If you’re building a **complete security ecosystem** alongside a TIP, Network Detection & Response (NDR), and a SIEM, there are several other complementary components that usually fit in.  
Here’s a breakdown by category so it’s not just a random list:

**1. Threat Detection & Intelligence**

* **Endpoint Detection & Response (EDR)** – Detects and responds to threats on endpoints like laptops and servers.
* **XDR (Extended Detection & Response)** – Consolidates EDR, NDR, SIEM data for unified threat response.
* **Deception Technology / Honeypots** – Lures attackers to fake assets to study and detect them.
* **Threat Hunting Platform** – For proactive search of hidden threats.

**2. Security Automation & Orchestration**

* **SOAR (Security Orchestration, Automation, and Response)** – Automates incident response workflows between TIP, SIEM, EDR, etc.
* **Playbook Automation Tools** – Pre-defined response templates for common threats.

**3. Network & Perimeter Security**

* **Firewall / NGFW** – Traditional and next-gen firewalls with intrusion prevention.
* **IDS / IPS** – Intrusion Detection/Prevention Systems for packet-level inspection.
* **Secure Web Gateway (SWG)** – Protects from malicious sites and enforces browsing policies.
* **DNS Security** – Detects domain-based threats and blocks them before connections happen.

**4. Identity & Access Security**

* **IAM (Identity and Access Management)** – Controls user permissions.
* **PAM (Privileged Access Management)** – Protects high-privilege accounts.
* **MFA / Zero Trust Access** – Ensures strong authentication and minimal trust by default.

**5. Cloud & Application Security**

* **CSPM (Cloud Security Posture Management)** – Detects misconfigurations in cloud platforms.
* **CWPP (Cloud Workload Protection Platform)** – Protects workloads across cloud environments.
* **API Security Gateway** – Monitors and protects APIs from exploitation.
* **WAF (Web Application Firewall)** – Protects apps from OWASP Top 10 attacks.

**6. Monitoring & Analytics**

* **UEBA (User and Entity Behavior Analytics)** – Detects anomalies in user and device behavior.
* **Log Management System** – Centralizes logs from all sources for analysis.
* **Dark Web Monitoring** – Detects stolen credentials and sensitive data leaks.

**7. Incident Response & Recovery**

* **Digital Forensics Tools** – Investigates breaches and gathers evidence.
* **Backup & Disaster Recovery Platform** – Ensures continuity after cyberattacks.