



2025

**Defending Against APT36  
(Transparent Tribe):  
A Modern Analysis  
of Espionage  
Threats and AI-  
Driven Security**



*Insights into APT36's cross-platform espionage campaigns and the AI-powered strategies to disrupt them.*

## Executive Summary

APT36, also known as Transparent Tribe, Mythic Leopard, Earth Karkaddan, and Operation C-Major, represents one of the most persistent state-sponsored cyber espionage threats targeting South Asian defense, government, and critical infrastructure sectors. Active since at least 2013 and attributed to the Pakistani Inter-Services Intelligence (ISI), this Advanced Persistent Threat group has demonstrated remarkable adaptability in pursuing strategic intelligence objectives.

This white paper provides a comprehensive analysis of APT36's tactics, techniques, and procedures (TTPs), examines recent campaign evolution through 2024-2025, and details how the Seceon Open Threat Management Platform delivers advanced defensive capabilities specifically designed to detect, prevent, and respond to sophisticated threats like APT36.

**Key Findings:**

- APT36 has evolved from simple Windows-focused malware to multi-platform attacks targeting Linux, Android, and cross-platform environments
- The group leverages social engineering, current events, and sophisticated impersonation to maximize phishing effectiveness
- Recent campaigns show increased technical sophistication with cross-platform programming languages (Python, Golang, Rust)
- APT36 exploits legitimate cloud services (Google Drive, Telegram, Discord, Slack) for C2 and exfiltration to evade detection
- Seceon's AI-driven platform provides comprehensive defense through real-time threat detection, behavioral analytics, and automated response

## APT36 Threat Actor Profile

**Attribution and Operational History**

APT36 is a Pakistan-linked Advanced Persistent Threat group conducting cyber espionage operations since at least 2013. Operating under multiple aliases, including Transparent Tribe, Mythic Leopard, ProjectM, COPPER FIELDSTONE, Earth Karkaddan, Storm-0156, and Operation C-Major, the group has been consistently attributed to Pakistani state interests.

**Attribution:** Multiple cybersecurity organization's including TrendMicro, Cisco Talos, BlackBerry, CloudSEK, and CYFIRM, have attributed APT36 to the Pakistani Inter-Services Intelligence (ISI). Attribution is based on operational security mistakes, infrastructure analysis, targeting patterns, and timing correlation with geopolitical events.

**Primary and Secondary Targets****Primary Targets:**

- Indian Government Agencies and Defense Organizations

- Ministry of Defence and defense contractors
- Indian Air Force and aerospace sector entities
- Military and diplomatic personnel
- Critical Infrastructure: Railways, Oil & Gas, Energy sectors
- Research organizations and educational institutions
- State-run defense production facilities

### Secondary Targets:

Afghanistan, Sri Lanka, Australia, Austria, Belgium, Canada, China, Germany, Iran, Japan, Malaysia, Nepal, Netherlands, Oman, Romania, Saudi Arabia, Spain, Sweden, Thailand, Turkey, United Arab Emirates, United Kingdom, United States, and civil society activists in Pakistan.

## Technical Capabilities and Evolution

### Malware Arsenal

#### Windows-Targeted Malware:

- **Crimson RAT:** Signature Windows Remote Access Trojan (first observed 2017) with keystroke logging, screen capture, file exfiltration, and remote command execution capabilities
- **ObliqueRAT:** Advanced Windows malware delivered via macro-enabled documents, often hidden within bitmap images, featuring enhanced stealth capabilities
- **Additional Tools:** Dark Comet RAT, Luminosity RAT, Breach RAT, NJRat, Quasar RAT, Bozok, Peppy, USBWorm

#### Android-Targeted Malware:

- **CapraRAT:** Sophisticated Android RAT with capabilities mirroring Crimson RAT, targeting mobile devices of military and government personnel
- **Stealth Mango, Tangelo, ElizaRAT:** Mobile surveillance malware with extensive data collection and exfiltration capabilities

## Linux-Targeted Malware (Recent Evolution):

- **Poseidon Backdoor:** Golang-based agent for Linux/macOS leveraging Mythic C2 framework with 40+ commands including shell access, file operations, keystroke logging, and screenshot capture
- **Malicious .desktop Files:** Innovative attack vector targeting BOSS Linux (Indian government distribution), weaponizing Linux shortcut files to appear as PDF documents
- **Python Downloaders:** Lightweight ELF binaries compiled with PyInstaller with minimal detection signatures (aldndr.py, basha.py variants)

## Attack Methodology

### Initial Access Vectors:

- **Spear-Phishing:** Highly targeted emails with contextually relevant lures exploiting current events (Kashmir conflict, Pahalgam terror attack) and impersonating legitimate organizations
- **Malicious Attachments:** Weaponized PDFs, Office documents, ISO images, VHDX archives, and ZIP files containing payloads
- **Malvertising and Domain Impersonation:** Google Ads promoting Trojanized software and typo-squatted domains mimicking Indian government portals (mail.mgovcloud.in, virtualeoffice.cloud)
- **ClickFix Social Engineering:** Adapted for Linux systems, tricking users into executing malicious commands
- **Watering Hole Attacks:** Compromising legitimate websites (e.g., Indian Industries Association) to host malicious payloads

### Command and Control:

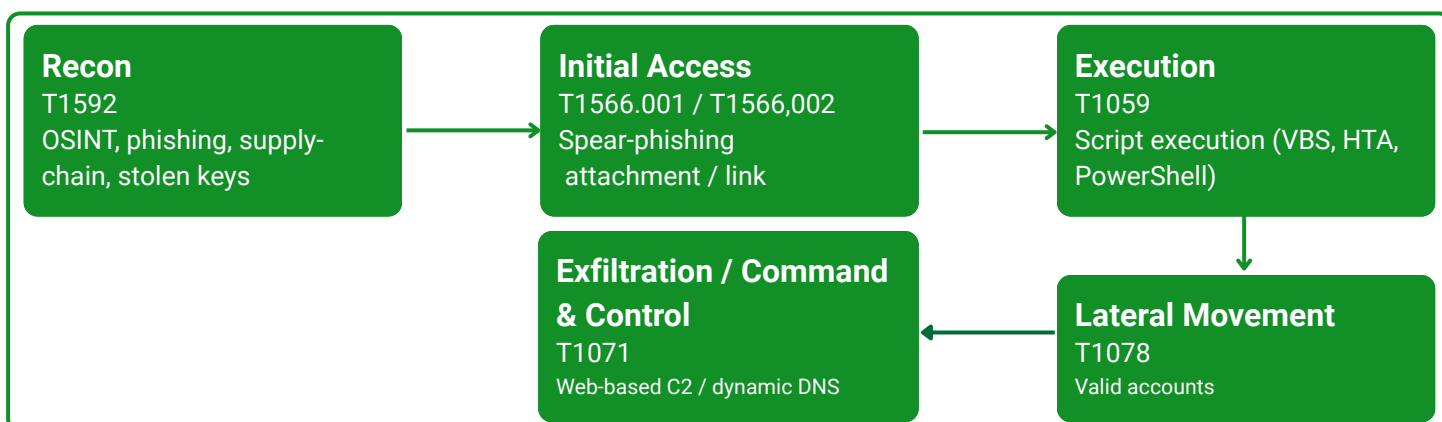
- Abuse of legitimate cloud services: Google Drive, Telegram, Discord, Slack for C2 and data exfiltration
- Over 100 phishing domains hosted on providers like AlexHost using deceptive TLDs (report, .support)
- Infrastructure tied to Pakistani IT firms (e.g., Zah Computers)
- The Mythic C2 framework provides robust backdoor communications

## MITRE ATT&CK Framework Mapping

APT36 operations map extensively across the MITRE ATT&CK framework:

- **Reconnaissance (TA0043):** Phishing for information (T1598), targeting defense sector employees
- **Initial Access (TA0001):** Spear-phishing attachments (T1566.001), links (T1566.002), exploiting public-facing applications
- **Execution (TA0002):** User execution (T1204.001, T1204.002), command and scripting interpreters
- **Persistence (TA0003):** Scheduled tasks/jobs, registry modifications, startup folder manipulation
- **Defense Evasion (TA0005):** Obfuscated files, virtualization/sandbox evasion through time zone checks, masquerading
- **Credential Access (TA0006):** Input capture (T1056), credential dumping, brute force attacks, MFA bypass techniques
- **Collection (TA0009):** Data from local system (T1005), clipboard data, screen capture, keylogging
- **Command and Control (TA0011):** Application layer protocol (T1071), web protocols, encrypted channels using legitimate services
- **Exfiltration (TA0010):** Exfiltration over C2 channel, alternative protocols, cloud storage services
- **Privilege Escalation (TA0004):** Use of valid accounts (T1078), token manipulation, DLL sideloading
- **Discovery (TA0007):** Account discovery (T1087), network discovery (T1018), system information discovery (T1082)
- **Lateral Movement (TA0008):** Valid account reuse for remote access (T1078), remote services (RDP/SMB)

## Attack Flow Diagram



# Seceon Platform Defense Capabilities

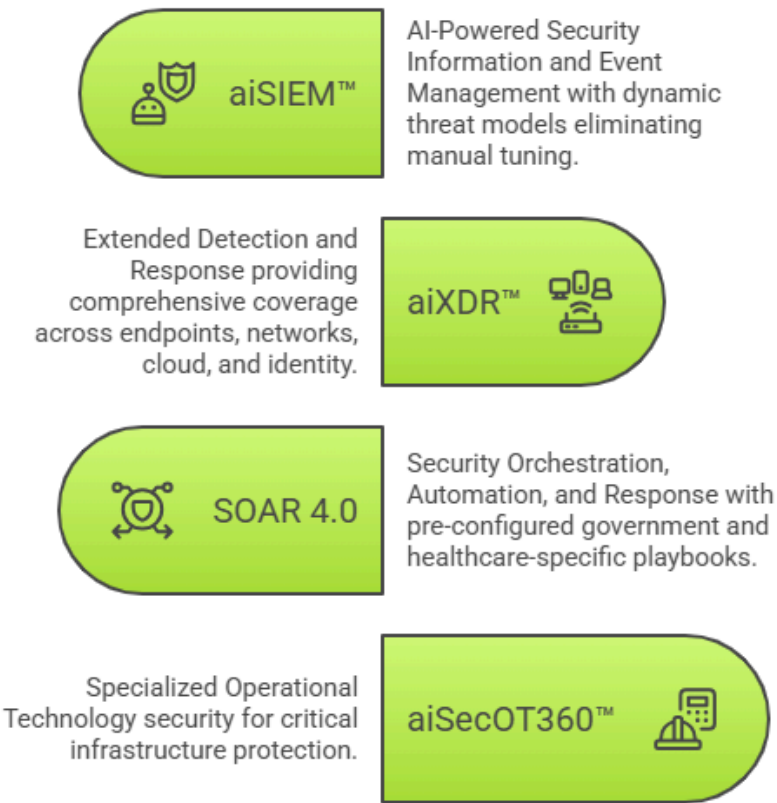
## Platform Overview

The Seceon Open Threat Management (OTM) Platform represents a paradigm shift in cybersecurity defense, specifically designed to address sophisticated, persistent threats like APT36. Unlike traditional security solutions requiring extensive manual configuration, Seceon's AI-driven platform delivers immediate, actionable threat intelligence with automated response capabilities.

### Core Platform Components:

- **aiSIEM™**: AI-Powered Security Information and Event Management with dynamic threat models eliminating manual tuning
- **aiXDR™**: Extended Detection and Response providing comprehensive coverage across endpoints, networks, cloud, and identity
- **SOAR 4.0**: Security Orchestration, Automation, and Response with pre-configured government and healthcare-specific playbooks
- **aiSecOT360™**: Specialized Operational Technology security for critical infrastructure protection

### Platform Core Component



### Platform Scale:

- 1.5 Trillion Security Event across 9300+ customers
- Supports 950+ pre-built connectors for comprehensive data ingestion
- Processes 150 million events per second with real-time correlation



- Integrates 70+ threat intelligence feeds for contextual enrichment
- Provides Day 1 effectiveness without weeks of manual rule tuning



## Detection Capabilities Against APT36

### Phishing and Initial Access Detection:

- **Email Security Integration:** Advanced correlation identifying APT36's spear-phishing campaigns, malicious attachments (PDFs, Office documents, ISO images), and suspicious sender patterns
- **Domain Reputation Analysis:** Real-time detection of typo-squatted domains, newly registered domains mimicking government portals, and connections to known malicious infrastructure
- **Behavioral Analytics:** Machine learning models identifying anomalous email patterns, unusual attachment types, and social engineering indicators consistent with APT36

### Malware Detection and Analysis:

- **Multi-Platform Threat Detection:** Comprehensive monitoring across Windows, Linux (including BOSS Linux), Android, detecting Crimson RAT, ObliqueRAT, CapraRAT, Poseidon, and Python/Golang malware variants
- **Sandbox Integration:** Automatic submission of suspicious files to integrated sandbox environments for dynamic analysis and behavioral profiling
- **Behavioral Malware Detection:** AI-powered detection of malicious behaviors, including process injection, privilege escalation, credential dumping, and suspicious network connections



Network Threat Detection:

- **C2 Communication Detection:** Identification of command and control traffic to legitimate cloud services (Google Drive, Telegram, Discord, Slack) through behavioral analysis and traffic pattern anomalies
- **DNS Tunneling Detection:** Advanced algorithms detecting DNS-based exfiltration and C2 communications
- **Network Flow Analysis:** Deep packet inspection and metadata analysis identifying lateral movement, data staging, and exfiltration activities

User and Entity Behavior Analytics (UEBA):

- **Credential Theft Detection:** Anomaly detection for credential access attempts, brute force attacks, unusual authentication patterns, including Kavach MFA bypass attempts
- **Privilege Escalation Alerts:** Identification of unauthorized privilege elevation and lateral movement
- **Data Exfiltration Detection:** Behavioral analytics identifying unusual data access patterns, large file transfers, and unauthorized document sharing

Detection Use Cases

Detection Area	What to Look For
Email	Defense-themed phishing, spoofed domains, malicious doc attachments
Endpoint	Office → scripting engine (wscript, mshta, powershell) → network traffic
Network	C2 traffic to dynamic DNS domains (duckdns, no-ip, etc.)
Persistence	Suspicious scheduled tasks, execution from %AppData%
User Behavior	Unusual VPN logs, abnormal time-of-day access

## MITRE ATT&CK Integration

Seceon provides native MITRE ATT&CK framework integration, enabling security teams to map threat indicators directly to adversary tactics and techniques.

- **Automatic Technique Mapping:** All security alerts correlate with relevant ATT&CK techniques and sub-techniques
- **ATT&CK Navigator Integration:** Visual representation of detected techniques across the ATT&CK matrix
- **Coverage Gap Analysis:** Identification of detection gaps across tactics requiring additional security controls
- **Threat Actor Profiling:** Correlation of detected techniques with known APT36 TTPs for attribution confidence
- **Custom Correlation Rules:** ATT&CK-based rule creation for organization-specific threat scenarios

## Automated Response and SOAR

Seceon's SOAR 4.0 provides an automated, orchestrated response to APT36 threats, dramatically reducing dwell time and limiting damage potential.

### Automated Response Capabilities:

- **Phishing Response:** Automatic quarantine of malicious emails, blacklisting sender addresses, and blocking domains/URLs
- **Endpoint Isolation:** Immediate network isolation of compromised endpoints, preventing lateral movement
- **Malware Containment:** Automated process termination, file quarantine, registry rollback, system restoration
- **Credential Reset:** Automatic password resets for compromised accounts, MFA enforcement, and session termination
- **Firewall Automation:** Dynamic firewall rule updates blocking malicious IPs, domains, and C2 infrastructure

- **Forensic Data Collection:** Automated evidence preservation including memory dumps, disk images, and network captures

## Critical Infrastructure Protection

Given APT36's targeting of critical infrastructure (Railways, Oil & Gas, Energy), Seceon's aiSecOT360 provides specialized security for OT, ICS, and IoT environments.

- **Protocol-Aware Monitoring:** Deep inspection of industrial protocols (Modbus, DNP3, OPC, BACnet), detecting unauthorized PLC commands
- **Asset Discovery:** Passive network analysis for comprehensive OT/ICS asset inventory without disrupting production
- **IT/OT Convergence Security:** Unified visibility detecting lateral movement from corporate networks to control systems
- **Zero-Disruption Response:** Safety-aware response capabilities protecting critical operations while containing threats

## Defense Strategy and Implementation

### Layered Security Approach

Defending against sophisticated APT actors like APT36 requires a comprehensive, layered security strategy:

#### Layer 1 - Perimeter Defense:

- **Email Security:** Advanced spam filtering, attachment sandboxing, URL rewriting, DMARC/DKIM/SPF enforcement
- **Web Security:** Web application firewalls (WAF), DNS filtering, malware protection
- **Network Segmentation:** Zero Trust architecture, micro-segmentation, east-west traffic inspection

#### Layer 2 - Endpoint Protection:

- Next-generation antivirus with behavioral detection

- Endpoint Detection and Response (EDR) integration
- Application whitelisting and control
- Patch management and vulnerability remediation

### Layer 3 - Identity and Access Management:

- Multi-factor authentication (MFA) enforcement, including Kavach
- Privileged access management (PAM)
- Least privilege access controls
- Strong password policies and credential rotation

### Layer 4 - Detection and Analytics:

- Seceon aiSIEM for comprehensive security monitoring
- User and Entity Behavior Analytics (UEBA)
- Network traffic analysis and anomaly detection
- Threat hunting and proactive investigation

## Building a Robust Defense Strategy



### Layer 5 - Incident Response:

- SOAR-driven automated response
- Incident response playbooks and runbooks
- Forensic analysis and evidence preservation
- Post-incident review and continuous improvement

## Conclusion and Recommendations

### The APT36 Threat Landscape

APT36 (Transparent Tribe) represents a persistent, sophisticated, and continuously evolving threat to the Indian government, defense, and critical infrastructure sectors. The group's demonstrated ability to adapt tactics, expand to new platforms (Linux, Android), and leverage current geopolitical events makes them a formidable adversary requiring comprehensive, intelligent defense capabilities.

### Key Takeaways:

- APT36 has evolved from basic Windows malware to sophisticated cross-platform capabilities
- The group expertly leverages social engineering, geopolitical events, and government impersonation
- Recent campaigns show increased technical sophistication with abuse of legitimate cloud services
- Traditional security tools struggle with APT36's evasion techniques and operational security
- Defense requires comprehensive, AI-driven threat detection with automated response capabilities

### Seceon Platform Advantage

The Seceon Open Threat Management Platform provides decisive advantages in defending against APT36:

**1. AI-Driven Detection:** Dynamic threat models provide Day 1 effectiveness, automatically adapting to APT36's evolving TTPs without manual tuning

- 2. Comprehensive Visibility:** Unified monitoring across Windows, Linux, Android, cloud, and OT/ICS environments eliminates blind spots
- 3. Automated Response:** SOAR-integrated playbooks dramatically reduce dwell time, containing APT36 before strategic objectives are achieved
- 4. Behavioral Analytics:** UEBA capabilities detect credential theft, privilege escalation, and lateral movement characteristic of APT36
- 5. Threat Intelligence:** Integration of 70+ feeds with APT36-specific IOCs provides contextual awareness and attribution confidence
- 6. MITRE ATT&CK Integration:** Native framework mapping enables strategic defense planning and coverage gap identification
- 7. Critical Infrastructure Protection:** aiSecOT360 provides specialized security for Railways, Oil & Gas, and Energy sectors targeted by APT36

## Strategic Recommendations

### Immediate Actions (0-30 Days):

- Deploy Seceon aiSIEM for immediate visibility into APT36 indicators
- Enable APT36-specific threat intelligence feeds and correlation rules
- Conduct a security assessment identifying high-risk targets (defense personnel, critical systems)
- Implement enhanced email security controls and user awareness training
- Enforce MFA across all privileged and government accounts

### Short-Term Actions (1-3 Months):

- Deploy aiXDR for comprehensive endpoint protection across all platforms
- Implement UEBA for behavioral anomaly detection
- Configure SOAR playbooks for automated APT36 response
- Conduct threat hunting exercises focusing on APT36 TTPs
- Establish incident response procedures and communication plans

# APT36 THREAT INTELLIGENCE

Pakistan-Linked Advanced Persistent Threat & Comprehensive Defense Strategy

## MALWARE ARSENAL



**Crimson RAT**  
Windows RAT



**ObliqueRAT**  
Windows Malware



**GLOBSHELL**  
Cross-Platform



**CapraRAT**  
Android RAT



**Python Loaders**  
ELF Binaries







## Threat Profile

- ◆ **Active Since**  
2013 - Present (12+ Years)
- ◆ **Attribution**  
Pakistani Inter-Services Intelligence (ISI)
- ◆ **Primary Targets**
  - Indian Government & Defense
  - Critical Infrastructure (Railways, Oil & Gas)
  - Aerospace & Military Contractors
  - Research & Education Institutions

## Attack Chain

- ◆ **Initial Access**  
Spear-Phishing with malicious attachment
- ◆ **Execution**  
Macro-enabled docs & scripts
- ◆ **Persistence**  
Schedule tasks & registry mods

## Seceon's Defense

-  **AI-Driven Detection**  
Dynamic threat models, Day 1 effectiveness
-  **Multi-Platform Coverage**  
Windows, Linux, Android, Cloud, OT/ICS
-  **Automated Response**  
SOAR 4.0 with government playbooks
-  **Behavioral Analytics**  
UEBA detecting credential theft & lateral movement
-  **MITRE ATT&CK**  
Native framework integration & coverage analysis
-  **Critical Infrastructure**  
aiSecOT360 for OT/ICS/SCADA protection

## SECEON PLATFORM AT SCALE

**1.5T**

Security Events  
Monitored Daily

**9,300+**

Customers  
Protected Globally

**950+**

Pre-Built  
Connectors

**150M**

Events/Second  
Processing

*Stop APT36 at the source; with Seceon's autonomous, predictive cyber defense*



### **Long-Term Actions (3-12 Months):**

- Implement Zero Trust architecture with microsegmentation
- Deploy aiSecOT360 for critical infrastructure protection
- Establish a proactive threat hunting program with dedicated resources
- Conduct regular purple team exercises validating APT36 defenses
- Develop threat-informed defense strategy based on MITRE ATT&CK
- Participate in information-sharing communities (CERT-In, ISACs)

### **Final Thoughts**

The threat posed by APT36 is not diminishing -it is evolving and intensifying. As geopolitical tensions persist and India's defense modernization programs advance, APT36 will continue developing new capabilities and attack vectors. Organizations cannot afford reactive security postures in this threat environment.

The Seceon Open Threat Management Platform provides the comprehensive, intelligent, and automated defense capabilities required to protect against sophisticated APT threats like APT36. By combining AI-driven detection, behavioral analytics, automated response, and critical infrastructure protection, Seceon enables organizations to move from reactive incident response to proactive threat defense.

Organizations facing APT36 threats should act decisively to implement these capabilities before the next wave of attacks. The time to defend is before compromise occurs, not after.

### **About Seceon**

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms.

The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 700 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.



## References and Citations:

This whitepaper is based on research and data from:

- **Trend Micro Research (2022).** *Investigating APT36 (Earth Karkaddan) Attack Chain and Malware Arsenal.*
- **BlackBerry Research & Intelligence Team (2024).** *Transparent Tribe Targets Indian Government, Defense, and Aerospace Sectors Leveraging Cross-Platform Programming Languages.*
- **Cisco Talos Intelligence Group (2021).** *Analysis of Pakistan-Linked APT36 Campaigns and Infrastructure.*
- **CERT-In Advisory (2023).** *Advisory on APT36 Targeting Indian Government and Defense Organizations.*
- **US-CERT (CISA) Bulletin (2022).** *Alert on State-Sponsored Espionage Groups Targeting Defense and Critical Infrastructure.*
- **Microsoft Threat Intelligence Center (MSTIC) (2023).** *Storm-0156: Pakistan-Linked Espionage Activity Targeting South Asia.*
- **Kaspersky Global Research & Analysis Team (2020).** *Transparent Tribe: Long-Term Espionage Operations Targeting Defense and Military Personnel.*
- **Recorded Future Insikt Group (2023).** *Pakistan-Aligned Threat Activity Targeting Strategic Indian Sectors.*
- **CYFIRMA Threat Research (2024).** *APT36 Campaign Evolution and Cross-Platform Malware Development.*
- **Indian Defence Cyber Agency (2024).** *Threat Assessment Report on Pakistan-Linked APT Threats.*

# About the Author

## Smit Kadakia

Co-founder, Seceon Inc.

---



Smit leads Seceon's data science and machine learning team, focused on developing a state-of-the-art behavior anomaly detection solution. Smit holds a B.S. from VJTI, Mumbai, an MS in Computer Science from Indian Statistical Institute, Kolkata, and an MBA from Southern New Hampshire University, Manchester. Smit and the team at Seceon have built the industry's first and only fully automated threat detection and remediation system using a combination of machine learning and artificial intelligence techniques. Seceon's approach includes analysis of all traffic, flows, and processes in and out of the network and correlates them near-simultaneously with behavioral analytics, recognized and zero-day exploits, and policies to surface threats and proposed responses in near-record real-time.

# About the Author

## Anamika Pandey

AI/ML Cybersecurity Engineer, Seceon Inc.

---



Anamika leverages artificial intelligence, machine learning, and Dynamic Threat Modeling (DTM) to fortify IT, OT, IoT, and cloud infrastructures. Her expertise lies in advancing AI-driven defense strategies that not only ensure compliance and resilience but also deliver measurable ROI. Through Seceon's OTM Platform, she helps organizations anticipate, detect, and mitigate evolving cyber threats, empowering them to stay secure, adaptive, and future-ready.