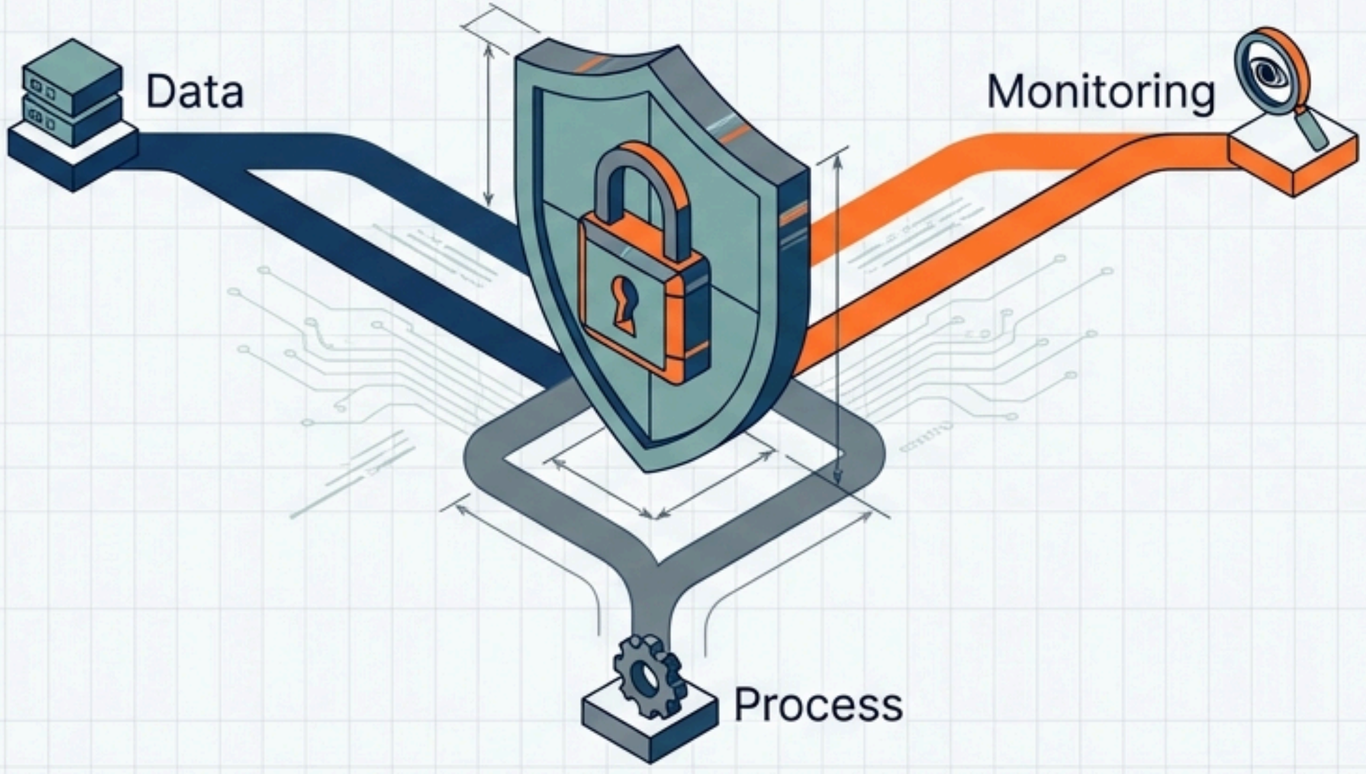
Engineering Editorial

Hybrid Enterprise DLP Architecture

Integrating Microsoft Purview, SOC Visibility, and Offensive Validation for Resilient Data Defense.

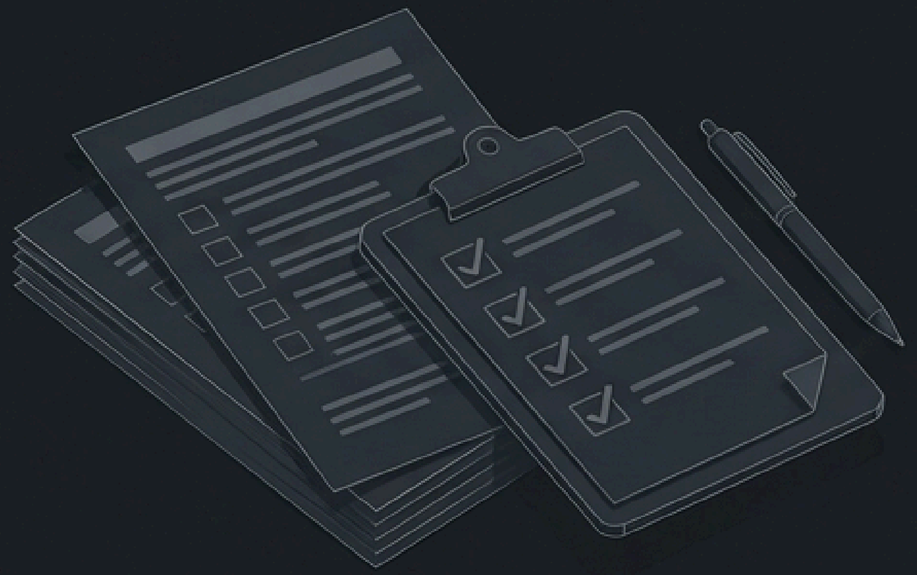


Author: Mohamed AZZAM
Context: AXA / AXA GBS Project
Version: 1.0 (Implementation & Validation)

NotebookLM

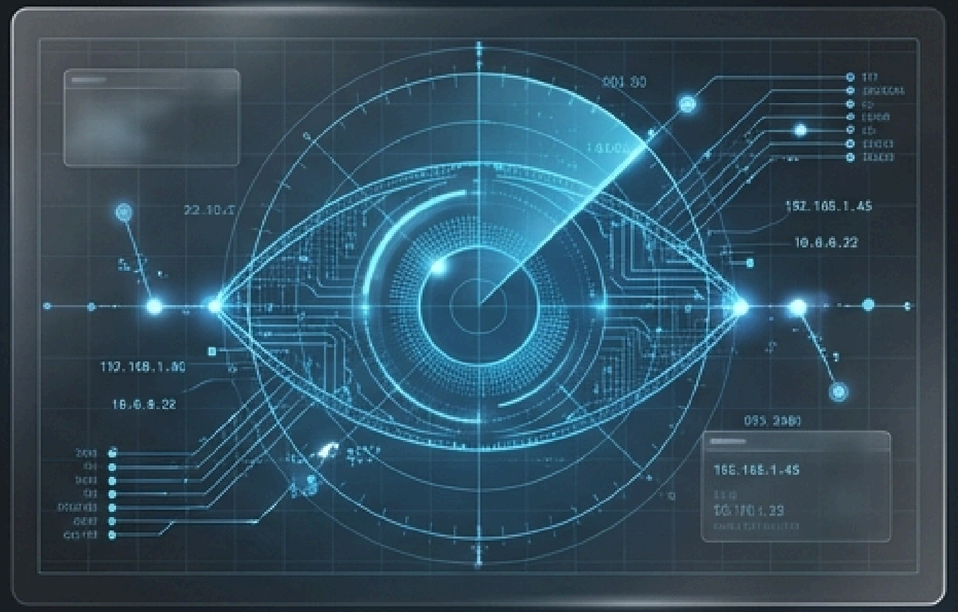
THE GAP BETWEEN THEORY AND REALITY

THEORETICAL DLP



- Focus on Compliance Checkboxes
- Rules exist but are unseen
- No proof of resilience

OPERATIONAL DLP

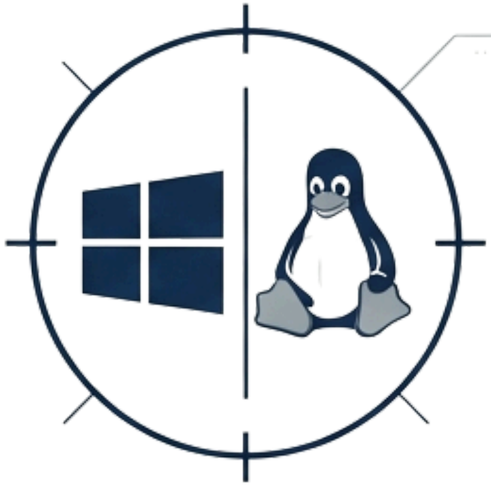


- Know Your Data
- Continuous Monitoring (SOC/Logs)
- Offensive Validation
- Workflow Escalation

"You cannot protect what you cannot see."

SIMULATING THE ENTERPRISE SECURITY OPERATIONS CENTER

A functional replication of a real-world DLP ecosystem, spanning classification, detection, correlation, and governance.



1. Hybrid Detection

Cross-platform engines (Windows 11 + Linux) utilizing Python, Bash, and Snort for comprehensive coverage.

2. Zero Trust Identity

Integration with Microsoft Entra ID (MFA & Conditional Access) to enrich alerts with identity context.

3. D+1 Governance

Full lifecycle workflow for incident escalation and automated Security Incident Report (SIR) generation.

METRIC: Validated against offensive campaigns (Kali Linux) with Mean Time to Detect (MTTD) < 30 seconds.

NotebookLM

The v3 Architecture: A Five-Layer Defense Stack

Layer 1: Identity

Microsoft Entra ID | MFA | Context Score (Ic)

Layer 2: Endpoint

Windows 11 Enterprise | Kali Linux ' Internal IPs (192.168.100.x)

Layer 3: Detection

Python DLP Engine ' Snort 3 IDS | Wazuh FIM

Layer 4: Correlation

Wazuh Manager | OpenSearch | Rule 100010

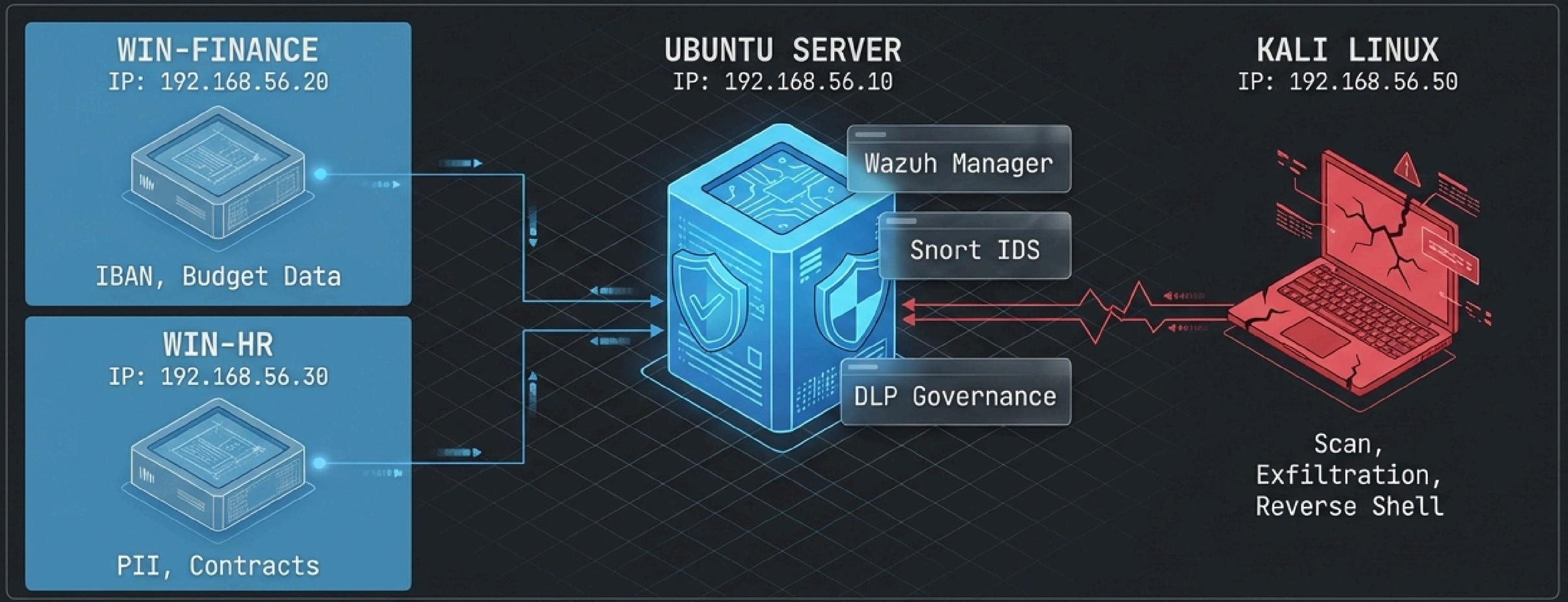
Layer 5: Governance

Flask/React Platform | Risk Scoring ' D+1 Queue

NotebookLM

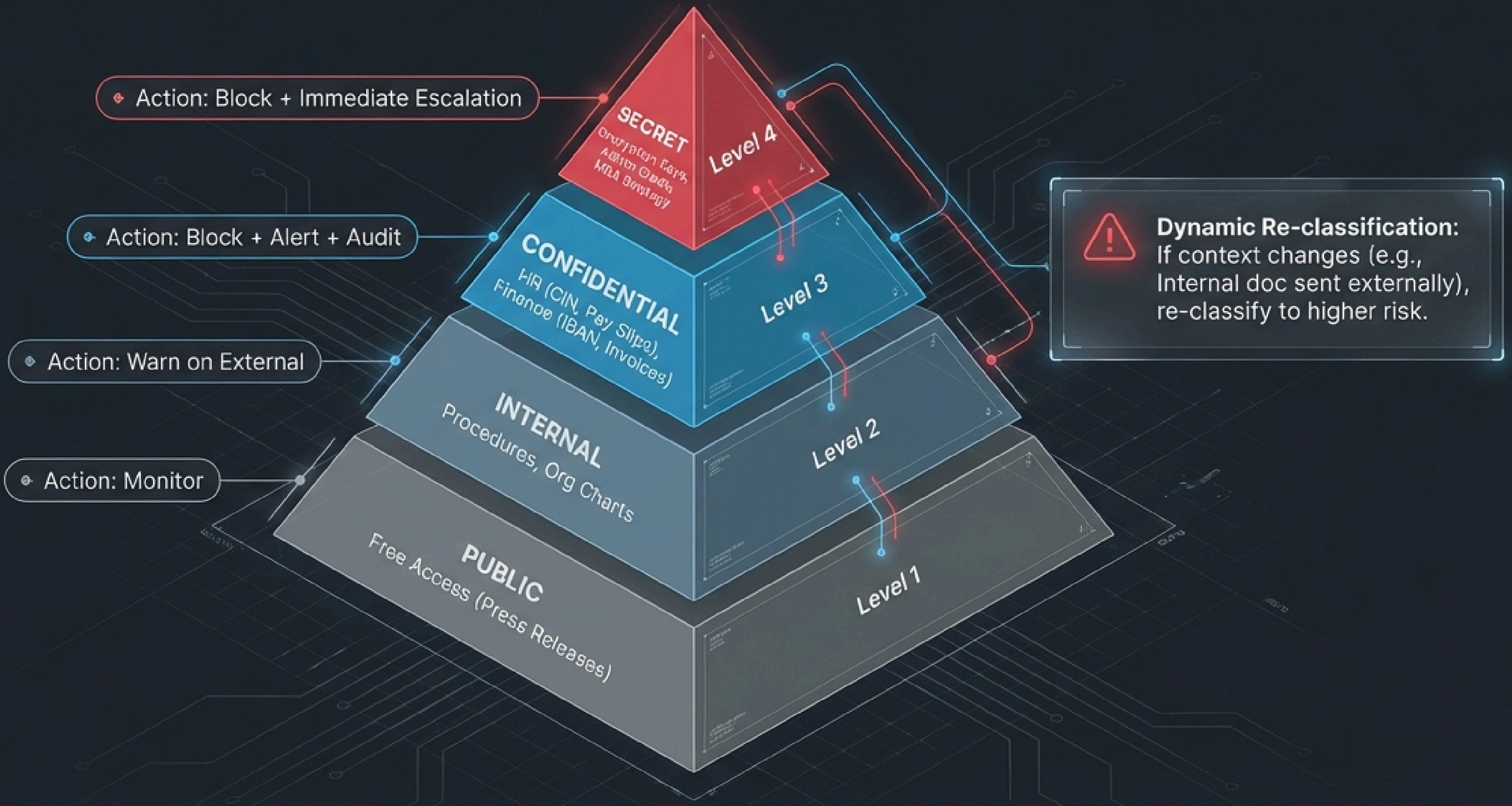
The Operational Architecture

VMware Host-Only Network (Subnet 192.168.56.0/24)

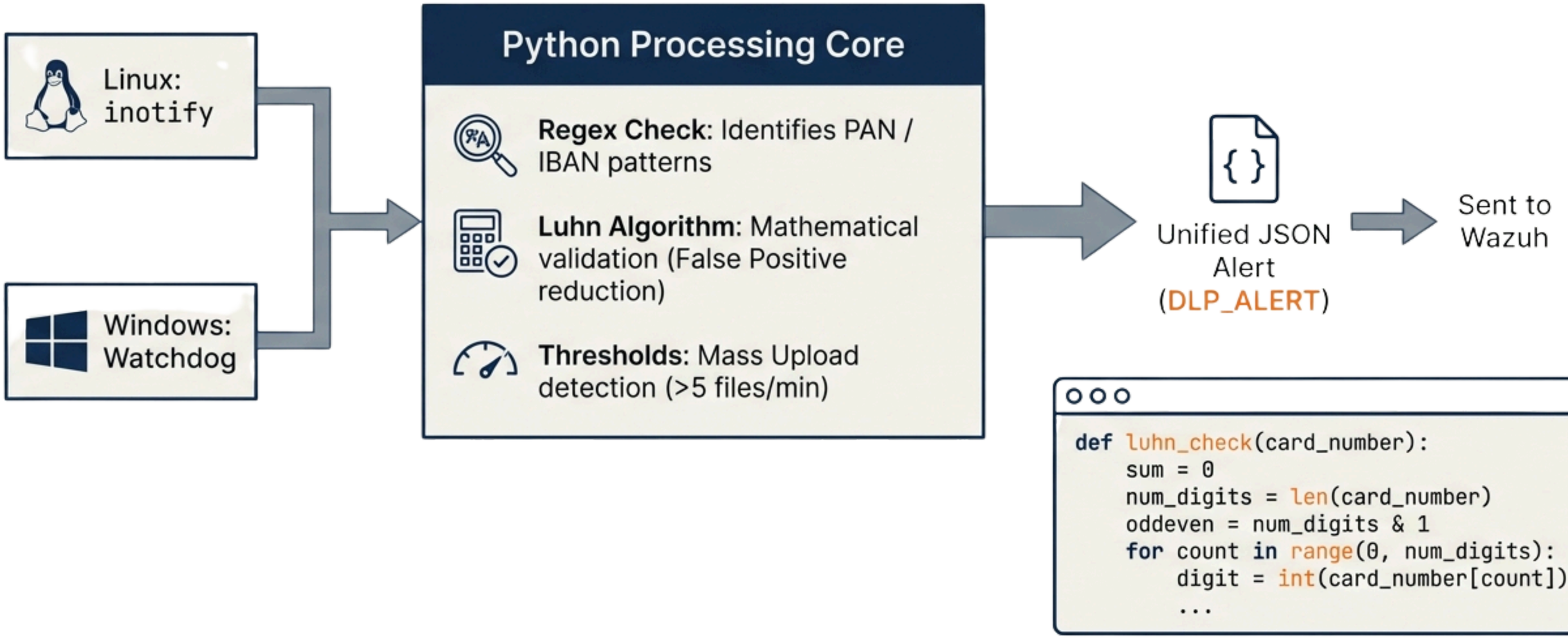


Infrastructure built on VMware Workstation Pro.

Data A: Data Classification Taxonomy



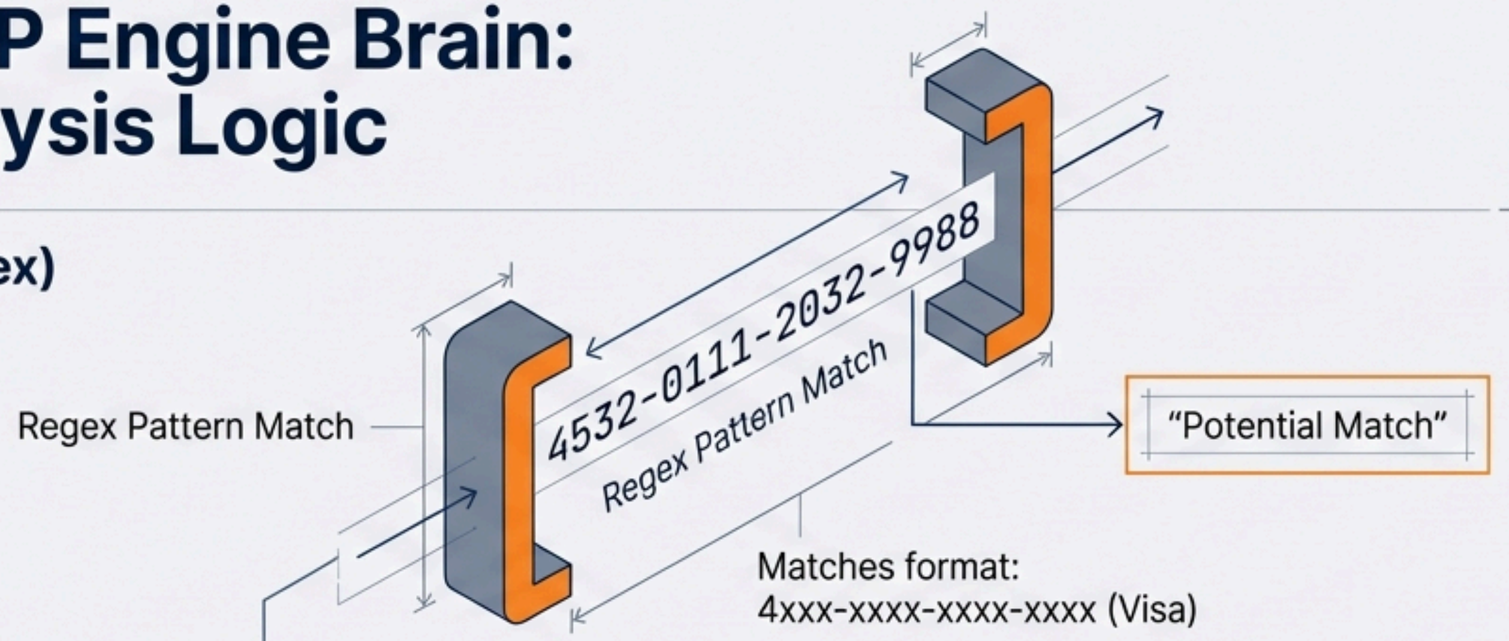
The DLP Engine: Cross-Platform Logic



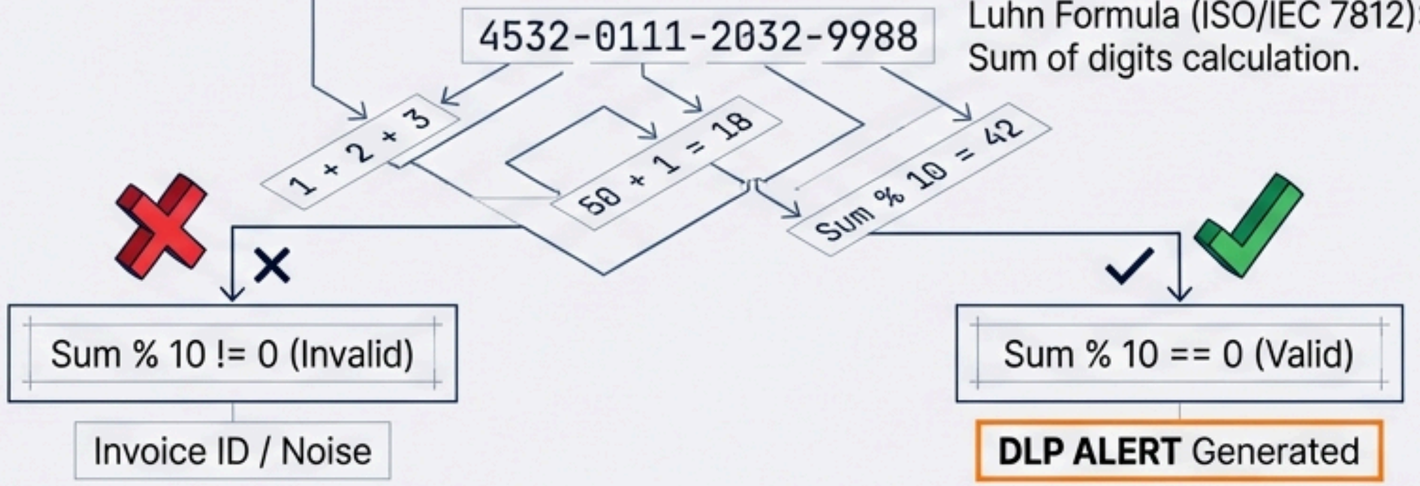
NotebookLM

Q2 — The DLP Engine Brain: Content Analysis Logic

Step 1: The Net (Regex)



Step 2: The Filter (Luhn Algorithm)



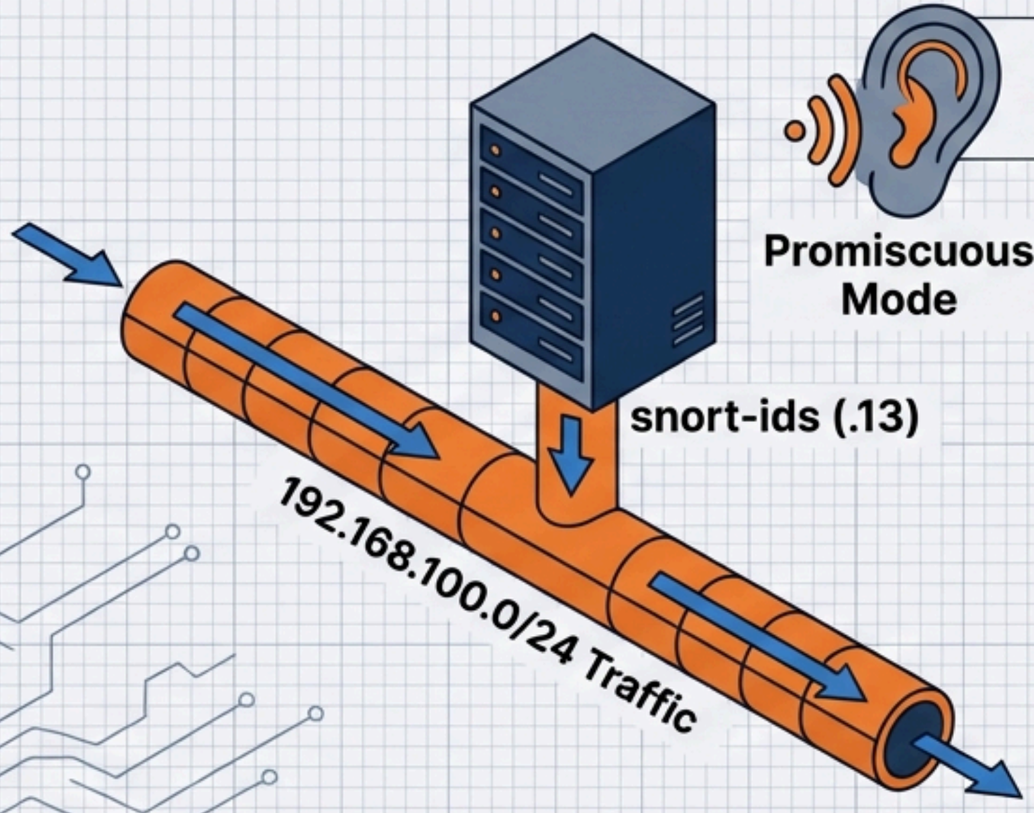
Without Luhn, an invoice number like "4532..." triggers a false positive.

With Luhn, only valid PANs trigger.

KEY INSIGHT: Regex casts the net; Luhn checks the fish.

NotebookLM

Q5 — The Network Layer: Snort IDS Visibility



Listening to **ALL** traffic, not just traffic addressed to itself.

Packet A: SSH (Admin)	Small Packets, Interactive	**IGNORED**
Packet B: SCP (Exfiltration)	Bulk Data Transfer, Port 22	**ALERT** SID 2000001

KEY INSIGHT: In Promiscuous mode, Snort inspects every packet on the subnet, distinguishing suspicious bulk data transfers (SCP) from standard SSH.

NotebookLM

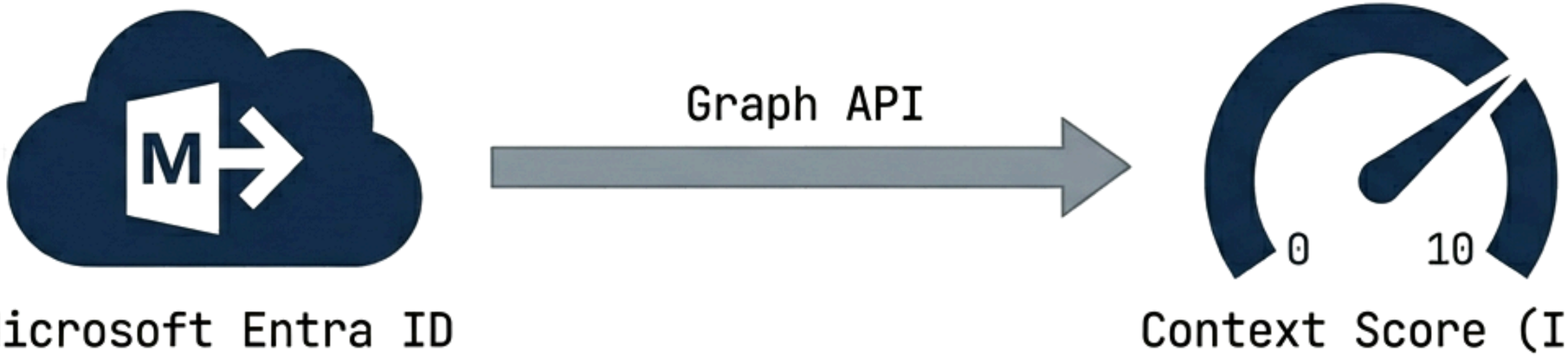
The Pivot Point: Multi-Source Correlation

Wazuh Rule ID: 100010

Transforming two independent ‘suspicious’ events into one ‘confirmed’ exfiltration attempt.

NotebookLM

Layer 3: Identity & Zero Trust Context



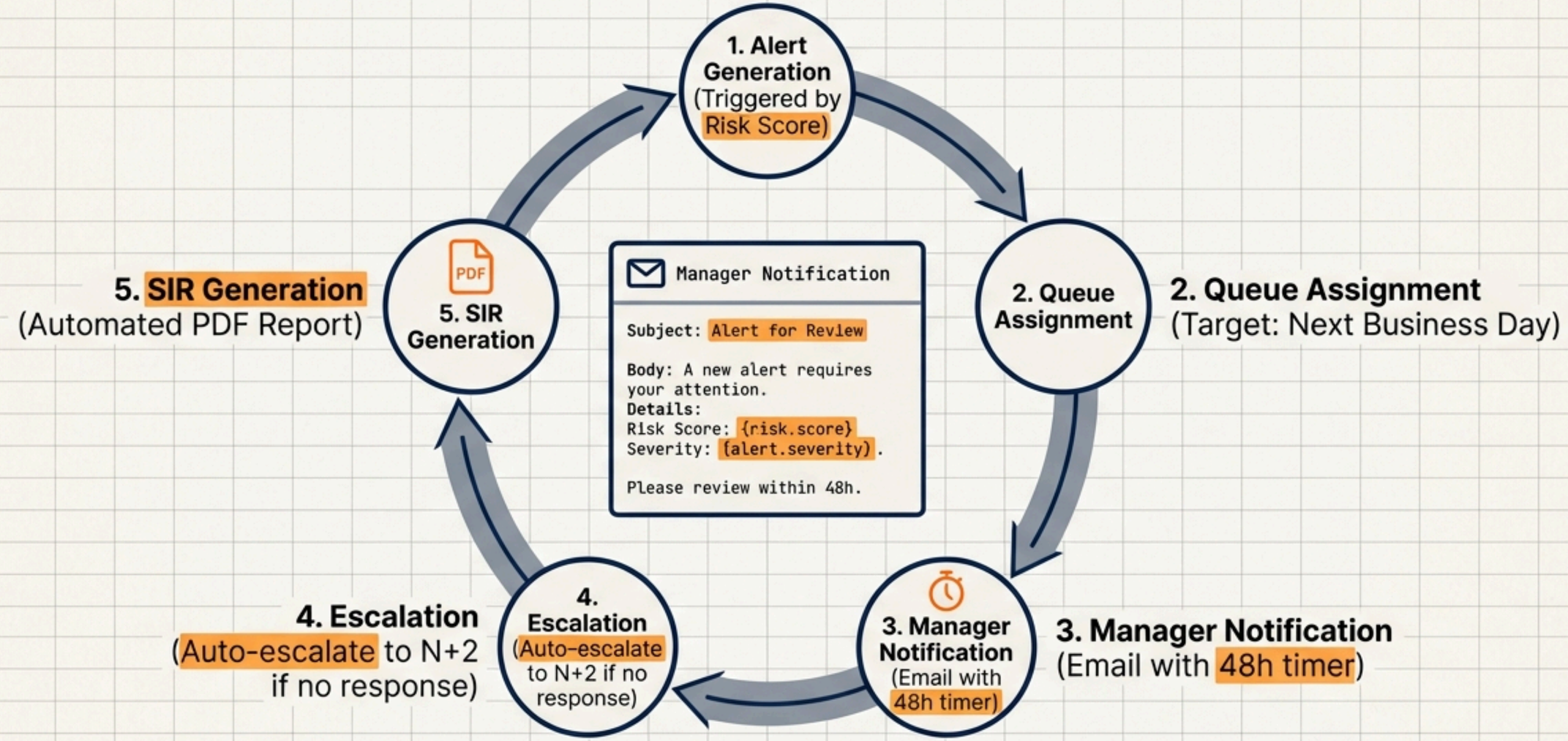
Identity Context Score (Ic)

- **+4 Points**: MFA Missing (Policy Violation)
- **+4 Points**: Conditional Access Blocked (Device/IP mismatch)
- **+3 Points**: Unrecognized Location
- **+2 Points**: High-Privilege Account

Context is King. A file access by an admin without MFA is treated differently than a standard access.

NotebookLM

Governance Operations: The D+1 Workflow



NotebookLM

Offensive Validation: The Attack Matrix

Linux Vectors

A. Attack: Nmap Recon → Detection: Snort 2000030 (<60s)

B. Attack: SCP Exfiltration → Detection: Rule 100010 (<30s)

Windows Vectors (v3)

A. Attack: SMB Brute Force (Hydra) → Detection: Event ID 4625 (Burst)

B. Attack: PowerShell Reverse Shell → Detection: Event ID 4688 + Snort

100% Attack Chain Correlation Achieved in v3 Testing.

Notebook

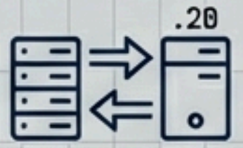
Scenario Deep Dive: The Exfiltration Chain

Attacker Actions

T+0s: Nmap Scan initiated

T+10s: SSH Login
(Brute Force/Creds)

T+15s: Copy
fiche_bancaire_SECRET.txt



T+20s: SCP Transfer to .20

System Response

T+5s: Snort Alert (SYN Scan)

T+11s: Wazuh Auth Log (Login)

T+16s: FIM Alert + DLP Engine
(Luhn Check Passed)

T+21s: Correlation Rule 100010
Triggered (CRITICAL)

NotebookLM

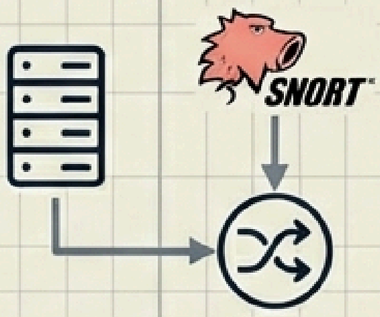
Architectural Evolution: v1 -> v3

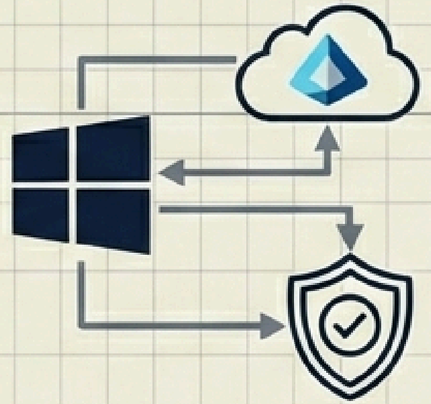
100% Attack Chain Correlation achieved.

Final v3

Enhanced v2

Baseline v1





Blind to network traffic, no correlation. SCP Exfiltration Invisible.

Snort added + Correlation. MTTD reduced by 10x.

Windows Ent. + Entra ID + Governance. Full Contextual Awareness & Zero Trust Alignment.

Notebookl

Conclusion & Future Evolution

The v3 Architecture successfully correlates Identity, Endpoint, and Network signals to detect sophisticated insider threats.

Current State

- Passive Detection
- Alerting & Governance
- Manual Remediation

Future State

- SOAR Integration (Active)
- AI Anomaly Detection
- Automated Block (Account Disable)

Detection is robust. The next frontier is automated remediation.

NotebookLM

Conclusion: Secure by Design

We built a Hybrid, Governed, Validated architecture.
Security is not a product; it is a process of continuous validation.
Result: A system that doesn't just alert—it protects and evolves.

Proceed to Phase 4 (Identity Integration).

NotebookLM