LUPOVIS

Turn your network from a flock of sheep to a pack of wolves

National Cyber Security Centre
For Startups
Alumni

Lupovis

Making cyber deception and contextual threat intelligence affordable and accessible to all cybersecurity teams.

WHY DECEPTION, WHY NOW?

A study highlighted by Help Net Security reveals that SOC teams face significant challenges, receiving an average of 4,484 alerts daily, with nearly three hours spent on manual triage. Shockingly, 67% of these alerts cannot be addressed, and 83% are false positives. This scenario underscores the overwhelming volume and inefficiency plaguing cybersecurity efforts.

This inefficiency contributes to longer adversary dwell times, often reported to be several months before detection. These statistics underscore the need for more efficient and accurate security solutions to reduce false positives and improve detection times.

WHY DIDN'T WE DETECT?

We can help you avoid this question from your CEO...

We deploy decoys, lures, targets inside and outside your network, these act as low-hanging fruits for adversaries, helping you detect pre-breach and post-breach events without false positives.

WITHOUT FALSE POSITIVES, YOU SAY?

That's right, see decoys shouldn't be interacted with from legitimate users, hence an alert on a decoy, should automatically raise a question.

Furthermore, the versatility of deception, allows detecting rogue employees, insider threats, ransomware groups, etc.

WE LITERALLY TURN YOUR NETWORK FROM A FLOCK OF SHEEP TO A PACK OF WOLVES

- Source: https://www.helpnetsecurity.com/2023/07/20/soc-analysts-tools-effectiveness

Lupovis Snare

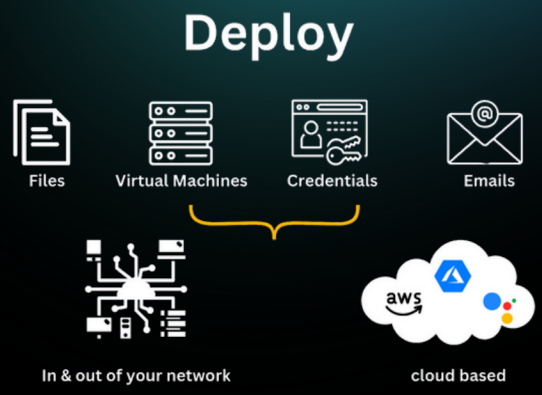
DECEPTION PLATFORM

Snare is a state-of-the-art SaaS-based platform, expertly crafted to deploy an array of decoys within minutes, transforming your network from a flock of sheep to a pack of wolves. By weaving a web of meticulously designed lures, Snare presents potential intruders with low-hanging fruits, while in reality, it's a controlled environment for detection, monitoring and analysis.

At the heart of Snare strategy is the concept of 'lures'. These are sophisticated, virtual entities that seamlessly blend into your network's fabric. Each lure is replicating network components like servers, applications, and services. They are indistinguishable from real elements in your infrastructure, presenting an array of tempting targets to would-be attackers.

Once an attacker engages with these lures, Snare springs into action. It tracks the intruder's movements, recording their methods, the tools employed, and the vulnerabilities they seek to exploit. An alert is then raised to your team.

Snare is not just a security platform; it's a proactive guardian, creating a dynamic, deceptive landscape where every action by a potential attacker is a step towards their own downfall.



INTEGRATIONS

splunk>

Microsoft Azure Sentinel

IBM QRadar

FORTINET

AND MORE

Lupovis Snare

PROBLEM

FALSE POSITIVES

Conventional security systems often inundate teams with a relentless stream of alerts, leading to a state of constant overload. These constant notifications result in event fatigue, a condition where critical signals are lost amidst a sea of data, resulting in paralysis and the overlooking of vital alerts. This issue is widespread and significant.

Any interaction with a Snare decoy is suspicious in nature, making it extremely effective in detecting attacks irrespective of tools or tactics used.

NETWORK VISIBILITY

In today's environment of intricate and expansive networks, businesses often find themselves with limited visibility beyond their own perimeter defenses. This lack of transparency significantly hampers their ability to identify and respond to intrusion attempts effectively.

Decoys and lures placed across the network detect intrusions giving you unparalleled visibility into malicious activities in your network.

CONTEXTUAL INTELLIGENCE

With network boundaries increasingly blurred, many organizations face the challenge of having negligible insight into external threats. This blind spot outside their network perimeter leaves them vulnerable, as they are unable to see or predict who might be targeting them. This lack of external visibility not only hinders their ability to proactively defend against potential attackers but also limits their understanding of the evolving threat landscape they are operating in.

Lupovis allows for decoys to be placed at the boundary of your network to detect humans during the reconnaissance phase of an attack. Drastically improving response time and ignoring the noise.

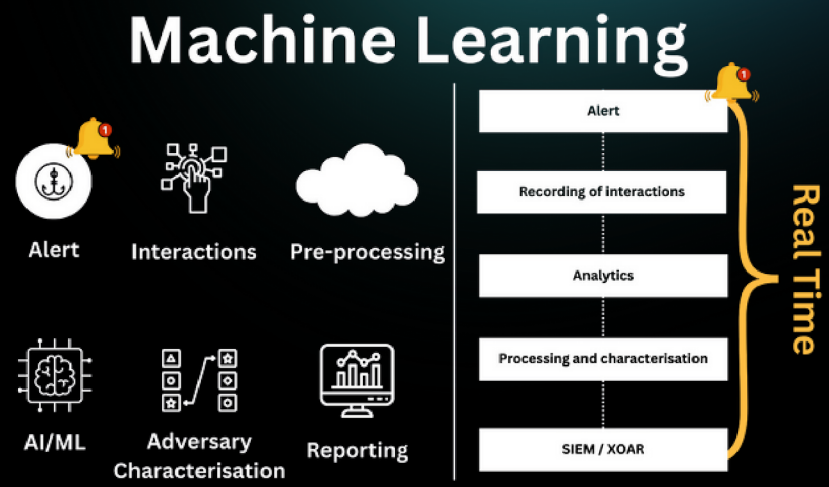
Lupovis Snare

WHY SNARE

- Offers a unique, customized defence against targeted threats.
- Able to detect ransomware attacks and adversaries stealing data.
- Native integrations with security solutions for automated response.
- 10 minutes deployments of a full deceptive environment
- No-code solution, no training required, deploy and forget
- Benefit from our global threat intelligence feed

DECOYS SUPORTED

- External Decoys
- Internal Decoys
- Operational Decoys
- Cloud Decoys
- IoT Decoys
- Network Decoys
- File Decoys



LUPOVIS

Lupovis provides precise, high-fidelity threat identification with a drastically reduced alert to noise ratio through a SaaS Deception as a Service platform.

Gain targeted, contextual intelligence specific to your company. Stay steps ahead with insights that pinpoint insider threats, and pre-breach events such as leaked credentials. Dive into actionable intelligence without the distractions.

Email: hello@lupovis.io
Phone: +44 770 015 8050
Web: https://www.lupovis.io

National Cyber Security Centre
For Startups
Alumni