Vehere NDR and SOAR

Automating Threat Response through Seamless Integrations

vehere

WHITEPAPER

VEHERE NDR AND SOAR

Automating Threat Response through Seamless Integrations

Executive Summary

Vehere's Network Detection and Response (NDR) platform seamlessly integrates with leading SOAR systems to automate triage and response. By leveraging enriched threat intelligence, lossless network packet visibility, and orchestrated actions, Vehere enables high-confidence, low-latency threat mitigation across enterprise networks.

Architecture Overview

Vehere NDR acts as a central intelligence layer by inspecting deep network traffic (East-West, North-South, and flow) to detect anomalies via ML and rule-based engines. The platform integrates with SOAR to automate the entire detection-to-response lifecycle.

Integrated Data Sources and Enrichment:

- Threat Intelligence Platforms (TIP/MISP)
- User Identity Platforms (e.g., Active Directory)

Supported Ingestion Mechanisms:

- API
- TAXII/STIX (for threat feeds)

Architecture Components

1. Vehere NDR

- Ingests East-West, North-South, and Flow-based network traffic.
- Applies Deep Packet Inspection (DPI).
- Generates ML and rule-based alerts.

2. SOAR Platform

- Central orchestrator for automated and manual triage.
- Interfaces with multiple subsystems for enrichment and response execution.

3. External Integrations

- TIP / MISP via TAXII for threat feed ingestion.
- User Identity Systems (e.g., AD) via index API calls

SOAR Workflow with Vehere NDR

1. Alert Ingestion and Playbook Trigger

- Alerts from Vehere NDR are ingested via logvehere-alerts-* indexes.
- Automated playbooks are triggered based on alert type and severity.

2. Automated Triage

- Risk scoring, correlation, and contextual validation via API calls.
- Auto enrichment using TIPs, asset context, and identity mapping.

3. Manual Triage (Optional)

- SOC analysts can drill down into session details and payloads (PCAP) using Vehere NDR-provided deep packet data.
- On-demand querying via logvehere-probe-* API endpoints.

4. Notification and Escalation

- SOC notified via email.
- Tickets are generated and actions logged for auditing.

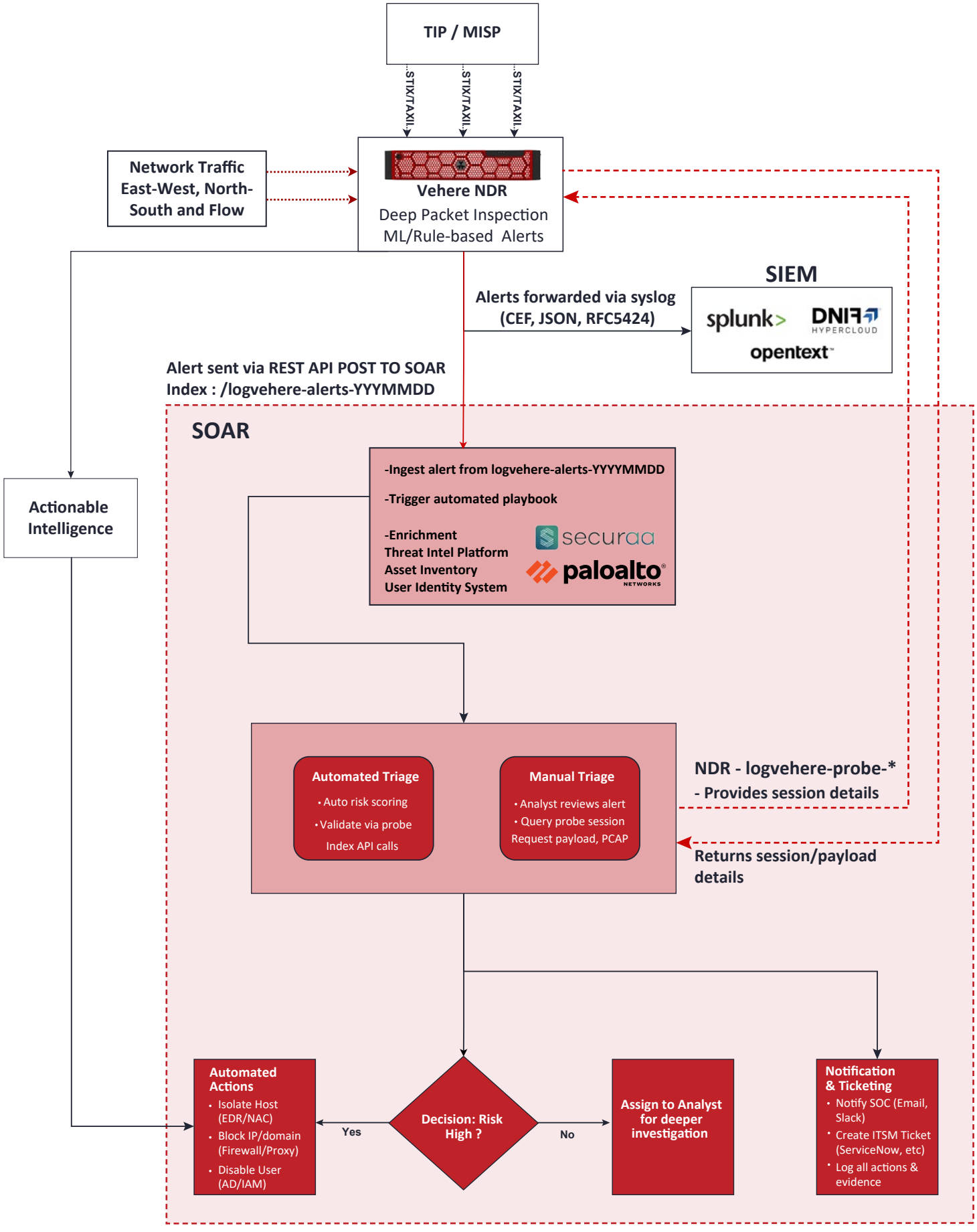

Fig.: Vehere NDR in Action: Ecosystem Integration

End-to-End Flow Description

1. Alert Generation
Vehere NDR generates alerts from deep packet analysis using ML/rule-based models.

2. Alert Ingestion into SOAR

- Alerts are indexed in SOAR from the logvehere-alerts-YYYYMMDD source.
- Ingestion triggers automated playbooks.

3. Triage Phase

- Automated Triage:
  - Performs risk scoring.
  - Validates alerts by querying the Vehere probe using index API calls.
- Manual Triage:
  - Analysts review alerts manually.
  - Option to query Vehere probe for:
    1. Payload
    2. PCAP
    3. Session details
  - Queries are executed via logvehere-probe-* endpoints.

4. Notification and Ticketing

- Alerts are forwarded to SOC via:
  - Email

Key SOAR Integrations

Component	Role in Integration
Active Directory, LDAP, LDAPS,OpenLDAP	User identity mapping, account disablement
TAXII/TIP Feeds/STIX	External threat intelligence enrichment
Email	SOC notification and case management

Business Outcomes

- Faster Detection and Containment: Real-time detection feeds into SOAR workflows for immediate action, reducing dwell time and risk of exposure.
- Reduced Analyst Workload: Automated triage and contextual enrichment eliminate redundant tasks, allowing teams to focus on advanced investigations.
- Audit-Ready Investigations: Every step is logged and ticketed, enabling compliance tracking and retrospective analysis.
- Scalable Response Framework: Unified playbooks adapt to varied environments without increasing analyst overhead or complexity.

Technical Summary

- Data Sources: Vehere NDR ingests raw traffic and alerts; SOAR enhances context via integrated feeds.
- APIs Used: logvehere-alerts-*, logvehere-probe-*, and index-level enrichment APIs.
- Response Logic: Conditional workflows with automated and analyst-driven branches.
- Enrichment Stack: TIP, asset register, user identity systems.

Conclusion

Vehere's integration with SOAR platforms transforms threat response from reactive to proactive. By embedding deep packet intelligence into automated workflows, security teams gain faster, more accurate, and cost-effective threat mitigation capabilities - critical to today's high-stakes cyber landscape.