Threat Intelligence Integration

OSINT and Commercial Feeds

August 2024

31 Pages

Nexora Security Research Team
security@nexora.io

Executive Summary

Threat intelligence is critical for proactive defense. This whitepaper details Nexora's architecture for real-time threat intelligence aggregation from NIST NVD, MITRE ATT&CK, AlienVault OTX, and commercial feeds.

Integration of 15+ threat intelligence sources provides comprehensive coverage of emerging threats.

Automated correlation reduces mean time to detect (MTTD) to 1.8 seconds.

1. Threat Intelligence Sources

1.1 Open Source Intelligence (OSINT)
Public threat intelligence feeds:
• NIST National Vulnerability Database (NVD)
• MITRE ATT&CK Knowledge Base
• AlienVault Open Threat Exchange (OTX)
• Abuse.ch threat feeds
• CIRCL OSINT feeds

1.2 Commercial Feeds
Premium threat intelligence:
• Recorded Future
• Anomali ThreatStream
• Mandiant Threat Intelligence
• CrowdStrike Falcon Intelligence
• Palo Alto Networks Unit 42

2. STIX/TAXII Integration

2.1 STIX 2.1 Format

Structured Threat Information Expression:

- Indicator objects (IoCs)
- Attack patterns (MITRE ATT&CK)
- Malware and tool descriptions
- Threat actor profiles
- Courses of action (mitigations)

2.2 TAXII 2.1 Protocol

Trusted Automated eXchange of Intelligence:

- Collection-based data exchange
- Real-time feed subscriptions
- Bidirectional sharing
- Authentication and encryption
- Rate limiting and quotas

3. Automated Correlation

3.1 Entity-to-Threat Mapping
Real-time correlation engine:
• CVE to entity exposure mapping
• Attack pattern to behavior matching
• Threat actor to campaign attribution
• IoC to entity activity correlation

3.2 Risk Scoring
Dynamic threat scoring (0-100):
• Severity: CVSS score weighting
• Exploitability: Active exploitation indicators
• Exposure: Entity vulnerability assessment
• Context: Business criticality factor
• Aggregation: Multi-source confidence scoring

4. References

[1] NIST National Vulnerability Database, NIST, 2024
[2] MITRE ATT&CK Knowledge Base, MITRE, 2024
[3] STIX/TAXII 2.1 Specification, OASIS, 2021
[4] AlienVault OTX Documentation, AT&T Cybersecurity, 2024