Here’s how the **Security/Network Engineer** role would fit into your Threat Intelligence Platform pipeline — their focus will be **protecting the platform, securing its infrastructure, ensuring compliance, and enabling safe integrations with external systems**.  
They’ll work closely with **Backend Engineers** for API security, **Data/AI Engineers** for safe data handling, and the **Flutter Dev** for secure mobile access.

**Phase 0 – Platform Architecture & Infrastructure Setup**

* Design **secure network architecture** (VPC, subnetting, firewalls, VPN, bastion hosts).
* Define **zero-trust principles** and enforce **least privilege access**.
* Deploy **intrusion detection/prevention systems (IDS/IPS)**.
* Configure **TLS/SSL encryption** for all data in transit.
* Harden servers (OS, database, application layer).
* Set up **network monitoring tools** (Zeek, Suricata, Wazuh).

**Phase 1 – Data Acquisition & Ingestion**

* Validate **source feed security** (ensure no malicious payloads).
* Configure **secure API keys, tokens, and certificates** for external data feeds.
* Ensure ingestion points are **protected from DoS/DDoS** attacks.
* Implement **traffic filtering** for ingestion endpoints (only trusted IP ranges).

**Phase 2 – Data Normalization & Storage**

* Enforce **data encryption at rest** (disk-level and database encryption).
* Implement **TLP-based access control** for sensitive threat data.
* Work with Backend Engineer to prevent **injection attacks** through queries.
* Configure **network segmentation** for databases to prevent lateral movement.

**Phase 3 – Threat Data Management**

* Set up **IOC access policies** (only authorized analysts can see certain TLP levels).
* Monitor **data exfiltration risks** from enrichment APIs.
* Validate data integrity during enrichment processes.
* Apply **content sanitization** to remove malicious scripts in data fields.

**Phase 4 – Analysis & Correlation**

* Secure **AI/ML service endpoints** (API keys, role-based access).
* Validate that no **sensitive or regulated data** is passed to external AI APIs (GDPR compliance).
* Work with AI Engineer to design **safe prompt injection prevention measures** for LLMs.
* Audit correlation jobs to ensure they don’t leak restricted data in results.

**Phase 5 – Visualization & Reporting**

* Ensure dashboards **authenticate and authorize properly**.
* Apply **field-level security** (some users shouldn’t see certain indicators).
* Implement **logging and monitoring** for all report generation requests.
* Use **digital signing** for exported reports to ensure integrity.

**Phase 6 – Security Operations Integration**

* Configure **secure integrations with SIEM/SOAR systems** (TLS, VPN, IP whitelisting).
* Ensure **alerting channels** (email, Slack, SMS) are encrypted and trusted.
* Test and validate **SOC playbook integrations** for security.
* Monitor for **unauthorized API access attempts** from external SOC tools.

**Phase 7 – Governance, Compliance & Security**

* Implement **RBAC** across all layers of the platform.
* Maintain **audit logs** for all network, API, and data access activities.
* Ensure **GDPR/CCPA compliance** for data storage, sharing, and deletion.
* Define and enforce **data retention policies** with secure deletion methods.
* Manage **secrets and key rotation policies** using Vault or cloud KMS.
* Conduct **regular security assessments & penetration tests**.

**Phase 8 – AI & Automation (if included)**

* Work with AI Engineer to **secure AI inference endpoints** from abuse.
* Monitor AI/LLM requests for **prompt injection attacks** or malicious queries.
* Set network-level restrictions on which AI APIs can be called.
* Log and audit all AI-assisted decisions for **accountability**.

**Expected Outcomes from Security/Network Engineer’s Work**

* **Zero major security incidents** through strong preventive controls.
* **Fully encrypted, segmented, and monitored infrastructure**.
* **Secure API integrations** with external threat feeds, SIEMs, and mobile apps.
* **Compliance-ready system** that can pass security audits.
* **Resilient network** against DDoS, intrusion attempts, and data leaks.

**UPDATE PLAN:  
Here’s a Security/Network Engineer responsibilities breakdown for your TIP roadmap, mapped to the exact phases you provided and considering the other roles (Data Engineer, AI Engineer, Backend Engineer, Flutter Dev).**

**Security/Network Engineer – Responsibilities in TIP Pipeline**

**Phase 0 – Project Initiation & Planning**

* **Define security & compliance requirements for the entire platform (GDPR, ISO 27001, SOC 2, local laws).**
* **Advise on deployment architecture from a security standpoint (on-prem, cloud, hybrid).**
* **Estimate security infrastructure costs (firewalls, VPNs, intrusion prevention).**
* **Contribute to risk assessment for platform components and data flows.**

**Phase 1 – Data Acquisition & Ingestion**

* **Secure network connections to threat intel sources:**
  + **TLS 1.3 enforcement, API key vault storage, mutual TLS if supported.**
* **Implement rate-limiting and IP whitelisting for ingestion endpoints.**
* **Monitor source authenticity and detect tampered or malicious feeds.**
* **Set up VPNs or private peering for sensitive/commercial feed access.**
* **Collaborate with Backend Engineers to ensure connectors follow secure API practices.**

**Phase 2 – Data Normalization & Storage**

* **Ensure database-level security:**
  + **Encryption at rest (AES-256) and in transit (TLS).**
  + **Network segmentation for DB servers.**
* **Implement access control lists (ACLs) to restrict DB queries to authorized services.**
* **Review storage choices (SQL, NoSQL, graph DB) for compliance & isolation needs.**
* **Help define secure backup and recovery plans.**

**Phase 3 – Threat Data Management**

* **Apply RBAC and TLP rules to data access.**
* **Audit enrichment API calls to prevent data leakage to third parties.**
* **Monitor for suspicious query patterns (possible misuse or compromise).**
* **Work with AI Engineers to sanitize inputs/outputs to LLMs (avoid sensitive IOC leaks).**

**Phase 4 – Analysis & Correlation**

* **Secure ML pipelines:**
  + **Isolate AI model environments to avoid contamination from untrusted data.**
  + **Ensure safe storage and transfer of enriched/correlated results.**
* **Monitor for adversarial ML attacks (poisoned training data, prompt injection).**
* **Support secure API calls to external threat scoring or enrichment services.**

**Phase 5 – Visualization & Reporting**

* **Ensure secure API access for Flutter apps and web dashboards:**
  + **JWT/OAuth2 authentication, TLS enforcement.**
* **Review graph and map visualizations to ensure no sensitive geo/IP data is exposed to unauthorized users.**
* **Collaborate with Flutter Dev to enforce secure session management.**

**Phase 6 – Security Operations Integration**

* **Lead SIEM/SOAR integration:**
  + **Secure bidirectional data flows between TIP and SOC tools.**
* **Configure alert channels (Email, Slack, Teams, PagerDuty) with secure authentication.**
* **Implement incident response hooks securely:**
  + **IOC pushes to firewalls, WAFs, EDRs.**
* **Build SOAR playbooks for automated blocking and incident ticketing.**
* **Harden platform network perimeter:**
  + **Network segmentation.**
  + **Intrusion Detection/Prevention (IDS/IPS).**
  + **API rate limiting & anomaly detection.**

**Phase 7 – Testing & QA**

* **Conduct penetration testing on:**
  + **APIs**
  + **Mobile app connections**
  + **Backend services**
* **Perform vulnerability scanning (internal & external).**
* **Simulate network attacks (DDoS, MITM) to verify resilience.**

**Phase 8 – Governance, Compliance & Security *(Main Responsibility Zone)***

* **Design and enforce RBAC, MFA, least privilege principles.**
* **Maintain audit logs for all user and system actions (immutable/WORM storage).**
* **Oversee data retention & disposal policies for compliance.**
* **Manage secrets & key rotation via Vault or AWS Secrets Manager.**
* **Vet and periodically review feed provider trustworthiness.**

**Phase 9 – Deployment & Release Management**

* **Approve security sign-off before release.**
* **Validate staging environments mirror production security configurations.**
* **Secure CI/CD pipelines (artifact signing, secret scanning).**

**Phase 10 – Monitoring & Continuous Improvement**

* **Maintain continuous security monitoring:**
  + **Intrusion detection.**
  + **Threat feed availability.**
  + **Unusual network activity.**
* **Review security incidents and feed lessons learned into platform hardening.**
* **Update security controls for new threats (zero-days, evolving attack methods).**

**Phase 11 – Documentation & Training**

* **Create security SOPs for platform use and incident handling.**
* **Train analysts and developers on secure data handling practices.**
* **Document network diagrams with security zones and controls.**

**Collaboration Points**

* **Backend Engineers – API security, network protocols, authentication flows.**
* **Data Engineers – Secure ingestion pipelines, encrypted storage.**
* **AI Engineers – Secure ML pipelines, prevent sensitive data leaks in AI outputs.**
* **Flutter Developers – Secure mobile communications, session management, offline data encryption.**