Security Engineering

Level/Skill	**Impact**	**Knowledge**	**Communication/Writing**	**Threat Fluency**	**Scope**
1	Creates a design document based on well-defined requirements and writes code to implement it with assistance from team.	Proficient at self-study when encountering new topics. Knows when they don't know the answer and asks for help. Comfortable writing code in at least one programming language Teleport uses. Rapidly learns security best practices such as public key cryptography, certificates, authn/authz, RBAC, the principle of least privilege, and blameless postmortem analysis. Learns team code review, on-call, incident response, and interviewing processes.	Actively solicits feedback from peers. Reports progress on a regular basis as required by the team's operational requirements.	Learns from current and historical security incidents across the industry. Familiar with and able to execute the most common attacks such as the OWASP Top 10.	Works on one or two small projects at a time, mostly within their own team.
2	Estimates implementation timelines and makes business appropriate tradeoffs to deliver high quality work on time. Participates in on call rotations, security incident response, and interviewing with supervision.	Develops a primary security discipline. Builds deep familiarity within this discipline and an understanding of common best practices across disciplines. For example an application security engineer can securely implement CA based architectures while a cloud security engineer can properly secure IAM and network boundaries. Either can applies industry best practices like setting up strong TLS, or picking appropriate authentication and authorization mechanisms. Proficient in the tools and languages of the chosen discipline. E.g. Golang, gRPC and Make for an app security engineer or Terraform, AWS and Kubernetes for a cloud security engineer. Customizes security recommendations to serve business need.	Writes high quality documentation. Provides constructive review on immediate peers' code and design. Helps new team members during their first weeks or mentors interns.	Understands attack vectors for client server architectures and network protocols. Applies lessons learned from Teleport's past security vulnerabilities.	Leads one or two medium or large projects at a time. Recognized for occasional participation in cross-team relationships and projects
3	Collaborates to scope requirements and triage priorities, based on Teleport's operating plan and team quarterly goals. Participates in on call rotations, leads incident response, and interviews without dedicated backup/mentorship.	Demonstrates deep security domain knowledge within one field and broad familiarity across adjacent fields. Proficiently navigate Teleport policies, codebases and tech stacks to find the right place at which to address security concerns. Familiar with security and GRC standards such as SOC2, ISO 27001, and the GDPR. Incorporates these standards as into design and review.	Supports less experienced peers' technical skills, answering questions and being a resource. Documents and improves team practices. Reviews RFDs from across the company for security concerns. Improves company wide security policies. Writes detailed, internal blameless postmortems for security incidents.	Able to chain attacks and apply Teleport specific details to develop attacks.	Leads cross-team projects and plays a significant role in major organizational initiatives. Relied upon to keep complex projects on-track and sustainably implemented.
4	Leads the implementation of isolated security projects that measurably and significantly impacts company security and business outcomes.	Serves as the expert resource to peers within or more technical areas.	Writes technical articles/blog posts, delivers tech and lightning talks representing the company's technical vision. Develops new company wide security policies, educates peers, and monitors outcomes to ensure policy objectives are accomplished. Effectively communicates with customers and the public about Teleport's security incidents. Senior engineers are not expected to find any notable security oversights in RFDs written or reviewed by Level 4+ Security Engineers.	Maintains a deep, comprehensive, and current understanding of attacks as well as the best techniques to mitigate them. Develops novel proof-of-concept attacks against Teleport's infrastructure and threat model.	Independently identifies and mitigates large security risks within Teleport.
5	Leads timely implementation of critical security infrastructure and programs in collaboration with all other teams.		Writes advanced technical articles/blog posts, gaining significant industry traction or delivers technical talks on major conferences representing the company's vision.		
6	Designs novel solutions that solve contemporary industry wide security issues and create notable competitive advantage for Teleport.		Produces peer-reviewed research papers, patent applications, or books.		Independently identifies and mitigates large security risks across the industry.