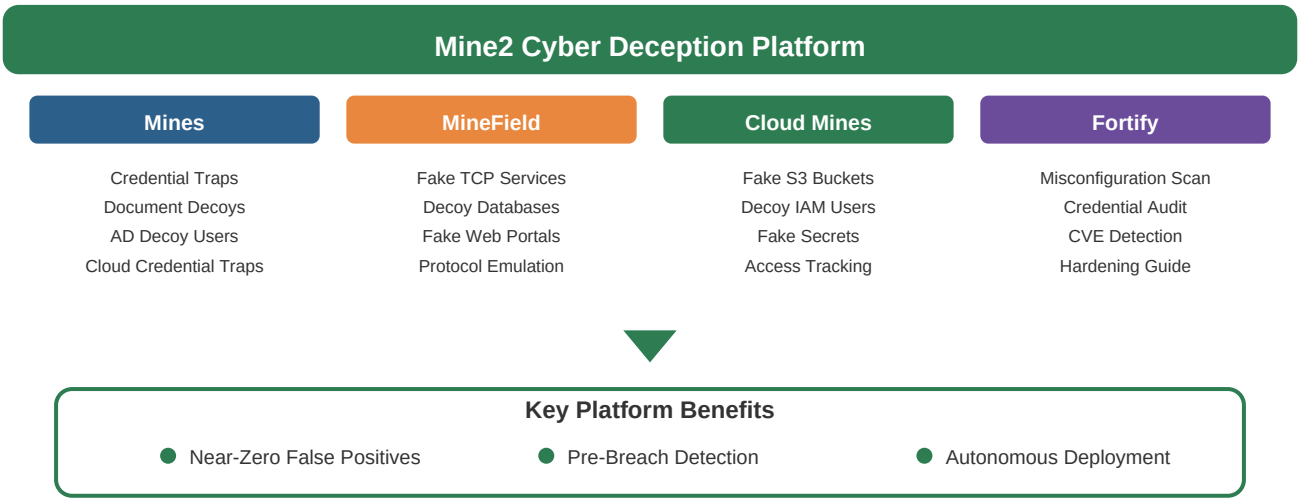
DECEPTION AS A SERVICE (DaaS)

The Future of Proactive Cyber Defense

A Mine2 Technical Whitepaper | 2026



On-Prem | Cloud | Hybrid | SIEM/SOAR/EDR Integration

www.mine2.io | info@mine2.io

Why Traditional Detection Is Failing

Enterprise SOCs deploy 45-75 security tools generating thousands of daily alerts. 40-60% are false positives. Despite billions spent on firewalls, EDR, and SIEM, breaches accelerate. Average dwell time exceeds 200 days. The root cause is architectural: every traditional tool is reactive -- it waits for an attacker to act, then tries to classify the action as malicious using signatures, heuristics, or behavioral models.

- **Alert Fatigue:** SOC analysts spend 80% of time on false positives. Real threats are missed not because tools failed, but because no one had time to investigate.
- **Zero-Day Blindness:** Signature-based detection misses novel attacks by definition. CatB ransomware at AIIMS Delhi, GhostSpider backdoor by Salt Typhoon -- both evaded all signature databases.
- **Living-off-the-Land:** Attackers use stolen credentials and built-in tools (PowerShell, WMI, RDP). These actions are indistinguishable from legitimate admin activity.
- **Lateral Movement:** Once inside, attackers spend weeks mapping infrastructure before striking. BSNL's 278 GB breach was discovered by a third-party firm on a dark web forum -- not by BSNL's own security stack.
- **EDR Is Bypassable and Predictable:** EDR tools follow known detection logic that red teams and attackers routinely study, reverse-engineer, and evade. Kernel-level unhooking, direct syscalls, and in-memory execution bypass most EDR agents. If defenders can test an EDR, so can attackers -- before deploying.
- **No Defense Against Phishing & Social Engineering:** Firewalls, EDR, and SIEM have no answer for a well-crafted phishing email or a vishing call that convinces an employee to hand over credentials. The human layer remains entirely unprotected by traditional technical controls.
- **Supply Chain Blind Spot:** Traditional tools monitor your perimeter and endpoints -- not your vendors. The Iyuno/Netflix breach originated at a localization partner's insecure API. SolarWinds, MOVEit, 3CX -- supply chain attacks bypass every layer of traditional defense by entering through trusted channels.

200+	80%+	40-60%
days average attacker dwell time globally	of breaches involve stolen or leaked credentials	of SOC alerts are false positives

What Is Cyber Deception?

Deception takes a fundamentally different approach: instead of distinguishing malicious activity from legitimate behavior, it places realistic but fake assets throughout infrastructure -- fake credentials, decoy servers, fabricated documents. These have no legitimate purpose. When something interacts with them, it is a confirmed threat. No signatures to update, no baselines to train.

> *A defender only needs to place traps along likely attack paths. An attacker, navigating blind, must avoid every single one. One misstep = confirmed detection. This is why deception achieves near-zero false positives -- a property no other detection technology can claim.*

Mine2: Deception as a Service Platform

Mine2 is a unified DaaS platform that delivers comprehensive deception from a single console -- spanning on-premises infrastructure, cloud environments, Active Directory, and the application layer. Four core components create a layered deception fabric:

Mines (Digital Tripwires)

Mines are realistic but fabricated digital artifacts planted across your environment -- fake credentials, decoy documents, dummy user accounts, and planted configuration files. They are designed to be indistinguishable from real assets to anyone navigating the environment without institutional knowledge. Any interaction triggers an immediate, high-confidence alert with full forensic context: source IP, user identity, timestamp, and action performed. No triage required. No false positive investigation.

MineField (Active Decoy Infrastructure)

MineField transforms any system into a deception platform by running realistic fake TCP services and network listeners. To an attacker scanning the network, MineField services are indistinguishable from production systems -- fake databases, file transfer services, mail servers, web portals, and custom protocol emulators. Every connection is logged with full telemetry: credentials submitted, commands executed, and network traversal.

Cloud Mines (Automated Cloud Deception)

Cloud Mines extends deception into AWS through a three-stage workflow: Scan your existing infrastructure, Suggest decoy resources matching your naming conventions (fake S3 buckets, IAM users, secrets, API keys), and Deploy with one-click approval. Continuous monitoring via CloudTrail provides full attribution for every access attempt.

Fortify (Attack Surface Hardening)

Fortify complements deception by reducing the real attack surface -- scanning for misconfigurations, weak credentials, known CVEs, and security hygiene issues. By hardening real infrastructure and leaving Mine2's controlled traps as the path of least resistance, defenders funnel attackers toward detection.

Deception Coverage Across the Kill Chain:

Reconnaissance	MineField decoy services, fake open ports
Credential Access	Mines: planted fake credentials and configs
Lateral Movement	AD decoy users, fake database servers
Data Exfiltration	Decoy documents on shares and repositories
Cloud Attack	Cloud Mines: fake S3, IAM, Secrets in AWS

AI-Driven Deception (AI Mines)

Mine2 leverages AI to enhance the entire deception lifecycle, ensuring deception assets remain realistic, strategically positioned, and responsive to evolving attack patterns:

- **Intelligent Placement:** Analyzes infrastructure topology, AD structure, and traffic patterns to recommend optimal mine placement along likely attack paths -- not random scattering.
- **Realistic Decoy Generation:** Generates content that blends with your environment -- naming conventions, credential formats, document styles. Critical against sophisticated attackers who test for honeypot indicators.
- **Behavioral Analysis:** Classifies attacker interactions in real time -- distinguishing automated scanners from manual human operators from targeted exploitation. Enriches alert context for SOC prioritization.
- **Adaptive Deception:** Continuously learns from attacker interactions across the platform and adjusts strategies. If attackers ignore certain decoy types, AI adapts. New techniques emerge, new decoys follow.

Mine2Mate: Autonomous Deployment

Enterprise-scale deception requires automation. Mine2Mate is the autonomous deployment engine that streamlines the entire lifecycle:

- **Auto-Discovery & Deploy:** Discovers infrastructure, recommends deception strategy, and deploys mines, MineField services, and Cloud Mines with minimal manual intervention. New segments covered in minutes.
- **Continuous Management:** Monitors health and coverage of deployed deception assets. Auto-rotates mines, updates decoy services, and tracks infrastructure changes.
- **SOC Integration:** Routes alerts to SIEM, SOAR playbooks, and ticketing systems with pre-built response procedures for each alert type.

Mine2 Console

The centralized management platform providing complete visibility into the deception environment:

- **Asset Management:** Full inventory of all deployed mines, MineField services, and Cloud Mines across the enterprise.
- **Real-Time Alerting:** Immediate notification with full forensic context -- source IP, identity, timestamp, action, and lateral movement correlation.
- **Attacker Telemetry:** Tools used, credentials submitted, commands executed, network traversal patterns. Enriched with MITRE ATT&CK mappings.
- **Attack Path Visualization:** Visual mapping of attacker movement showing which deception assets were triggered in what sequence -- a real-time view of active intrusion.

Deployment Architecture

On-Premises: Full deployment within customer data centers for strict data sovereignty. **Cloud-Native:** Cloud Mines deploy natively within AWS (Azure/GCP support). **Hybrid:** Most common model -- mines and MineField on-prem, Cloud Mines in cloud, unified management through Mine2 Console.

Native integrations: SIEM (Splunk, Elastic, QRadar), SOAR (Palo Alto XSOAR, Splunk SOAR), EDR (CrowdStrike, SentinelOne), Cloud (AWS, Azure, GCP).

Benefits of Deception as a Service

Near-Zero False Positives

Deception assets have no legitimate users. Any interaction is a confirmed threat. This eliminates the alert fatigue that paralyzes SOC teams -- analysts only investigate real intrusions, not noise.

Pre-Breach Detection

Mines and MineField detect attackers during reconnaissance and lateral movement -- before they reach high-value targets, deploy ransomware, or exfiltrate data. Detection shifts from post-breach to pre-breach.

Rich Threat Intelligence

Every attacker interaction generates telemetry: tools, techniques, credentials, intent. This intelligence informs defensive improvements, threat hunting, and incident response across the organization.

Reduced Dwell Time

By detecting early-stage activity, Mine2 reduces dwell time from months to hours. The AIIMS attack's 10+ day disruption could have been prevented by detecting the initial AD enumeration.

Low Operational Overhead

No signatures to update. No baselines to train. No tuning required. Mine2Mate automates deployment and management. The SOC only sees confirmed threats.

Regulatory Compliance

Demonstrable, proactive detection satisfies DPDP Act 2023, CERT-In 6-hour reporting mandate, and sector-specific regulations (Telecom Cyber Security Rules 2024, NABH, RBI, TPN/MPAA).

Market Opportunity

The cyber deception market is at an inflection point. Several macro trends are accelerating adoption:

- **SOC Efficiency Mandate:** 3.5 million global cybersecurity talent shortage. Deception's zero false positive rate directly addresses this constraint.
- **Ransomware Epidemic:** Ransomware groups spend weeks in recon before deploying encryption. Deception detects this pre-encryption activity -- the phase where intervention prevents catastrophic damage.
- **Cloud Complexity:** Multi-cloud environments create visibility gaps traditional tools cannot address. Cloud-native deception extends detection without additional infrastructure.
- **Regulatory Pressure:** DPDP Act, CERT-In, sector-specific mandates demand demonstrable proactive security. Deception provides auditable evidence of active threat detection.
- **Standardization:** Deception is evolving from 'nice-to-have' to a standard security layer alongside EDR, SIEM, and CSPM.

Use Cases

1. Credential Theft Detection

Without Mine2: Attacker compromises a workstation via phishing, harvests credentials from memory and config files, and uses them to access production databases. Discovery: months later during audit.

With Mine2: Among real credentials, the attacker finds Mine2-planted decoy creds. When they attempt to use them, alert fires immediately with source IP and attempted actions. SOC isolates the compromised workstation before any real credentials are exploited.

2. Ransomware Lateral Movement

Without Mine2: Ransomware operator gains access, scans network for databases, backups, and file shares. Spends 5-7 days mapping AD. Deploys encryption on Day 8. Hospital/enterprise discovers breach when systems go dark.

With Mine2: During network enumeration on Day 1, the scanner connects to a MineField fake database service. Alert fires immediately. Security team identifies compromised system and initiates containment. Ransomware never deployed.

3. Insider Threat Detection

Without Mine2: Malicious insider with legitimate access browses shared drives for sensitive data. Copies files to personal storage over weeks. Discovery: only when data appears externally.

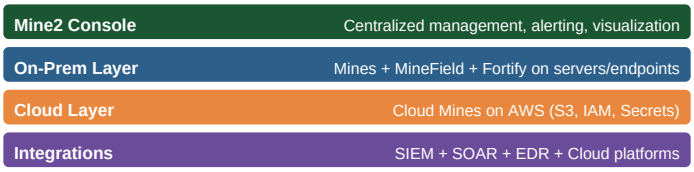
With Mine2: The insider opens a Mine2 decoy document on a shared drive. Alert fires with user identity, workstation, and timestamp. Forensic-grade evidence captured for HR proceedings and legal action.

4. Cloud Breach Detection

Without Mine2: Attacker discovers exposed AWS credentials in a public repository. Enumerates IAM policies, lists S3 buckets, and exfiltrates data. Discovery: weeks later via anomalous billing.

With Mine2: The credentials are Cloud Mines decoys. Every API call is logged via CloudTrail with full attribution. Security team alerted before attacker pivots to real resources.

Integration Architecture



Conclusion

The cybersecurity industry has spent decades building higher walls. Attackers have consistently demonstrated their ability to go over, under, or around them. The result is a defensive posture that is perpetually reactive -- detecting breaches after the damage, investigating alerts that are overwhelmingly false, responding to incidents that could have been prevented.

Deception technology represents a paradigm shift. Instead of building better walls, deception fills the space inside the walls with traps. Instead of trying to identify attackers among millions of legitimate actions, deception creates environments where only attackers will tread. Instead of generating thousands of ambiguous alerts, deception produces confirmed detections with zero false positives.

Mine2's Deception as a Service platform delivers this capability as a unified, automated, AI-enhanced solution. Mines detect credential theft and unauthorized data access. MineField catches lateral movement and network reconnaissance. Cloud Mines extend detection into cloud environments. Fortify hardens the real infrastructure while funneling attackers toward controlled traps. AI Mines ensures deception assets are realistic, strategically placed, and continuously adapted. Mine2Mate automates the entire lifecycle.

> *The asymmetry of cyber conflict has always favored the attacker: defenders must be right every time, while attackers only need to succeed once. Deception inverts this equation. With deception, attackers must be right every time -- avoiding every trap, every decoy, every mine -- while the defender only needs one trigger. Mine2 ensures that trigger is always within reach.*

Why Mine2 DaaS:

- Near-zero false positives: every alert is a confirmed intrusion
- Detects attackers during recon -- before damage occurs
- Works equally against external attackers AND malicious insiders
- Complements existing EDR, SIEM, SOAR -- not a replacement
- Autonomous deployment via Mine2Mate and AI Mines
- On-prem, cloud, hybrid with native SIEM/SOAR integration

Contact Mine2 Today

www.mine2.io | info@mine2.io