to Raft

Who we are:

Raft (https://TeamRaft.com) is a **customer-obsessed non-traditional small business** with a purposeful focus on **Distributed Data Systems, Platforms at Scale, and Complex Application Development**, with headquarters in Reston, VA. Our range **of clients include innovative federal and public** agencies leveraging design thinking, cutting edge tech stack, and cloud native ecosystem. We build digital solutions that impact the lives of millions of Americans.

We’re looking for an experienced Senior Cybersecurity Engineer to support our customers and join our passionate team of high-impact problem solvers. This is a unique opportunity to help build and shape a game-changing organization where we put our customers and people first.

About the role:

As a Senior Cybersecurity Engineer, every day presents unique challenges as you navigate the intricate world of cyber defense. In this role, you'll be the first line of defense, safeguarding sensitive data and information systems of our defense sector customers against a wide array of cyber threats. You might start your day with a vulnerability assessment or a strategic meeting discussing advanced cybersecurity solutions. Perhaps you'll spend **your afternoon training team members** on **network security best practices,** or you may find yourself deep in analysis, identifying potential vulnerabilities in complex systems. Your excellent problem-solving skills will be challenged as you respond to potential security breaches, develop counteractive strategies, and ensure that our robust network security policies are in place and updated.

What we are looking for:

Comprehensive experience in information security or related field, with a focus on defense or government sector preferred

Extensive experience in planning, building, configuring, and maintaining cybersecurity tooling

Strong knowledge of various network architectures, security frameworks, and security incident management

Understanding of the lifecycle of a security incident and how to preserve the system and data to support investigation and recovery & reconstitution

Proficiency in cybersecurity tooling and software such as Prisma Cloud, Anchore, Trivy, Ansible, Splunk, ELK, SonarQube, Twistlock, Tenable, Fortify, or similar industry standard tools

Excellent problem-solving and analytical skills. Ability to work with software developers and engineers to understand and document why security controls can or cannot be implemented

Deep understanding of risk assessment tools, technologies, and methods

Detailed technical knowledge of database and operating system security. Knowledge of the latest cyber threats and proficiency in formulating strategies to counteract them

Excellent communication skills with the ability to explain complex security issues in simple terms

Highly **preferred**:

Cybersecurity-specific certification (e.g., CISSP, CISM, CEH)

Experience with cloud-based environments and their specific security challenges

Experience with containerization platforms (e.g. Docker & Kubernetes)

Experience with regulatory compliance and information security management frameworks (e.g., ISO 27001, **NIST**, GDPR)

Experience in conducting self-assessments to test the system’s security posture and recommending changes to Engineering teams

Experience with the process to obtain an Authority to Operate (ATO) and working with responsible compliance teams to gather required documentation

Experience in leading cross-functional teams or projects

Existing professional relationships with Platform One leadership and engineers

Clearance Requirements:

Ability to **obtain** and maintain a U.S. SECRET Security Clearance

* Work Type:  Talk **about Auditing, Monitoring and reviewing systems** to **identify** and **act on** Risks. Improving the security posture, collaborating with different teams to remediate vulnerabilities.
  + Mention experience using Gitlab and deploying Pre-Commit Checks and **Secrets Scanning** (GitLeaks, Truffle Hog), SAST, DAST, SCA Tools (Foritify, Snyk, SolarCloud, OWASP Zap), Container Security (Aqua **Trivy**)
  + Using **OWASP Top 10, ASVS, CVE** (Common Vulnerability Exposures), CWE (Common Weakness Enumeration), SANS 25 to identify and act on software vulnerabilities. Advising and working w/ devs to remediate issue
  + Qualys, Tenable Nessus, and DefectDojo for vulnerability management.
  + Threat Modeling - **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) and **DREAD** (Damage, Reproducibility, Exploitability, Affected Users, Discoverability)

Remote (Local to San Antonio, TX preferred)

What we will offer you:

Highly competitive salary

Fully covered healthcare, dental, and vision coverage

401(k) and company match

Unlimited PTO + 11 paid holidays

Education & training benefits

Annual budget for your tech/gadgets needs

Monthly box of yummy snacks to eat while doing meaningful work

Team off-site in fun places!

Generous Referral Bonuses

And More!

Our Vision Statement:

We bridge the gap between humans and data through radical transparency and our obsession with the mission.

Our Customer Obsession:

We will approach every deliverable like it's a product. We will adopt a customer-obsessed mentality. As we grow, and our footprint becomes larger, teams and employees will treat each other not only as teammates but customers. We must live the customer-obsessed mindset, always. This will help us scale and it will translate to the interactions that our Rafters have with their clients and other product teams that they integrate with. Our culture will enable our success and set us apart from other companies.

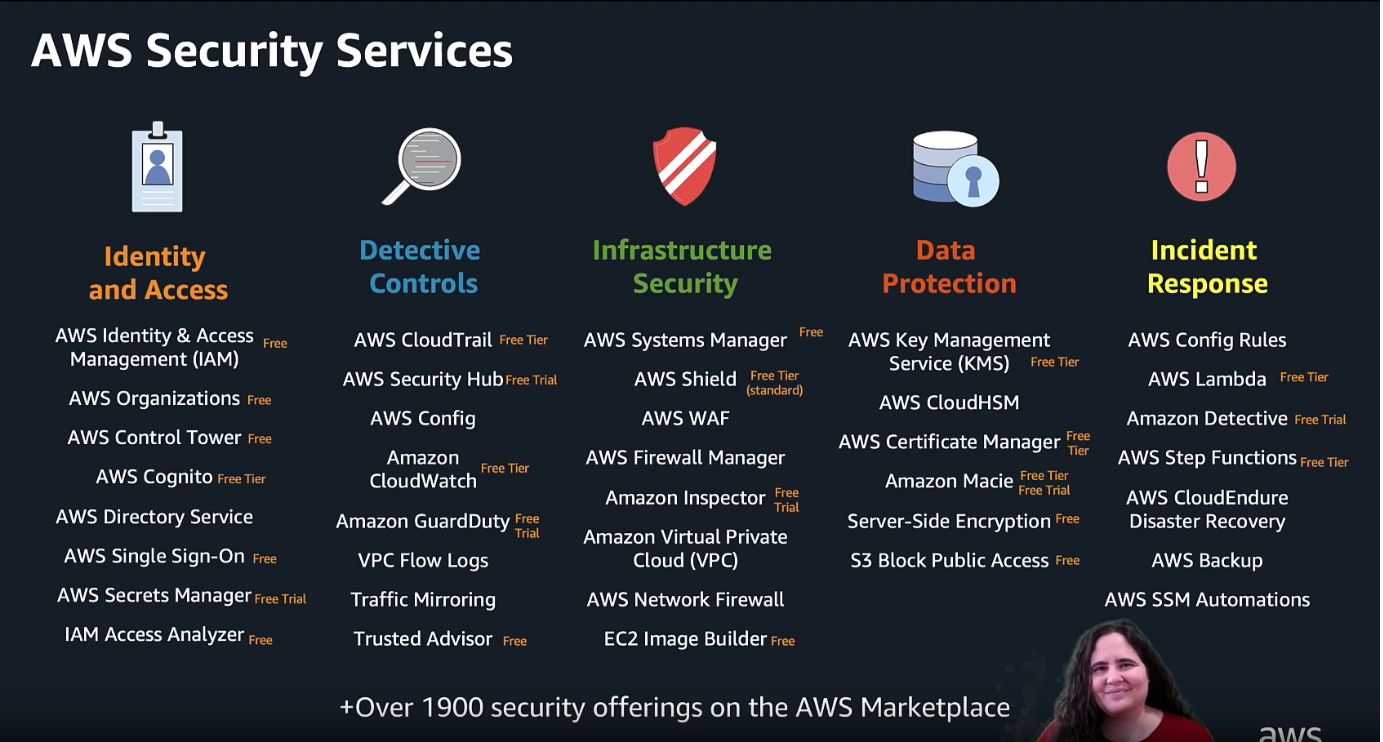
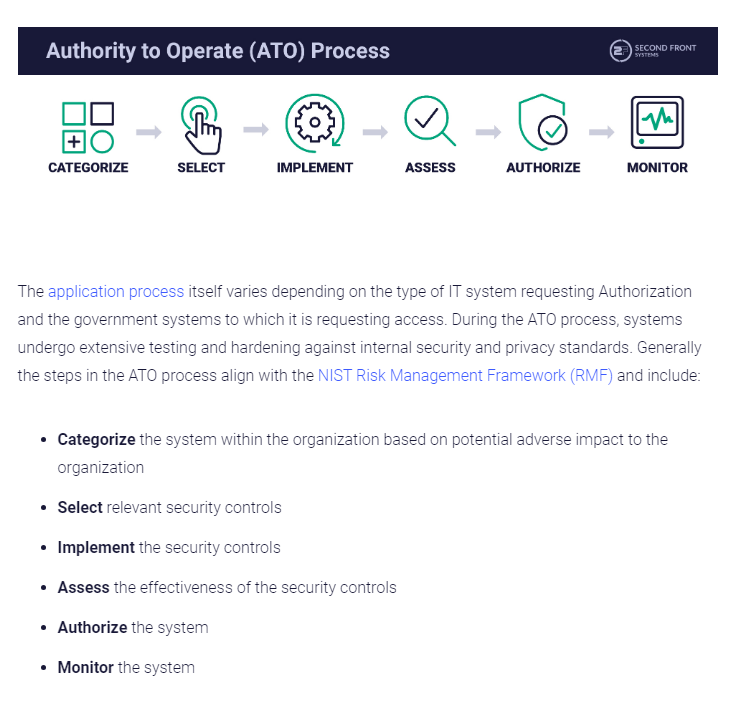
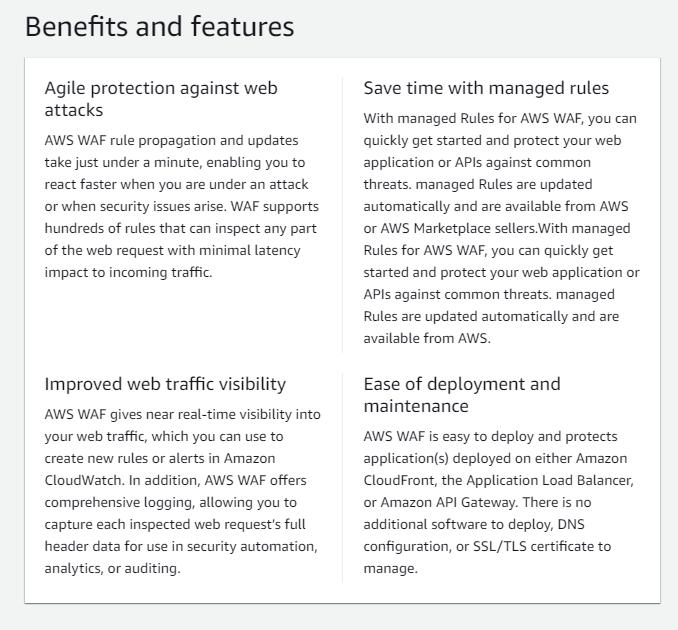
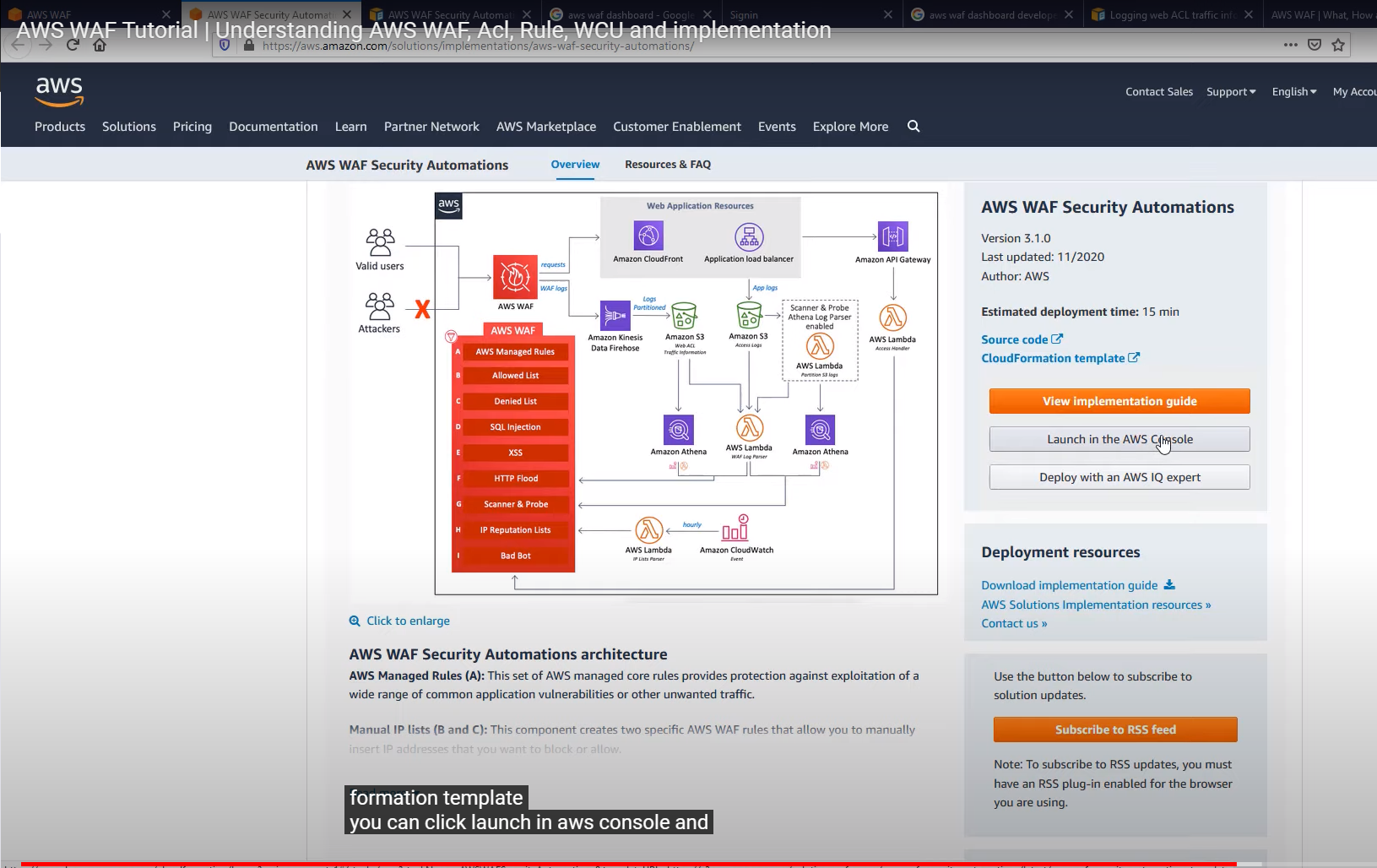
How do we get there?

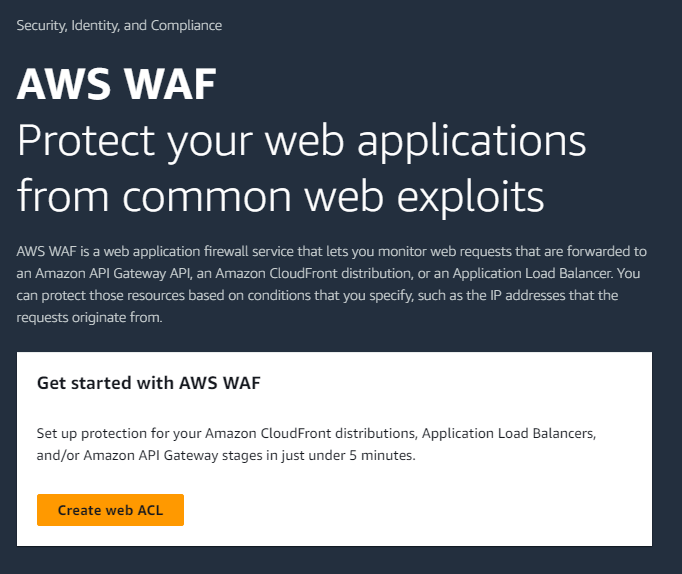
Public-sector modernization is critical for us to live in a better world. We, at Raft, want to innovate and solve complex problems. And, if we are successful, our generation and the ones that follow us will live in a delightful, efficient, and accessible world where out-of-box thinking, and collaboration is a norm.

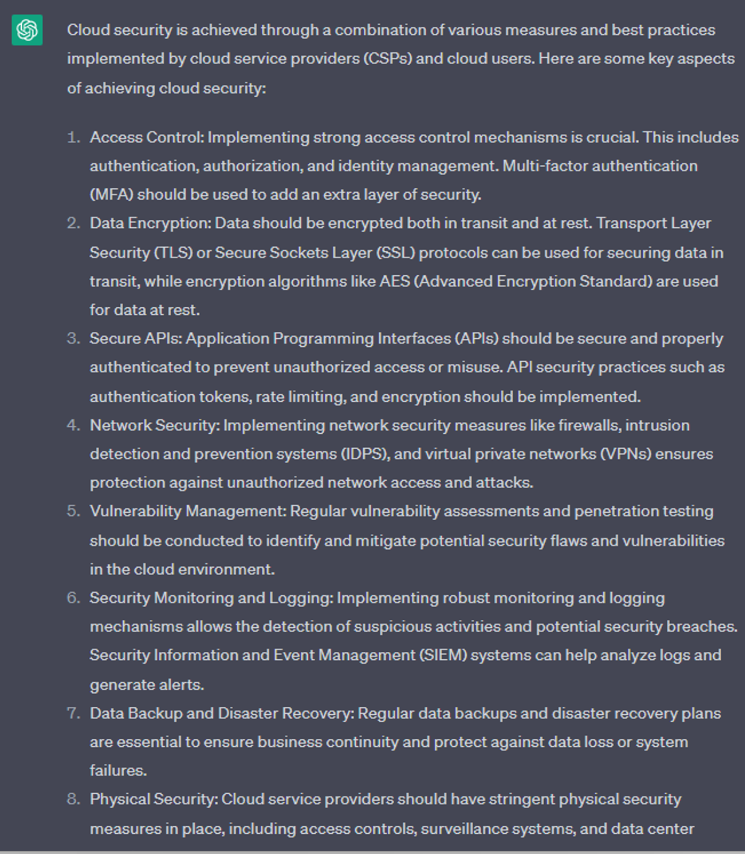
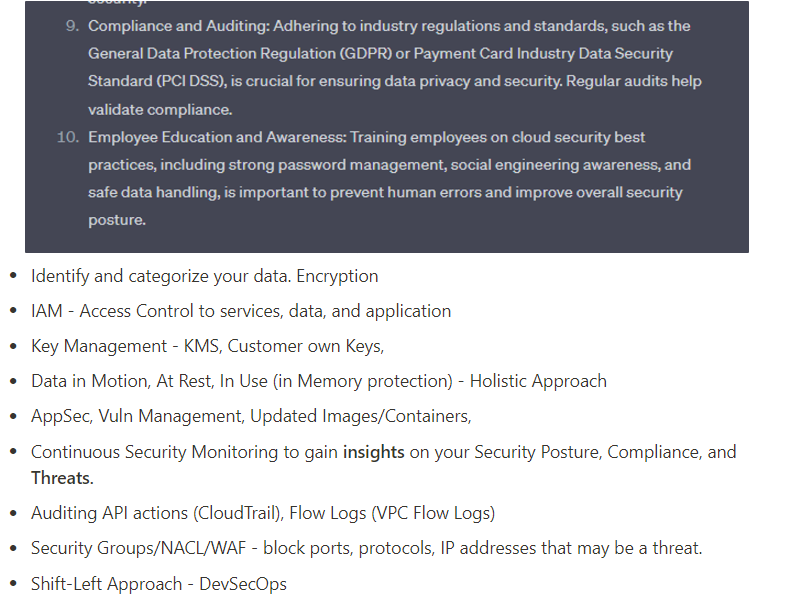
Raft’s core philosophy is Ubuntu: I Am, Because We are. We support our “nadi” by elevating the other Rafters. We work as a hyper collaborative team where each team member brings a unique perspective, adding value that did not exist before. People make Raft special. We celebrate each other and our cognitive and cultural diversity. We are devoted to our practice of innovation and collaboration.

We’re an equal opportunity employer. All applicants will be considered for employment without attention to race, color, religion, sex, sexual orientation, gender identity, national origin, veteran or disability status.

We’re an equal opportunity employer. All applicants will be considered for employment without attention to race, color, religion, sex, sexual orientation, gender identity, national origin, veteran or disability status.

* SIA – Security Impact Assessments – assessing a proposed change or addition to a system and the potential vulnerabilities that it may introduce. Collaborating with the architects and engineers planning to implement those changes. Documenting any new connections, changes to access, custom code, etc. Understanding the technical overview of the proposed change (ports, protocols, purpose of the change). Also, gathering the business impact it would bring, how would it affect the company, system and end-users? – communicate the findings with the ISO.
* PIA – Privacy Impact Analysis – Analyzing a system to see what sensitive information, PII, PHI, etc. it may contain that could affect user’s if exposed.
* POAMs - Plan of Action and Milestones – Audit systems/implementations to detect and document the steps that will be taken to mitigate risks and weaknesses in security controls.
* Monthly Software Audit – Audit Software list for any Unapproved or Divest status software via TRM and Fedramp. Communicate with developers to upgrade or remediate issues.
* Monthly Infrastructure Audits – Audit the Access Controls, User Privileges, Inactivity Accounts, New/Current VMs, Cloud Asset Management
* **AWS Security** – Leverage tools such **as IAM for proper access management. AWS Security Hub**, AWS Config (Compliance), AWS Macie (sensitive data), CloudWatch (Monitoring), CloudTrail (Auditing), **Wiz**, **Datadog (Observability)**, S3 Security (Bucket Policies, VPC Endpoints, KMS, Server-Side Encryption), SSM Patch Manager (Automate patches**), VPC Flow Logs, NACLs** (Subnet-level), Security Groups (EC2-level), IAM Access Control (permissions, users, roles, groups), AWS Organizations (SCPs), observe for any unused or rouge EC2 instance, S3 buckets, Databases, understanding Shared Responsibility Model for AWS, **GuardDuty** for Threat Detection = Act on Findings**, Billings Alarms** for Anomaly Detections, **Secrets Manager** to manage credentials and secrets. Load Balancers to prevent overloading servers and DoS. SSM Parameter Store - Secure storage for configuration and secrets, services in VPC, **AWS Config Rules** and AWS Lambda to automate Incident Response. Grant temp access with IAM roles or AWS Cognito (external users),
* Compliance & Frameworks – **NIST 800-53**, **CIS Benchmarks**, MARS-E 2.2, PCI-DSS, **AWS Security Maturity Model, CSA, AWS Well-Architected Framework, AWS Cloud Adoption Framework**
* The 5 ethics of the Security Cloud Adaption Framework****
* AWS WAF - Create rules to blacklist or whitelist (Web ACLs) requests based off IP addresses, Address ranges, CIDR blocks, URI path, location (geo region, specific countries). If a string matches exactly, starts with, ends with, contains a particular value. You can also use AWS Managed Rules or rules from AWS Market place. Prevent Brute force attacks, DDoS, Overwhelming your servers/applications with too many requests. **Rate Limits.**
* **help protect your web applications from common web application vulnerabilities and attacks, including SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).**
* **Prioritize rules based on your likings. Monitoring with CloudWatch.**
* **Integration with CloudFront and Application Load Balancers: You can integrate AWS WAF with AWS services like Amazon CloudFront and Application Load Balancers, which allows you to apply protection to your applications distributed over the AWS global network. Automation via CloudFormation templates**
* In your opinion, what are the key qualities or skills that make someone successful in this role and within the team?
* How is **success** measured in this role and how does one exceed expectations?
* What are some of the key challenges or pain-points that Goldman Sach’s and the auditing team face regarding Cloud Security?
* **ATO Process - ** 



Cloud Security entails  

Understanding the Shared Responsibility Model between CSP and