The National Technical Research Organisation - SIH25238 - SMART INDIA HACKATHON 2025

adAPT*

APT Detection in ELK: Behaviour-Driven Threat Rules for Stealthy Adversaries

Presented by Dedsec_01

National Technical Research Organisation - TEAM DEDSEC_01

01

Problem Statement

Development of Threat rules in ELK Stack for detecting Advanced Persistent Threats (APTs).

The Problem:
Governments face APT attacks that:

- Stay hidden for months
- Use legit tools (PowerShell, WMI, RDP)
- Leave almost no traditional indicators
- Evade commercial SIEM rules
- Blend into normal network noise

SMART INDIA HACKATHON 2025

Impacts of APT's

Advanced Persistent Threats (APTs) are highly targeted, long-term cyberattacks designed to quietly infiltrate systems and steal sensitive data. Their stealth and sophistication make them extremely dangerous, causing major financial, operational, and national-security risks.

01.

Severe Financial & Operational Damage

- APT incidents cost organizations $4.5M+ on average.
- They require nearly 280 days to detect and contain, causing prolonged exposure.

02.

High Targeting of Government & Critical Sectors

- More than 40% of APT campaigns focus on government, defense, and national infrastructure.
- Leads to loss of classified data, espionage, and disruptions in essential services.

03.

Long-Term Data Exposure & Espionage Risk

- APT groups maintain access for months to years, exfiltrating sensitive data silently.
- Over 60% of compromised systems show repeated re-entry attempts even after cleanup.

National Technical Research Organisation - TEAM DEDSEC_01

SMART INDIA HACKATHON 2025

The Threat is Real and Growing

Impact of APT36 on India

- **116,374 attacks recorded (Apr–Aug 2025):** Global Cyber Alliance sensors in India logged 116,374 APT36-linked incidents across 75 Pakistan-based ASNs, showing massive, sustained targeting. [source]

- Attack peak of **~26,000/day: On April 30, 2025,** India saw a spike of nearly 26,000 APT36-linked incidents in a single day, highlighting the scale of their operations.[source]

- High-value targets: As per a 2025 DSCI advisory, APT36 has targeted **Indian government ministries, defence, aerospace,** and critical infrastructure, mainly through spear-phishing and fake government-themed lures.[source]

- Shift to **cross-platform malware:** Recent campaigns use Golang-based backdoors and Linux-targeting malware, enabling infiltration into non-Windows systems used in Indian defence and government networks.[source]

Our Solution

APT Detection System

01 Identifying APT behaviours — Studied **common TTPs (MITRE ATT&CK)** like privilege escalation, lateral movement, and data exfiltration.

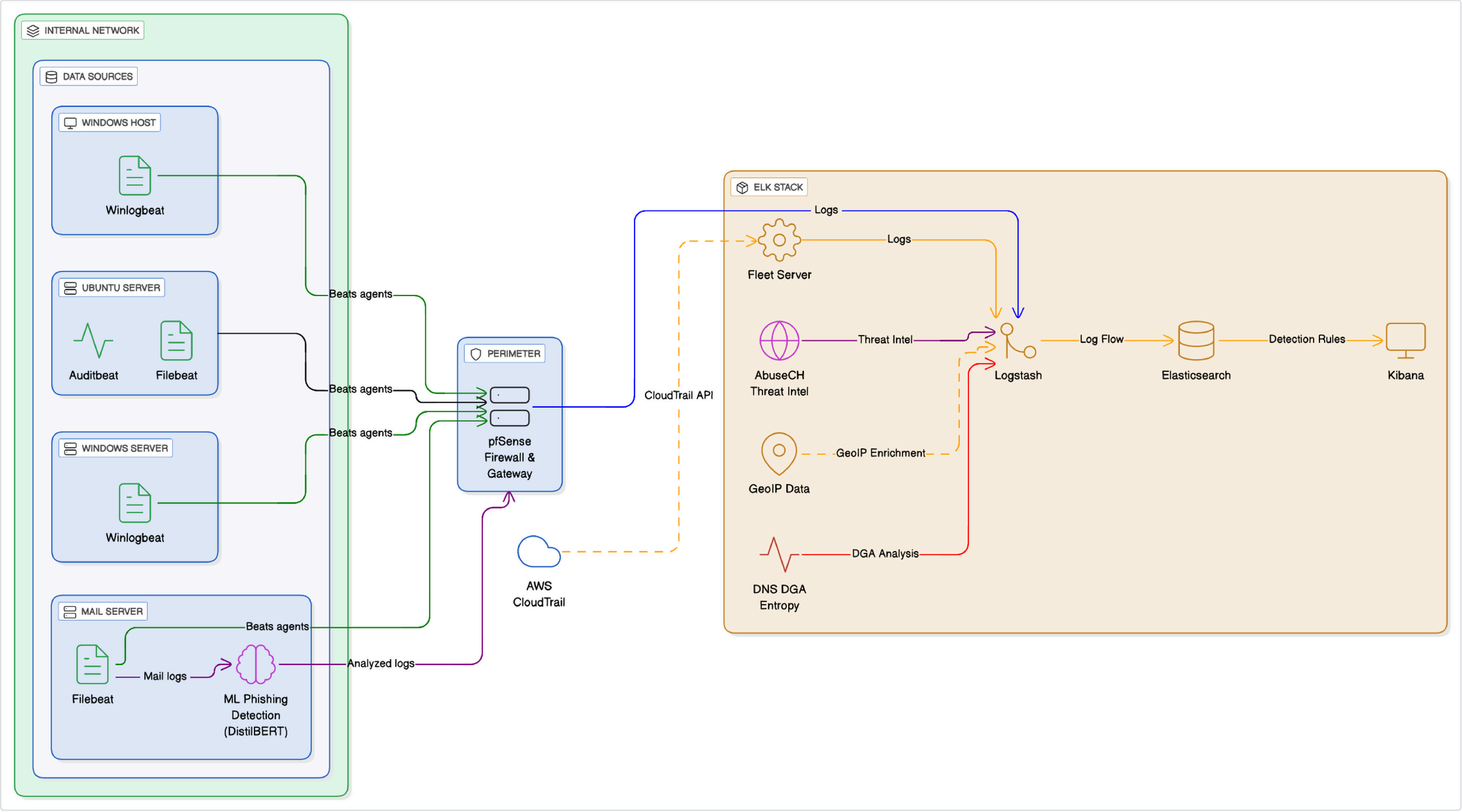
02 Mapping logs to attacks — Understood what log sources **(Windows Event Logs, Sysmon,Firewall,Authentication log**s) are required to detect APT patterns.

03 **Selecting critical detections** — Prioritized rules for credential access, persistence mechanisms, suspicious processes, and unusual network activity.

04 **Designing ELK pipelines** Planned how logs flow from Logstash → Elasticsearch → Kibana for real-time visibility.

05 **Building detection rules** — Used Sigma-like logic to create correlation rules for anomalies, rare events, and repetitive behaviours.

06 Creating dashboards & alerts **Built visualizations to track attack stages** and configured alerts for high-risk activity.



INTERNAL NETWORK

DATA SOURCES

WINDOWS HOST

Winlogbeat

UBUNTU SERVER

Auditbeat

Filebeat

WINDOWS SERVER

Winlogbeat

MAIL SERVER

Filebeat

Mail logs

ML Phishing Detection (DistilBERT)

Beats agents

Beats agents

Beats agents

Beats agents

Analyzed logs

PERIMETER

pfSense Firewall & Gateway

AWS CloudTrail

CloudTrail API

ELK STACK

Logs

Fleet Server

Logs

AbuseCH Threat Intel

Threat Intel

GeoIP Data

GeoIP Enrichment

DNS DGA Entropy

DGA Analysis

Logstash

Log Flow

Elasticsearch

Detection Rules

Kibana

06

Why Our Solution Stands Out

01 **Purpose-built for APT detection**
Unlike generic SIEM dashboards, our setup is specifically designed to detect long-term, stealthy APT behaviours, not just basic anomalies.

02 **Multi-source log correlation**
We combine Windows, Linux, Firewall, CloudTrail, DNS, and Threat Intel — giving deeper visibility than single-source detection systems.

03 **Threat-intelligence enriched**
Our pipeline integrates AbuseCH, GeoIP, and DGA entropy analysis, enabling faster identification of malicious IPs, C2 patterns, and risky domains.

04 **Custom detection rules**
Instead of relying on default ELK alerts, we created hand-crafted, attack-mapped rules aligned with MITRE ATT&CK, improving precision and reducing noise.

05 **Real-time monitoring with actionable dashboards**
Our Kibana visualizations show attack stages, severity, timelines, and IOC correlations, making incident investigation far more intuitive.

06 **Scalable, open-source, and cost-efficient**
Because the entire system uses open tools and optimized pipelines, it delivers enterprise-grade detection without enterprise-grade cost.

07 **Fully Offline, On-Prem Deployment**
Unlike cloud-dependent SIEMs, our entire ELK stack runs offline on a repurposed laptop, making it:

08 **Precise MITRE ATT&CK Mappings**
Our detection rules are directly mapped to high-impact MITRE techniques such as:

- T1059 – Command Execution, T1078 – Valid Accounts Misuse
- T1047 – WMI Execution, T1566 – Phishing Indicators
- T1027 – Obfuscated Scripts, T1110 – Brute Force Attempts

Solution / Approach	Deployment	MITRE Mapping	ML / UEBA	Strengths	Weaknesses
Our Project — AdAPt	On-prem, fully offline (Proxmox on repurposed laptop)	✓ Hand-mapped rules to MITRE techniques (APT36 focus)	✓ Targeted ML (email phishing classifier, DNS entropy, beacon clustering)	Air-gapped realism; full transparency; low-cost reproducible POC; focused on low-and-slow APT TTPs	Limited scale & retention; no 24×7 human monitoring; hardware constrained
Splunk Enterprise Security	Cloud / On-prem (enterprise)	✓ (commercial MITRE alignment available)	✓ Strong analytics & ML apps	Extremely mature, rich app ecosystem, high scale & polished workflows. (Splunk)	Very costly; complex to tune; not ideal for air-gapped testbeds
Elastic Security (Elastic commercial)	On-prem / Cloud (built on ELK)	✓ Built-in detection engine & ATT&CK mapping docs	✓ Detection engine + analytics	Fast search, storage efficiency, SIEM features built into ELK ecosystem. Good fit for rule engineering. (Elastic)	Commercial features behind subscription; needs tuning
Microsoft Sentinel	Cloud-native (Azure)	✓ MITRE-aware analytics & playbooks	✓ Heavy AI / automation focus	Massive cloud scale, automation, native MS signals and many connectors — great for cloud APT hunts. (Microsoft Learn)	Cloud-only model; not suitable for air-gapped/on-prem offline labs; cost can grow with ingestion
CrowdStrike (Falcon + Falcon Complete MDR)	Agent + Cloud	✓ Endpoint TTP mapping	✓ Strong EDR ML & detection	Industry-leading EDR, quick containment, human hunting via managed service. (crowdstrike.com)	Recurring service cost; cloud dependency; less transparent internals
Arctic Wolf (MDR)	Cloud + managed service	Varies (TI + playbooks)	✓ Behavioral analytics + AI	Human-led hunting, SOC-as-a-service, fast MTTD improvement. Good for organizations that outsource SOC. (Arctic Wolf)	Ongoing cost; not an on-prem/offline solution
Wazuh (Open source)	On-prem / Cloud (OSS)	You implement	You implement (rules + integrations)	Open source XDR/SIEM, strong community, lightweight for on-prem usage — realistic alternative for labs. (Wazuh)	Requires engineering time to tune & maintain

Impacts

Security

- Reduces mean time to detect (MTTD) APTs from months to hours through automated rule-based detection
- Provides comprehensive visibility across the entire APT attack lifecycle with correlated threat intelligence

Operational

- Enables real-time monitoring of critical assets and detection of sophisticated attack patterns
- Reduces false positives through context-aware rules and threat correlation

Compliance

- Helps organizations meet security monitoring requirements for ISO 27001, NIST, and other frameworks
- Provides audit trails and forensic capabilities for incident investigation

Economic Benefits

- **Reduced Breach Costs:** India's average breach cost in 2025 is **₹22 crore**; faster APT detection can reduce this by up to 38%, saving **₹6–8 crore per incident.**
- **Lower Operational Losses:** Early detection prevents system downtime, **avoiding ₹1.5–3 crore in** productivity losses for mid-to-large organizations.
- **Reduced Incident Response Costs:** Automated ELK-based detection cuts IR effort by **25–35%**, lowering the need for expensive forensics teams.
- **Lower Long-Term Security Spend:** Proactive threat rules reduce dependency on external MDR/SOC escalation, saving **15–20% annually** on security operations.
- **Avoided Reputational Damage:** Faster containment reduces customer churn and trust loss, protecting an estimated **₹50–80 lakh in brand value** per incident.

09 Business Plan

Revenue Model

- Subscription-Based Rule Packs
  - Monthly/annual subscription for updated APT detection rules.
- Managed Detection Service (MDR) Add-on
  - Organizations pay for continuous monitoring + alert tuning.
- Enterprise Licensing
  - One-time + annual maintenance for large deployments.
- Custom Rule Development
  - Premium service for organization-specific threat models.

Market Opportunity

- India's average breach cost reached ₹22 crore in 2025 — early APT detection cuts this by 38% (IBM).
- Indian cybersecurity market projected to hit USD 10 billion by 2027, with SIEM tools growing at 12% CAGR.
- Over 40% of cyberattacks on India are APT-style or targeted espionage, increasing demand for advanced detection capabilities.

Competitive Edge

- ELK is open-source, lowering deployment cost by 60–70% vs. commercial SIEMs.
- Rule sets are custom-built for Indian threat landscape, including groups like APT36, APT22, SideWinder, etc.
- Faster tuning, localization, and tailored threat-intel compared to generic global vendors.

SIH 2025

10

RESEARCH AND REFERENCES

Primary Standards and Frameworks:

- 1. MITRE ATT&CK Framework – "Enterprise Tactics, Techniques & Procedures" – https://attack.mitre.org
- 2. NIST Special Publication 800-61 – "Computer Security Incident Handling Guide" – https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- 3. Cyber Security Guidelines for APT Detection – CERT-IN, Ministry of Electronics and Information Technology – https://www.cert-in.org.in

Academic Research:

- 4. APT-LLM: Embedding-Based Anomaly Detection of Cyber Advanced Persistent Threats Using Large Language Models, arXiv 2025: https://arxiv.org/pdf/2502.09385
- 5. TSE-APT: An APT Attack-Detection Method Based on Time-Series and Ensemble-Learning Models, Electronics, 2025, 14(15), 2924. - https://www.mdpi.com/2079-9292/14/15/2924
- 6. Simulation-Based Evaluation of Advanced Threat Detection Systems Using the ELK Stack– Journal of Network and Computer Applications (Elsevier) 2024: https://www.sciencedirect.com/science/article/pii/S1569190X24001412

Industry Standards and Best Practices:

- 7. Elastic Security Detection Rules – "Detection Engineering for Advanced Threats" – https://www.elastic.co/security-labs

Thank You

Team Dedsec_01