The Illusive Active Defense Suite with Cortex XSOAR

High-Fidelity Threat Detection to Accelerate Response

Pinpoint threats with high fidelity at their earliest point in the post-breach attack lifecycle and automate immediate remediation and quarantine in response. Leverage customized Illusive Active Defense Suite playbooks designed especially for Cortex XSOAR to instantly see how far attackers are from critical data, significantly cut response times, and save your SOC from burnout and false positives.

How Illusive and Cortex XSOAR Work Together to Make Threat Detection SOAR

PLAYBOOK 1

Incident Data Enrichment

Receive comprehensive, automated, and source-based forensics about the machine where the attacker is located, including a timeline of all attacker actions associated with the incident, screenshots of the incident as it was taking place, and data about which credentials and endpoints are being used in the attack.

PLAYBOOK 2

Incident Escalation Automation

Combine Illusive forensics with Cortex XSOAR correlation rules to measure risk, see attacker proximity to critical assets, and automate rapid incident escalation to the correct tier.

With Illusive Networks and Cortex XSOAR working in tandem, your organization reaps the following advantages:

- Collect source-based forensics to determine which alerts truly matter
- Reduce average response time from hours to minutes
- Configure risk threshold scores for automated incident escalation
- First and only deception solution available through the Palo Alto Networks Cortex XSOAR Marketplace

CORTEX XSOAR BY PALO ALTO NETWORKS

How Illusive and Cortex XSOAR Work Together to Identify and Manage Threats

Ingests source IP and host name, and a risk threshold is triggered → **Collects Illusive intelligence about compromised host users and attacker location relative to critical data** → **Retrieves Illusive's comprehensive forensic artifacts from the incident** → **Containment performed according to correlation rules**

Save the SOC: Efficient Threat Detection for More Effective Containment

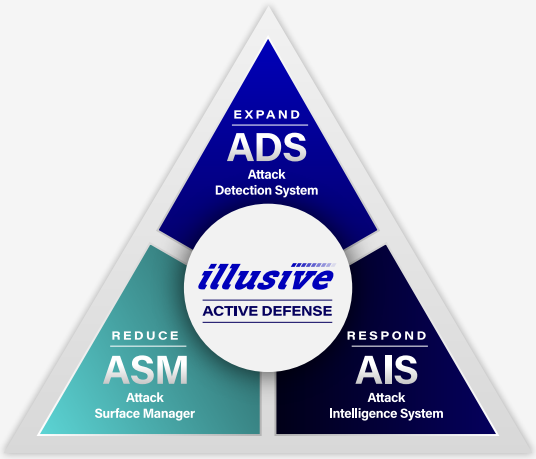
The "new abnormal" of employees compelled to telecommute was never contemplated by the algorithms and rule-writers underpinning behavior-based threat detection. With no baselines to rely on, alert volume and false positives have exploded. A new strategy is needed to cut through the noise.

Illusive attack surface management lets organizations find and remove unnecessary and leftover credentials and connections that attackers use to move laterally after a breach. Then, Illusive deception replaces those credentials and connections with illusory versions of the data attackers would expect to find and exploit. Once attackers attempt to use that deceptive data to move laterally, they are caught in the act, with full forensic evidence provided.

The Illusive integration with Cortex XSOAR can automate the prioritization of the riskiest threats identified by Illusive for mitigation and quarantine, providing a "Save the SOC" playbook collection for efficient incident detection and response no matter how our daily routine and the threats targeting it evolve.

Built by Attackers to Stop Attackers

Illusive's Active Defense Suite is a vital part of a diversified detection strategy, filling an important attacker lateral movement detection gap in existing perimeter defenses. Each of the products in the Illusive Active Defense Suite play an important role in preventing attackers from achieving their objectives by creating a hostile environment and accelerating the time to detection for an attacker that has established a beachhead.



Illusive and Cortex XSOAR in Collaboration: Key Benefits

- Trigger automated source-based forensics for any incident in your Cortex XSOAR platform
- Streamline intelligence about attacker proximity to critical assets for more efficient alert prioritization
- High-fidelity threat detection that doesn't require signatures and eliminates false positives
- Use forensics to free up tier 3 analysts for most pressing threats and downshift the rest
- Expand response capability through more sensitive detection and automated workflows

About Illusive

Illusive reduces cyber risk by shrinking the attack surface and stopping attacker movement. Despite significant investments, it's still difficult to see and stop attackers moving inside your environment. Illusive was founded by nation-state attackers who developed a solution to beat attackers. We help Fortune 100 companies protect their critical assets, including the largest global financials and global pharmaceuticals. Illusive has participated in over 130+ red team exercises and has never lost one! To learn more, visit **www.illusive.com**

About Cortex XSOAR

Palo Alto Networks Cortex™ XSOAR supercharges SOC efficiency with the world's most comprehensive operating platform for enterprise security. Cortex XSOAR unifies case management, automation, real-time collaboration, and threat intelligence management. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security use case - resulting in 90% faster response times and a 95% reduction in alerts requiring human intervention.