# Annual SOC Review

## 2025

An overview of SOC activities, threat trends, and security improvements delivered throughout the year.

CyberSafe

# Executive Summary

Throughout 2025, the SOC strengthened detection and response capabilities through improved correlation logic and expanded visibility, resulting in higher-confidence alerts and a more resilient security posture.

**12M+**

### Total Alerts Processed

Successfully analyzed and responded to security events

**135B+**

### Events Monitored

Continuous monitoring across all customer environments

**99.8%**

### SLA Compliance

Maintained exceptional response time standards

**1K+**

### Critical Incidents

Identified and mitigated before business impact

CyberSafe

# Alert Distribution and Threat Landscape

| | | | |
|---|---|---|---|
| Phishing | 14,200 | | |
| Malware | 11,800 | | |
| Unauthorized Access | 8,500 | | |
| Data Exfiltration | 5,300 | | |
| DDoS Attempts | | Policy Violations | 3,100 |

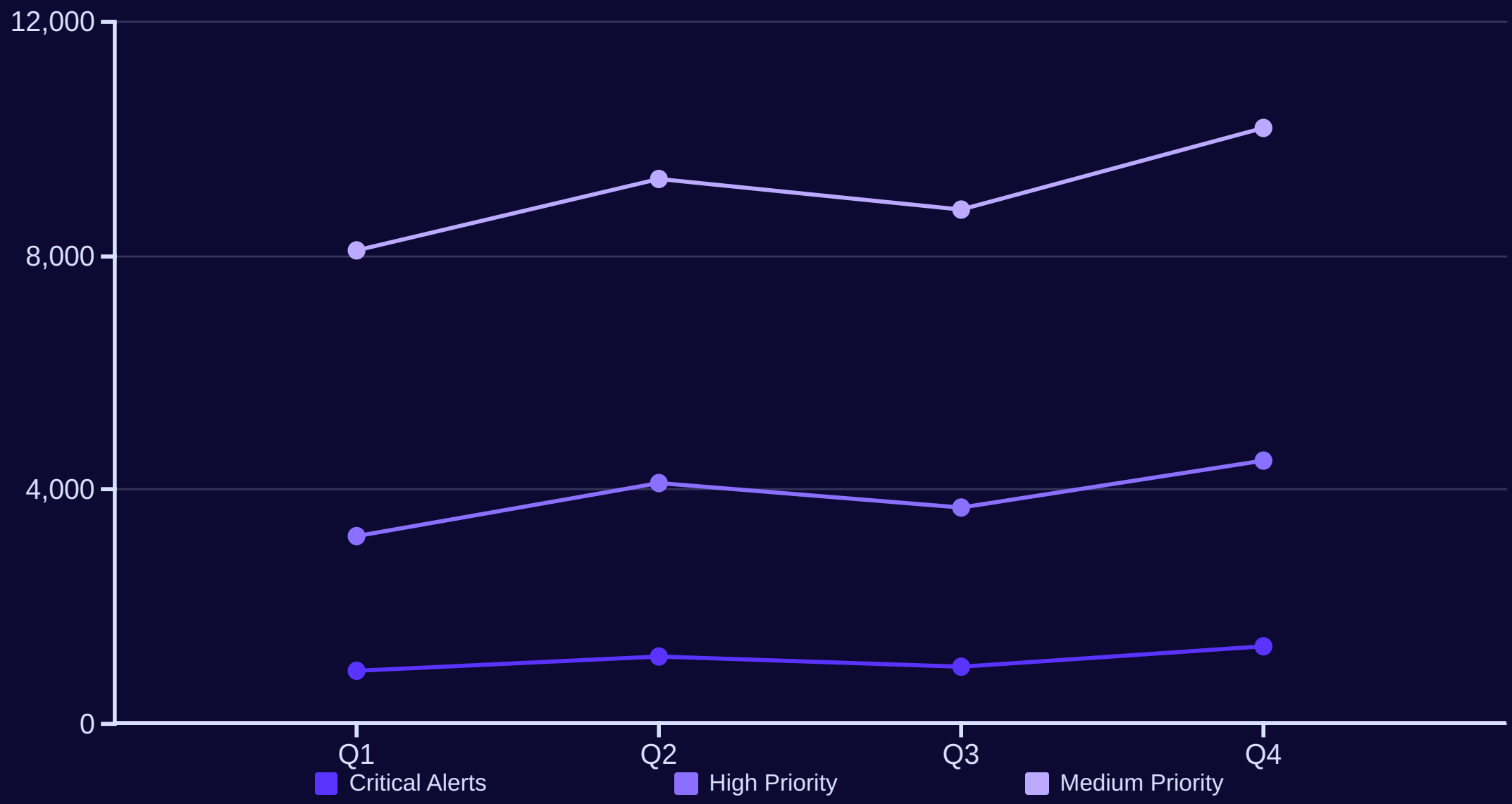
## Key Insights

Phishing remained the dominant attack vector at 30% of all alerts, followed closely by malware at 25%. We observed a significant 42% increase in unauthorized access attempts compared to 2023, primarily targeting cloud infrastructure and remote access systems.

Data exfiltration attempts peaked during Q2 and Q4, correlating with major ransomware campaigns globally. Our enhanced detection capabilities allowed us to identify and block 94% of these attempts within the initial stages.

CyberSafe

# Quarterly Alert Trends




Alert volumes peaked in Q4, driven by holiday-season phishing campaigns and year-end ransomware activity. The 29% increase in critical alerts during Q4 was successfully managed through enhanced staffing and improved automation. Our team's ability to scale operations during high-threat periods ensured continuous protection without service degradation. Medium-priority alerts showed steady growth throughout the year, reflecting expanded monitoring coverage across new customer environments and improved detection sensitivity.

CyberSafe

# Case Study:

## Multi-Stage Fileless Endpoint Compromise

### Incident Type

Fileless endpoint compromise initiated through malicious user interaction, leveraging script-based execution and abuse of legitimate remote access mechanisms for persistence.

### Detection Logic

Behavior-based detection identified abnormal script execution, chained PowerShell activity, and the creation of persistence mechanisms inconsistent with normal user behavior.

### SOC Response

The SOC rapidly investigated the alert, isolated the affected endpoint, removed persistence mechanisms, and blocked external communication paths associated with the attack.

### Outcome

The attack was disrupted at an early stage, preventing data exfiltration, lateral movement, and any business impact. Full remediation was completed within the same day.

---

### Key Takeaway

Early behavioral detection and rapid response were critical in stopping a sophisticated fileless attack before it could progress or cause damage.

CyberSafe

# Case Study:

## Silent Account Takeover via Federated Authentication Abuse

### Incident Type

Account takeover achieved through phishing-driven session hijacking, enabling access without password compromise or MFA interaction, followed by mailbox rule abuse to conceal activity.

### Detection Logic

Anomalous federated sign-in behavior was detected, followed by suspicious mailbox rule creation inconsistent with the user's normal access patterns.

### SOC Response

The SOC investigated the activity, revoked active sessions and authentication tokens, disabled malicious mailbox rules, and secured the affected account.

### Outcome

Unauthorized access was contained before data exfiltration or further misuse. Account integrity was restored with no business impact.

---

### Key Takeaway

Correlation between identity anomalies and mailbox activity enabled detection of a stealthy account takeover that bypassed traditional authentication controls.

CyberSafe

# Emerging Threats and Intelligence Insights

### AI-Powered Social Engineering

Attackers leverage generative AI to create highly convincing phishing campaigns with personalized content and deepfake audio, targeting executives and finance teams.

### Supply Chain Compromises

Third-party software vulnerabilities remain a critical attack vector. Malicious packages in open-source repositories and vendor breaches continue to pose significant risk.

### Cloud Infrastructure Exploitation

Misconfigured cloud storage and identity access management policies are exploited to gain unauthorized access through exposed resources and overprivileged service accounts.

### Ransomware-as-a-Service Evolution

The RaaS ecosystem grows more sophisticated with improved encryption methods, double extortion tactics, and automated victim profiling capabilities.

### Zero-Day Exploitation Acceleration

Actively exploited zero-day vulnerabilities in enterprise software require rapid emergency patching operations, often within hours of public disclosure.

CyberSafe

# Critical Vulnerabilities Tracked

## Top CVEs by Severity

- **CVE-2025-55182** – React2Shell (CVSS 10.0): Unauthenticated remote code execution in React 19 / Next.js via a deserialization flaw in the React Server Components “Flight” protocol, enabling full server takeover.
- **CVE-2025-64446** – FortiWeb (CVSS 9.8): Authentication bypass through path traversal in Fortinet FortiWeb, allowing unauthenticated attackers to compromise the web application firewall.
- **CVE-2025-14847** – MongoBleed (CVSS 8.7): Unauthenticated memory disclosure vulnerability in MongoDB caused by zlib decompression, leading to leakage of credentials and sensitive in-memory data.
- **CVE-2025-20188** – Cisco IOS XE Wireless Controller (CVSS 10.0): Hardcoded JWT authentication bypass allowing remote attackers to gain root-level access and fully compromise wireless controllers.
- **CVE-2025-3248** – Langflow (CVSS 9.8): Unauthenticated remote code execution via code injection in the Langflow AI orchestration framework, enabling takeover of AI infrastructure.


## Patching Response

Our vulnerability management program achieved 96% patch compliance within 72 hours for critical CVEs. Emergency patching procedures were executed for zero-day vulnerabilities, with average remediation time of 4.2 hours from disclosure to deployment.

CyberSafe

# SIEM / SOAR Improvements

## Correlation-driven detections built on expanded log sources

### Log Sources

**Identity & Email**
Entra ID, Google Workspace, FortiMail

**Endpoint & Servers**
SentinelOne, CrowdStrike, Defender, Windows, Linux

**Network & Perimeter**
Fortinet, Palo Alto, Check Point

**Cloud Platforms**
AWS CloudTrail, Azure, GCP

**Backup & Infrastructure**
Veeam, vCenter, Nutanix

### Correlation Logic

Abnormal login → Mailbox rule change

EDR alert → Cross-host lateral movement

External exploit → Internal execution

Risky cloud login → Role/permission change

Backup deletion → Snapshot manipulation

### Detection Capabilities

Account Takeover & BEC Detection

Lateral Movement & Privilege Escalation

Confirmed Compromise Validation

Risky Cloud Administrative Activity

Ransomware Blast Radius Reduction

---

**Operational Outcome:** Higher-confidence detections, reduced false positives, faster standardized response through playbooks.

CyberSafe

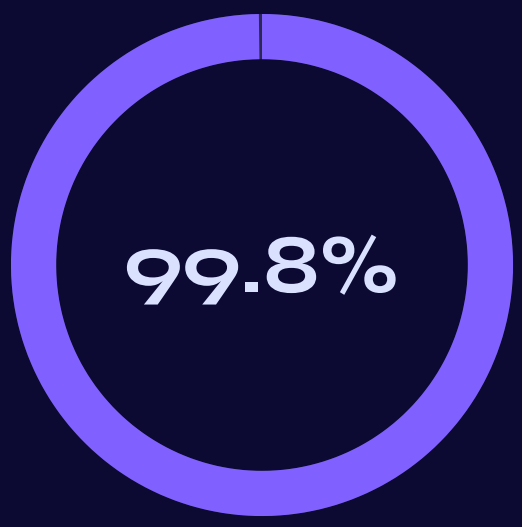
# Key Performance Indicators


**MTTD (Minutes)**

Mean Time to Detect critical threats

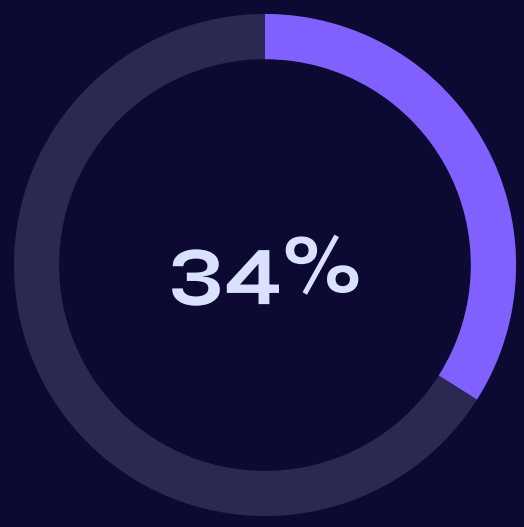

**MTTR (Minutes)**

Mean Time to Respond to incidents




**SLA Achievement**

Response time compliance rate




**FP Reduction**

False positive decrease year-over-year

Our SOC achieved industry-leading performance metrics throughout 2025. Mean Time to Detect improved by 23% compared to 2024, while Mean Time to Respond decreased by 31%. These improvements resulted from enhanced automation, improved analyst training, and optimized detection rules. We maintained 99.8% SLA compliance across all severity levels, with critical alerts receiving response within an average of 6.2 minutes. The 34% reduction in false positives significantly improved operational efficiency and reduced alert fatigue.

CyberSafe

# Customer Security Posture Assessment

## Security Strengths

- **Multi-Factor Authentication:** 87% MFA adoption across critical systems, exceeding industry average of 64%
- **Endpoint Protection:** 98% EDR coverage with consistent policy enforcement and real-time monitoring
- **Patch Management:** 92% compliance with critical patch deployment within 30-day window
- **Security Awareness:** Quarterly phishing simulation shows 79% employee resilience rate

## Priority Recommendations

### Privileged Access Management

Implement PAM solution to control and monitor administrative credentials. Current exposure: 156 accounts with standing privileges.

### Cloud Security Posture

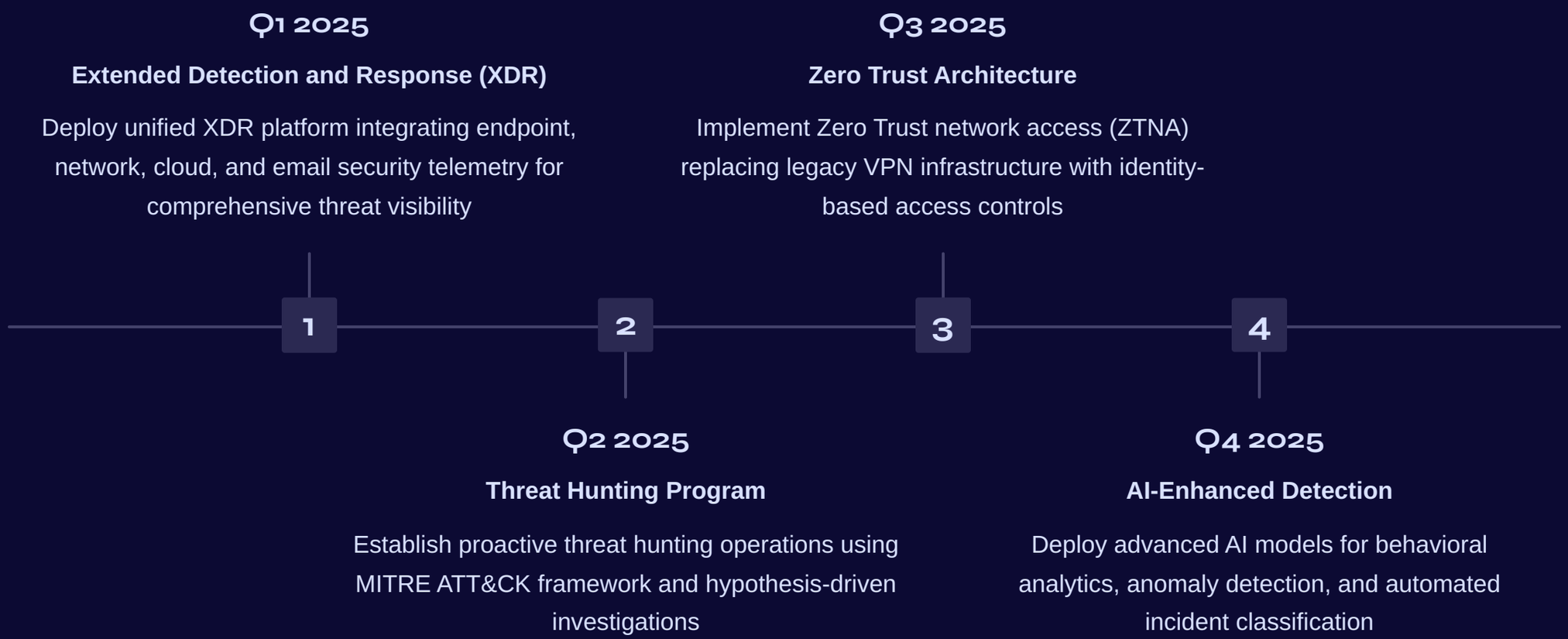
Deploy CSPM tools to continuously monitor cloud configurations. Identified 43 high-risk misconfigurations requiring remediation.

### Data Loss Prevention

Expand DLP coverage to cloud applications and endpoints. Current gap leaves 34% of sensitive data flows unmonitored.

CyberSafe

# 2025 Security Roadmap




Our 2025 roadmap focuses on advancing detection capabilities, reducing response times, and strengthening preventive controls. Strategic investments in XDR technology will provide unified visibility across the entire security stack. The proactive threat hunting program will identify sophisticated threats that evade automated detection. Zero Trust implementation will fundamentally improve access security and reduce attack surface.

CyberSafe

# Cyber Security Predictions for 2026

## Emerging Threats (Offense)

### Phone & SMS Scams

Exploiting urgency and fear

### AI-Generated Backdoors

Hidden vulnerabilities in trusted code

### AI-in-the-Middle

Automated data interception at machine speed

### API Ecosystem Abuse

Exploiting automation logic at scale

### Agentic Ransomware

Autonomous AI-driven extortion campaigns

### AI-Powered Worms

Self-replicating malware across LLM ecosystems

## Key Defensive Strategies (Defense)

### AI-Driven Detection & Response

Operating at machine speed to counter AI attacks

### Explainable AI (XAI)

Mandatory transparency in:

- Training data (prevent poisoning)
- Decision logic (reduce bias)
- Output validation (build analyst trust)

CyberSafe

# Meet Our Security Operations Team

## Continuous Learning

Team completed 340+ hours of advanced security training including SANS courses, threat intelligence certifications, and cloud security specializations

## Industry Recognition

Three analysts achieved GIAC certifications, two earned Offensive Security credentials, and our team placed 2nd in regional CTF competition

## Team Growth

Expanded from 8 to 12 analysts, adding expertise in cloud security, malware analysis, and digital forensics to enhance service capabilities

> "Our strength lies in combining cutting-edge technology with human expertise. Every team member brings unique skills and perspective, creating a culture of continuous improvement and collaborative problem-solving that directly benefits our customers."

CyberSafe



# Appendix: MITRE ATT&CK Coverage

## Detection Coverage by Tactic

| Tactic | Coverage |
|---|---|
| Initial Access | 94% |
| Execution | 89% |
| Persistence | 92% |
| Privilege Escalation | 87% |
| Defense Evasion | 83% |
| Credential Access | 91% |
| Discovery | 78% |
| Lateral Movement | 88% |
| Collection | 85% |
| Exfiltration | 90% |
| Command & Control | 86% |
| Impact | 93% |

## Top Indicators of Compromise

**Malicious IP Addresses** through threat intelligence platforms.

| |
|---|
| 94[.]154[.]35[.]115 |
| 45[.]77[.]33[.]136 |
| 91[.]92[.]240[.]219 |
| 206[.]237[.]3[.]150 |
| 143[.]198[.]92[.]82 |
| 183[.]6[.]80[.]214 |
| 62[.]106[.]66[.]112 |
| 157[.]20[.]182[.]45 |
| 161[.]35[.]172[.]55 |
| 167[.]99[.]224[.]13 |
| 194[.]11[.]246[.]78 |
| 194[.]11[.]246[.]101 |

CyberSafe

# Thank You for Your Trust

Our commitment to protecting your organization extends beyond monitoring and response. We serve as your strategic security partner, continuously adapting our capabilities to address evolving threats and business requirements.

The achievements outlined in this report reflect our team's dedication to excellence and your organization's investment in robust security operations. Together, we've built a resilient security posture that enables your business to operate confidently in an increasingly complex threat landscape.

## Looking Forward

As we enter 2025, we remain focused on delivering exceptional security outcomes through innovation, expertise, and unwavering commitment to your success. Thank you for the opportunity to serve as your trusted security partner.

Schedule Review Meeting | Contact Us

077-5509948
Info@cybersafe.co.il

CyberSafe