



ISARA + Microsoft Security Integration Brief

1. Executive Summary

ISARA Advance provides cryptographic discovery and risk prioritization that complements Microsoft security tools. Integration enables enhanced visibility, risk-based remediation, and compliance in Azure and hybrid environments.

2. Integration Overview

ISARA Advance collects telemetry from network traffic, endpoints, databases, and key management systems. Key Microsoft Security tools include:

- **Defender for Cloud:** Cloud security posture and threat protection
- **Azure Security Center:** Continuous assessment
- **Azure Sentinel:** Centralized SIEM and SOAR
- **Defender for Endpoint:** Endpoint detection and response

Integration allows ISARA Advance insights to feed Microsoft Security platforms for unified monitoring.

3. Key Integration Points

- **Azure vTAP:** Mirror VNet traffic; ISARA Network Analyzer ingests network protocol handshake metadata, cipher, and certificate data; insights forwarded to Sentinel.
- **Key Management:** Collect metadata from Azure Key Vault
- **Endpoints:** Agent-based or agentless scans; combined with Defender for Endpoint.
- **Databases/Apps:** TLS and certificate telemetry feeds into posture assessment; correlated with security alerts.

4. Benefits

- Unified cryptographic visibility
- Risk-based remediation prioritization
- Operational efficiency via automated workflows
- Compliance support
- Enhanced detection of weak or quantum-vulnerable cryptography

5. Deployment Recommendations

- Enable vTAP for critical VNets.
- Deploy ISARA Advance collectors for endpoints, databases, and key systems.
- Forward telemetry to Sentinel/Defender.



- Set up dashboards and alerts.
- Regularly review posture scores and remediation actions.

6. Conclusion

ISARA Advance integration with Microsoft Security tools provides actionable cryptographic insights, enhancing risk management, remediation, and compliance in cloud and hybrid environments.