Secure *Systems*

Team Members

Secure From Scratch

Securing a System is a Multi-Disciplinary Effort

- System Architects
- Security Engineers
- **Programmers**
- Database Administrators
- DevOps
- Cloud Engineers
- IT Personal
- Network Engineers
- Compliance Officers
- Penetration Testers
- Risk Management Experts
- Security Operations Center (SOC) Monitors

Secure From Scratch

System Architects

Design and structure the system's overall architecture.

- Ensuring security principles are integrated into the architecture.
  e.g., least privilege, defense in depth
- Identifying security risks in the system design
  and recommending mitigations.
- Planning for secure data flows between system components.
- Establishing clear boundaries
  for microservices, ensuring proper network segmentation.

Secure From Scratch

Security Engineers

Design, implement, and maintain security infrastructure.

- Establishing encryption standards for data at rest and in transit.
- Managing public key infrastructure (PKI) and certificate authorities (CA).
- Conducting security assessments
  e.g., penetration testing, red teaming
- Enforcing multi-factor authentication (MFA) for all critical systems.
- Reviewing and mitigating security risks in new systems or services.

Secure From Scratch

Programmers

Write and maintain secure code.

- Following secure coding practices
  e.g., input validation, avoiding insecure dependencies
- Implementing strong authentication, authorization, encryption
- Conducting code reviews with a focus on security vulnerabilities.
- Using tools for static and dynamic code analysis
  To detect potential security issues.
- Regularly updating third-party libraries and dependencies
  To patch vulnerabilities.

Secure From Scratch

Database Administrators (DBAs)

Manage databases

- Enforcing database access controls and encryption.
- Regularly applying security patches to database systems.
- Conducting database auditing and monitoring
  - For unauthorized access attempts.
- Implementing data masking or tokenization for sensitive information.
- Ensuring secure backup and restore mechanisms for databases.

Secure From Scratch

Cloud Engineers

Manage cloud infrastructure.

- Ensuring proper identity and access management (IAM).
- Configuring with least privilege.
  security groups, firewalls, and VPCs
- Enforcing encryption for cloud storage
  e.g., S3 buckets, cloud databases
- Regularly reviewing and securing API gateways and cloud service access points.
- Implementing backup and disaster recovery strategies
  in a secure manner.

Secure From Scratch

DevOps Engineers

Automate infrastructure deployment and management.

- Setting up automated CI/CD pipelines
  With integrated security checks (e.g., SAST, DAST).
- Managing container security
  Ensuring secure images and orchestration practices.
- Implementing infrastructure-as-code securely
  e.g., least-privileged access in cloud deployments
- Ensuring secrets management practices
  e.g., environment variables, secure storage) are in place.
- Monitoring and maintaining logs/audit trails for security events.

Secure From Scratch

IT Personnel

Manage the physical and virtual infrastructure.

- Regular OS updates and patching of all systems.
- Firewall management
  Ensuring only necessary ports and services are exposed.
- Managing VPNs, and network security (including certificates)
- Setting up and maintaining access control policies
  e.g., LDAP, Active Directory
- Implementing bandwidth throttling and anti-DDoS measures.
- *Physical security* of server rooms, ensuring limited access.

Secure From Scratch

Network Engineers

Manage networking infrastructure

- Configuring and managing secure networks, firewalls, and routers.
- Setting up VPNs and secure tunneling for remote access.
- Implementing network segmentation and zero-trust network architectures.
- Ensuring secure DNS, load balancing, and traffic routing.
- Monitoring network traffic for anomalies and potential threats.

Secure From Scratch

Compliance Officers

Ensure adherence to legal and regulatory standards.

- Ensuring compliance with security regulations
  Such as GDPR, HIPAA, or PCI-DSS.
- Conducting regular security audits and documentation reviews.
- Managing data privacy and ensuring policies are adhered to.
  e.g. data retention and user consent
- Overseeing regular security training and awareness programs for staff.

Penetration Testers (Pentesters)

Simulate attacks on the system to find vulnerabilities.

- Conducting penetration testing
  - On applications, infrastructure, and networks.
- Providing detailed vulnerability reports with risk assessments.
- Assisting developers and IT personnel
  - In fixing identified vulnerabilities.
- Testing for specific attack vectors
  - Like SQL injection, XSS, CSRF, and buffer overflows.

Secure From Scratch

Risk Management Experts

Assess and mitigate security risks.

- Performing risk assessments
  - To identify potential security threats.
- Developing risk mitigation strategies and policies.
- Coordinating with other departments
  - To ensure that identified risks are mitigated.
- Keeping up to date with industry security standards and trends to adapt security posture.

Secure From Scratch

Security Operations Center (SOC) Monitors

Monitor, detect, and respond to security incidents.

- Continuous monitoring of logs, alerts, and incidents in real time.
- Running intrusion detection/prevention systems (IDS/IPS)
- Investigating alerts.
- Performing threat hunting
- Identifying potential threats or vulnerabilities.
- Coordinating incident response and mitigating active threats.
- Regular vulnerability scanning and analysis of emerging threats.

Secure From Scratch

Securing a System is a Multi-Disciplinary Effort

Just remember:

It's not *all* on you.

- Some things are too hard/expensive to solve in *your* code.