DAYANANDA SAGAR
UNIVERSITY

HYBRID THREAT DETECTION SYSTEM

Fusing Network Intrusion Detection & User Behavior Analytics on AWS

Aarit Haldar | USN: ENG24CY0073 | Priyanshu Sithole | USN: ENG24CY0189 | Jay Bhagar | USN: ENG24CY0179

THE REALITY OF MODERN CYBER THREATS

EXTERNAL INTENSITY

- DDoS Attacks
- Brute Force Attempts
- High-Volume Intrusions
- Signal: Network Packets

INTERNAL SUBTLETY

- Compromised Credentials
- Insider Threats
- Anomalous Access Patterns
- Signal: User Behavior

THE CHALLENGE: Simultaneous vectors require simultaneous monitoring.

THE FAILURE OF SILOED SECURITY

Network Tools

Detects Traffic Volume

MISSES INSIDER THREATS

User Behavior Tools

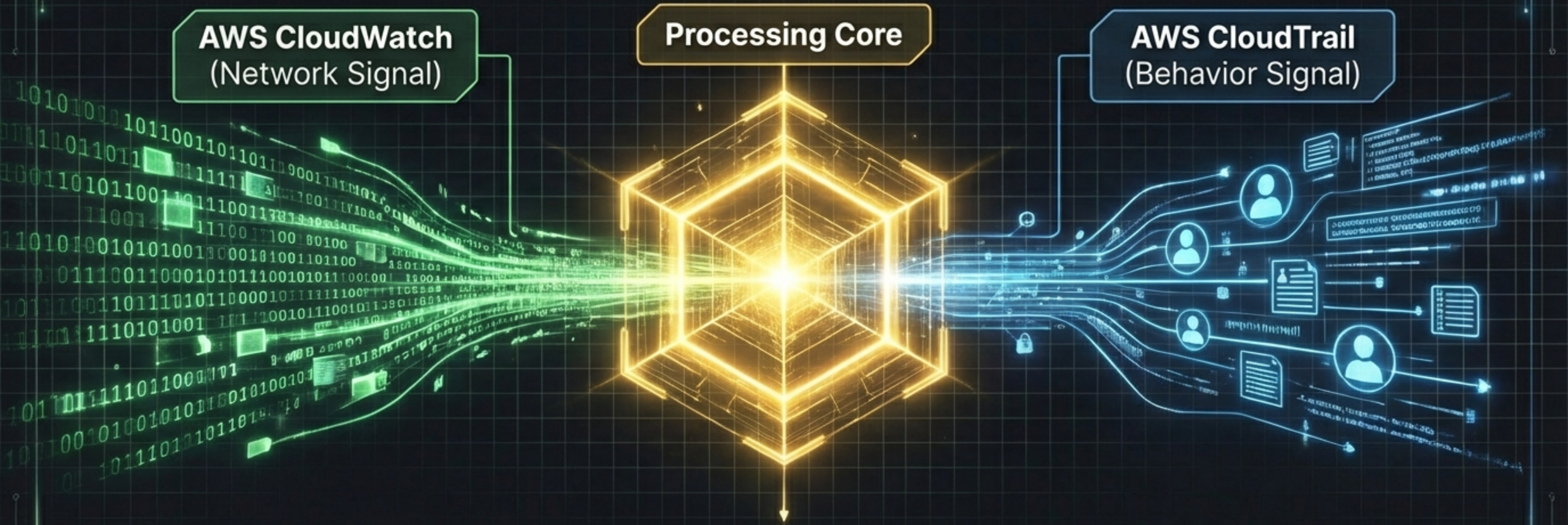
Detects Login Anomalies

MISSES DDoS ATTACKS

THE BLIND SPOT

- High False Positives (15-20%)
- Delayed Detection (>60 Seconds)
- Zero Correlation

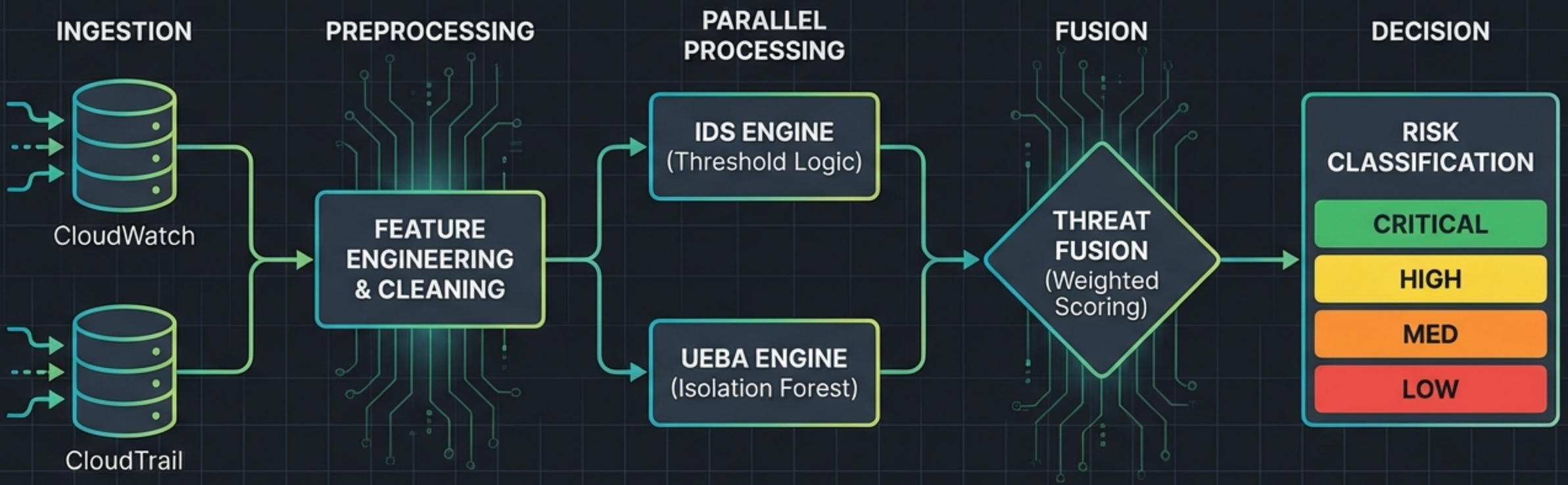
THE SOLUTION: CYBER-PHYSICAL FUSION



REAL-TIME CORRELATION ENGINE

10-SECOND MONITORING CYCLES

SYSTEM ARCHITECTURE



DEEP DIVE: NETWORK INTRUSION DETECTION (IDS)

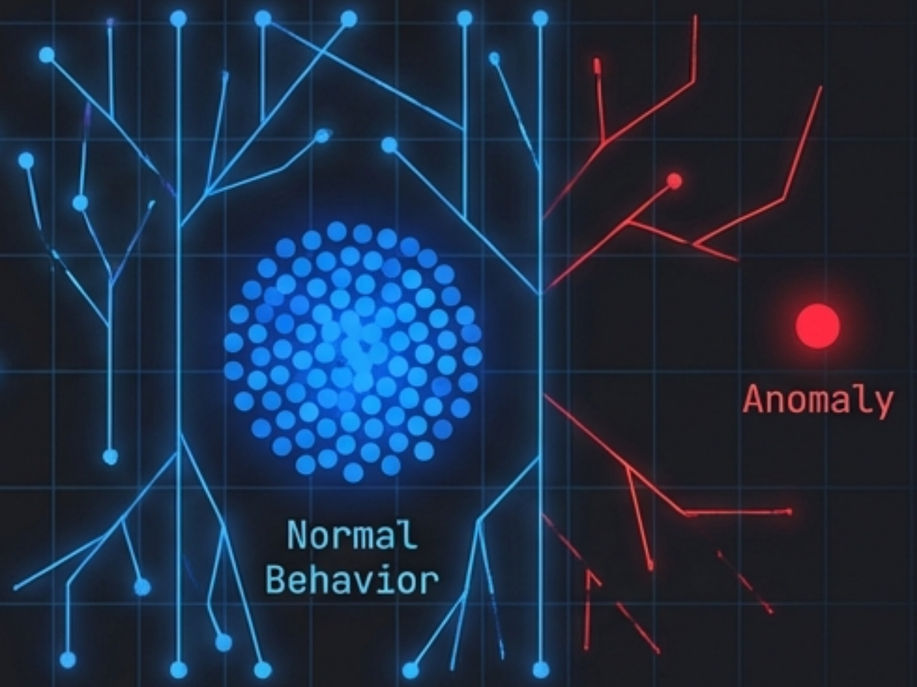
Source: AWS CloudWatch (EC2)
Metric: NetworkIn (Bytes)
Metric: NetworkPacketsIn (Count)

GOAL: IMMEDIATE VOLUMETRIC DETECTION (DDoS)

DEEP DIVE: USER & ENTITY BEHAVIOR ANALYTICS (UEBA)

Source: AWS CloudTrail (S3 JSON Logs)

Features: Time, Activity Volume, Service Diversity



Algorithm: Isolation Forest

Output: Normalized Risk Score (0 - 1)

THE FUSION ALGORITHM: WEIGHTED RISK SCORING

$$Final\ Risk = (0.6 \times Network\ Risk) + (0.4 \times User\ Risk)$$

60% WEIGHT: Network threats have immediate infrastructure impact.

40% WEIGHT: Behavior provides context but manifests slower.

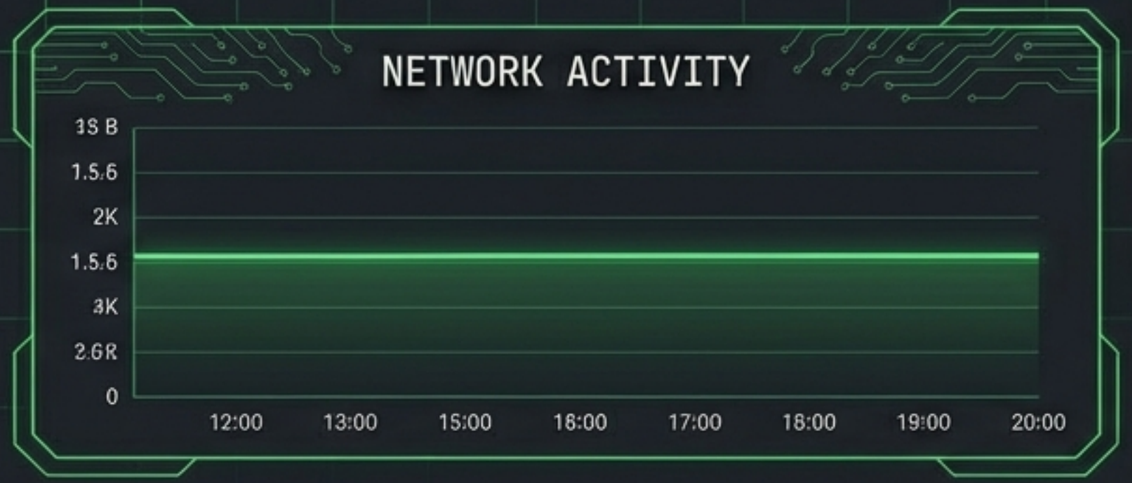
LOW (<0.4) → MEDIUM (>0.4) → HIGH (>0.6) → CRITICAL (>0.8)

EXPERIMENTAL SETUP & DATA

Dataset 1 (Network):
5-minute rolling windows via CloudWatch API.

Dataset 2 (Behavior):
'Current Day' JSON logs filtered for speed.

SCENARIO A: NORMAL OPERATION



Network In:
~15.6 KB

Packets:
78

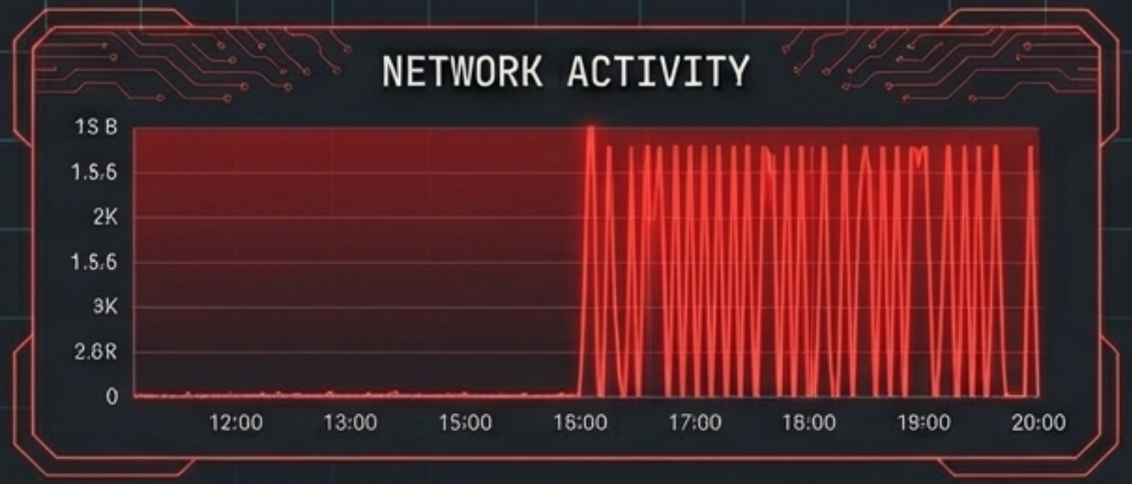
Network Risk Score:
0.05

User Risk Score:
0.10

FINAL RISK: 0.07 (LOW)

False Positives: 0

SCENARIO B: THE ATTACK (DDoS SIMULATION)



Network In:
~1,751,904 Bytes
(111x Increase)

Packets:
~21,189
(271x Increase)

Network Risk Score:
0.95
(CRITICAL)

User Risk Score:
0.10
(NORMAL)

FINAL RISK: 0.61 (HIGH)

Detection Latency: ~20 Seconds

PERFORMANCE SUMMARY: PEACE VS. WAR

NORMAL STATE		ATTACK STATE	
Bytes	15,685	Bytes	1.75 MB
Packets	78	Packets	21,189
Network Risk	0.05	Network Risk	0.95
Final Risk Score	0.07	Final Risk Score	0.61

RESULT: 0% False Positives with accurate Threat Identification.

BRIDGING THE RESEARCH GAP

Siloed Approaches

Literature focuses on Network OR Behavior. We fused both.

Theory vs. Practice

Most papers are theoretical frameworks. We built a live AWS-Native system.

Detection Speed

Standard is 60s. We achieved 10-20s.

BENCHMARKING AGAINST LITERATURE

Metric	Literature Standard	Our System	Status
Detection Time	30-60s	10-20s	✓ Faster
False Positive Rate	15-20%	0%	✓ Eliminated
Monitoring Cycle	1-5 min	10 sec	✓ Real-time
Architecture	Generic/Theoretical	AWS-Native	✓ Applied

UNIQUE TECHNICAL CONTRIBUTIONS

True Data Fusion

Combining raw metrics and logs, not just algorithm outputs.

Live Validation

Tested on 1,242x traffic spike attacks, not just synthetic datasets.

Optimized Processing

CloudTrail “Current Day” filtering reduced processing to ~3 seconds.

LIMITATIONS & FUTURE ROADMAP

CURRENT LIMITATIONS

- Single EC2 Instance Monitoring
- Threshold-based Network IDS
- Inherent CloudTrail Log Delays

FUTURE ROADMAP

- Multi-Region Deployment & Aggregation
- Automated Active Blocking (IPS)
- SNS Integration for Email Alerts

DAYANANDA SAGAR UNIVERSITY

CONCLUSION

1. **SILOS ELIMINATED** through Hybrid Data Fusion.
2. **SPEED MAXIMIZED** with <20 Second Detection.
3. **SCALABILITY PROVEN** via Cloud-Native Architecture.

A Production-Ready Proof of Concept.