illusive® CORTEX XSOAR BY PALO ALTO NETWORKS

High-Fidelity Threat Detection to Accelerate Response

The Illusive Platform with Cortex XSOAR

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 Platform 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.

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

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.

1. Cortex XSOAR ingests source IP and host name, and a risk threshold is triggered
2. Cortex XSOAR collects Illusive intelligence about compromised host users and attacker location relative to critical data
3. Cortex XSOAR retrieves Illusive's comprehensive forensic artifacts from the incident
4. Cortex XSOAR 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.

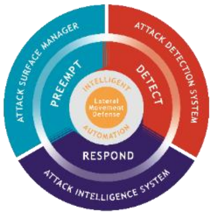
Illusive attack surface management lets organizations find and remove unnecessary and leftover credentials and connections that attackers use to move laterally after a breach. Then, Illusive deception replaces those credentials and connections with illusory versions of the data attackers would expect 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.

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

The Illusive Platform provides centralized management across even the largest and most distributed environments. Three modular components can work together or be operated separately to preempt, detect, and respond to cyberattacks.



Preempt: Finds and removes errant credentials, connections, and attack pathways to deter unauthorized lateral movement.

Detect: Forces attackers to reveal themselves early in the attack process by disorienting and manipulating their decision-making.

Respond: Enables rapid, effective response and remediation when attackers are present by providing contextual source and target forensics.

ABOUT ILLUSIVE

Illusive Networks stops attack movement from anywhere to anywhere by creating a hostile environment for attackers. Illusive shrinks the true attack surface to preempt attacks, creates the illusion of an expanded attack surface with deceptions for early detection of attacks in motion, and provides rich, real-time forensics that speeds response with actionable insights.

Agentless and intelligence-driven, Illusive deception technology enables organizations to avoid operational disruption and business losses by proactively intervening in the attack process so they can function with greater confidence in today's complex, hyper-connected world.

ABOUT PALO ALTO NETWORKS

Palo Alto Networks Cortex^{TM} 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.

Visit us at www.illusivenetworks.com

Email us at info@illusivenetworks.com

Call us at +1 844.455.8748 (North America)
or +972 73.272.4006 (EMEA and AsiaPac)

Engineered by people steeped in nation-state cyber intelligence and defense, we are here to help! See a demo or discuss steps for a free Attack Risk Assessment at info@illusivenetworks.com