**1. Threat Data Ingestion & Aggregation**

* **Multi-source integration** (internal + external feeds)
* **STIX/TAXII protocol support** for structured threat data
* **Open-source intelligence (OSINT) ingestion**
* **Commercial threat feed integration** (paid vendors)
* **Dark web and deep web monitoring feeds**
* **Malware analysis feed ingestion** (sandbox results)
* **Vulnerability database ingestion** (NVD, CVE feeds)
* **Integration with SIEM, SOAR, IDS/IPS, EDR** tools for telemetry ingestion
* **Custom feed ingestion** via APIs or file uploads

**2. Data Normalization & Enrichment**

* **Parsing and standardizing disparate data formats**
* **Deduplication of repeated IOCs**
* **Contextual enrichment** (geolocation, ASN, WHOIS, domain age)
* **Threat actor profiling** (group, motivation, campaign)
* **MITRE ATT&CK mapping** for TTPs
* **Link analysis** between related indicators
* **Historical threat data lookup**
* **Risk scoring & confidence scoring** for each IOC
* **Correlation with past incidents or alerts**

**3. Threat Analysis & Prioritization**

* **Automated correlation** across feeds and events
* **Relevance filtering** based on organization’s assets & industry
* **IOC prioritization** (critical, high, medium, low)
* **Campaign tracking & attribution**
* **Behavioral pattern recognition** (TTP patterns)
* **Machine learning–based threat prediction**
* **Trend and frequency analysis** of indicators
* **Threat clustering** (grouping related indicators/events)

**4. Visualization & Reporting**

* **Unified threat dashboard** with KPIs and metrics
* **IOC and relationship graphs** (link analysis visualization)
* **Threat timeline views** (campaign evolution over time)
* **Geospatial threat mapping** (heatmaps, origin locations)
* **Customizable reports** (executive vs analyst views)
* **Automated scheduled reporting**
* **Export to multiple formats** (PDF, CSV, JSON, STIX)

**5. Integration & Automation**

* **SOAR integration** for automated response playbooks
* **SIEM integration** for alert enrichment
* **Firewall, IDS/IPS, EDR, WAF rule updates** from intelligence
* **Custom API for bidirectional data exchange**
* **Automated blocking of malicious domains/IPs**
* **Real-time threat intelligence sharing** with ISACs/partners
* **Ticketing system integration** (Jira, ServiceNow)

**6. Collaboration & Sharing**

* **Role-based access control** for analysts and teams
* **Threat intelligence sharing communities** (industry ISAC/ISAO)
* **Anonymous sharing options** to protect source identity
* **Annotation & commenting** on intelligence items
* **Case management** for collaborative investigation
* **Cross-organization sharing policies**

**7. Security & Compliance**

* **Data retention policies**
* **Access logging & audit trails**
* **Encryption at rest and in transit**
* **Compliance mapping** (NIST, ISO 27001, GDPR, etc.)
* **Integration with compliance reporting tools**

**8. Advanced / Optional Features**

* **AI-assisted threat analysis & summarization**
* **Threat hunting workbench** within TIP
* **Malware sandboxing integration**
* **Incident simulation & wargaming**
* **Custom threat scoring algorithms**
* **Historical “replay” of threat landscapes**
* **Deception technology integration** (honeypots, honeytokens)