

ORYXLABS



HONEYPOT360

THREAT INTELLIGENCE & INSIGHTS

PRODUCT BROCHURE



INTRODUCTION

Cyber intrusions are a persistent reality for organizations across every sector. Adversaries do not rely on noisy attacks, they move quietly, blending into normal traffic and exploiting overlooked pathways. The result: in 2024, the global average dwell time was 11 days and the average global cost of a breach reached \$4.88 million in 2024.

Security investments have strengthened perimeters, but once adversaries gain access, visibility declines sharply. Firewalls, endpoint tools, and monitoring platforms provide alerts, but they rarely reveal the full scope of attacker activity or intent. This intelligence gap leaves defenders reacting late, while adversaries gain time and leverage.

INTRODUCING HONEYPOT360

HONEYPOT360 was designed to close this gap. Our solution is a deception and counter-intelligence platform that deploys realistic decoy environments across networks.

These environments attract attackers away from production assets, allowing defenders to observe their actions in a controlled setting. Every probe, lateral movement, and attempted exploit is captured in detail, producing intelligence that strengthens response and informs strategy.

HONEYPOT360 SHIFTS DEFENSE FROM PASSIVE MONITORING TO ACTIVE ENGAGEMENT:

- » Earlier detection of intrusions through adversary interaction with decoys.
- » Comprehensive telemetry on attacker tools, techniques, and procedures.
- » Secure analysis environments that prevent exposure of critical systems.
- » Actionable outputs that integrate with SIEM, SOAR, and case management platforms.

With HONEYPOT360, intrusions are no longer silent risks - they become opportunities to understand adversaries, strengthen defenses, and shorten response times.

In an environment where threats continue to evolve, HONEYPOT360 provides a decisive advantage: intelligence derived directly from the adversary's own actions.

\$ 4 . 8 8 M

Average global cost of a breach (IBM)

1 1

DAYS

Global median dwell time (Mandiant)

5 7 %

Compromises first identified externally (Mandiant)

6 2

MINUTES

Average time from initial host to lateral movement (CrowdStrike)

1 3 %

Projected growth rate of deception technology market through 2030

OUR SOLUTION

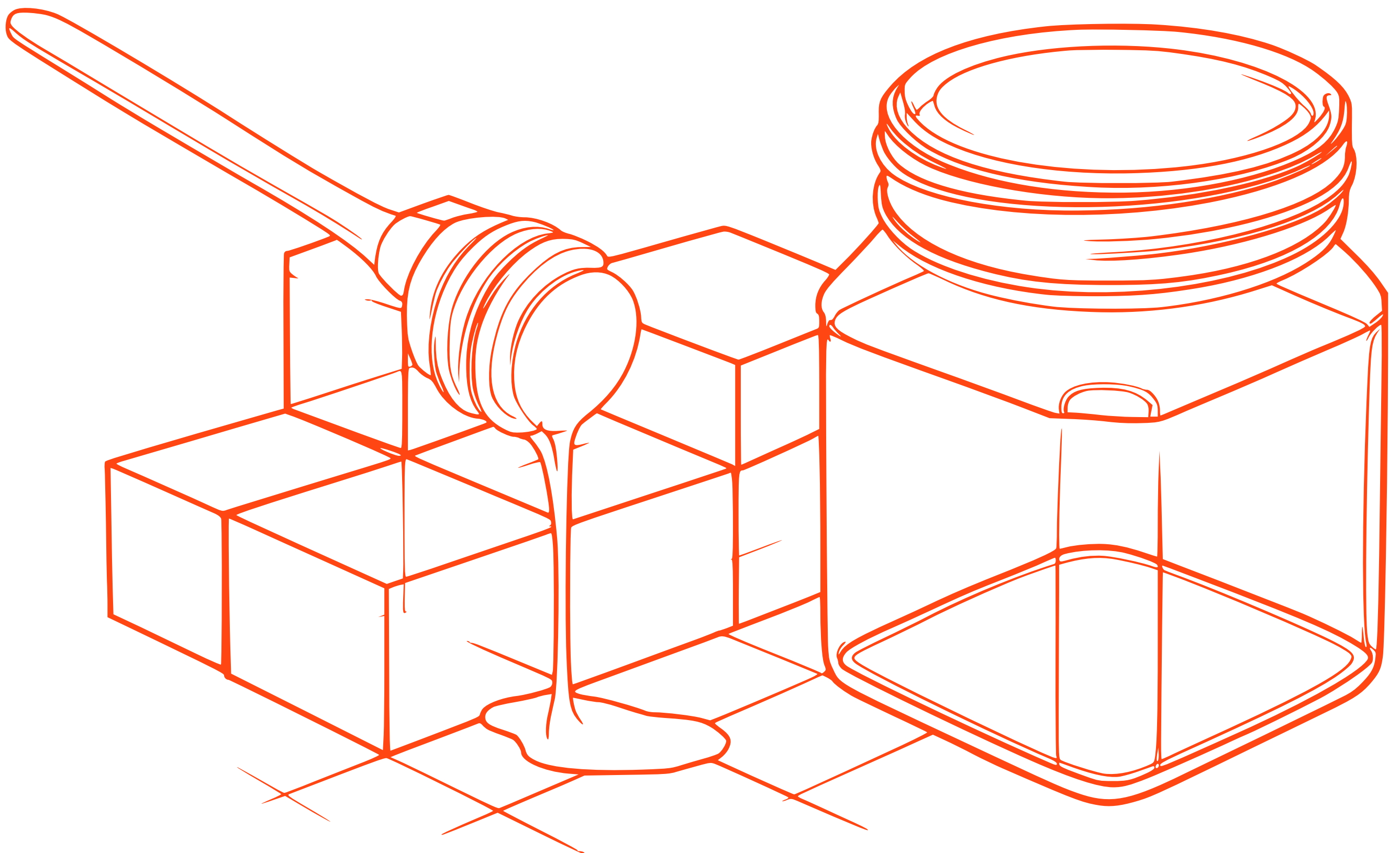
HONEYPOT360 provides organizations with a clear and intelligence-driven way to address the blind spots left by traditional defenses.

At its core, HONEYPOT360 uses deception to create convincing decoy environments that mimic real systems, services, and data. These decoys are strategically placed across the network to attract intruders and divert them away from valuable assets. Inside these controlled spaces, every action can be observed, analyzed, and turned into intelligence - revealing who the attackers are, what they want, and how they operate, while giving defenders valuable time to act before real harm is done.

Unlike conventional detection tools, HONEYPOT360 goes beyond simply raising alerts. It converts attacker behavior into actionable intelligence. As adversaries engage with decoys, the platform captures their tools, techniques, and movement patterns in real time. This context allows security teams to see the full scope of an intrusion, respond with speed and confidence, and continuously improve their defenses.

HONEYPOT360 is built to work with the stack you already trust. Intelligence from decoys flows directly into your SIEM for visibility and SOAR for automation. This means teams can respond faster without changing workflows. Because the interaction happens in a controlled space, the signal-to-noise ratio stays high, false positives stay low, and every engagement carries real investigative value that helps prioritize resources and sharpen decision-making across security operations.

In practice, HONEYPOT360 detects intrusions earlier, shortens the time attackers can stay hidden, and improves incident response. Over time, repeated engagements help harden defenses and strengthen your entire security architecture. Rather than replacing existing controls, HONEYPOT360 enhances them - delivering visibility where it matters most: inside the network, where attackers try to hide.



FEATURES

HONEYPOT360 provides organizations with a controlled and intelligence-driven way to observe adversaries inside the network. By deploying realistic decoys, the platform ensures that intruders interact with what appears authentic, while defenders capture every step in a safe and monitored environment.

- » **Multi-Layer Deception**

Coverage across network, endpoint, application, and identity layers with decoys designed to be indistinguishable from production assets.
- » **Centralized Management Console**

A unified planning, deployment, health and analytics views that let SOC teams design and operate deception at enterprise scale.
- » **High-Confidence Alerting**

Signals generated only from verified decoy interaction, reducing false positives and directing analysts to meaningful activity.
- » **Forensic Logging and Reply**

Integrity-protected event trails and full session playback that supports investigation, training, and post-incident review.
- » **Integration and APIs**

Seamlessly integrate with SIEM, SOAR, and threat intelligence platforms to enrich wider security operations.
- » **Adaptive Decoy Design**

Decoys can be tailored to mimic specific operating systems, applications, and environments, increasing realism and engagement effectiveness.

BENEFITS

HONEYPOT360 transforms security operations by turning live intrusion attempts into structured, actionable intelligence. The result: earlier detection, faster response, and continuous security improvement, all while reducing attacker dwell time and risk to production systems.

- » **Earlier detection**

Exposure of lateral movement within minutes of engagement, compressing attacker dwell time and limiting operational impact.
- » **Actionable Adversary Insight**

Clear visibility into attacker behavior, methods, and objectives enabling focused and proportionate response actions.
- » **Operational Efficiency**

Lower alert noise and higher signal quality that focus analyst time on verified threats and shorten investigation cycles.
- » **Continuous Resilience**

Each engagement brings insights that strengthen defenses, refine playbooks, and strengthen the architecture over time.
- » **Low-Impact Deployment**

Lightweight implementation alongside existing defenses - minimal change management, zero disruption.
- » **Reduced risk**

Diversion of intruders away from critical systems into safe, controlled environments that protect production while yielding intelligence.

ORYXLABS

WHO WE ARE

ORYXLABS was founded in Abu Dhabi in 2020 with a passion for cybersecurity-focused engineering.

A proudly diverse staff hailing from 22 different countries with backgrounds ranging from national defense to world-renowned top software engineering organizations joined together to develop best-in-class security solutions.

We leverage research and innovation to provide solutions in four key areas:

- » Cyber Security Assessment
- » Monitoring
- » Prevention
- » Improvement

When combined, ORYXLABS solutions provide a holistic approach to situational awareness and attack mitigation.

OUR MISSION

Our mission is to equip cybersecurity teams with first-in-class intelligence and technical solutions that continuously assess, monitor, and improve environments to mitigate ongoing or future attacks.

WHY US

As an agile and innovative company focused on cybersecurity, we pride ourselves on crafting highly tailored solutions to meet our clients' exact needs, not "one size fits all" products like our competitors in the domain.

With our combined experience in deep learning, AI, vulnerability research and big data, and partnerships with world-renowned subject matter experts, you can rest assured our solutions are built and run on information that is timely and accurate.

COMPANY AWARDS



2025
Most Innovative
CyberSecurity
Company

CyberSecurity
Excellence Awards



2023
Most Innovative
CyberSecurity
Company

CyberSecurity Excellence
Awards



2024
Most Innovative
CyberSecurity
Company

CyberSecurity
Excellence Awards



2022
Top CyberSecurity
Solutions Provider
Middle East

Enterprise Security



WEBSITE

Scan to view



VIDEO

Scan to view



21st Floor, Aldar HQ
Al Raha Beach
P.O. Box: 33289
Abu Dhabi, UAE

oryxlabs.ae