KOGNOS
never hunt alone

Kognos for MSSPs

KOGNOS XDR AUTOMATION SUITE

THE FIRST AND ONLY PLATFORM TO LEVERAGE THE POWER OF RELATIONSHIPS TO TRACE THE ATTACKER'S PATH IN REAL-TIME

The cybersecurity skill shortage and analyst burnout has forced many organizations to rely more on MSSPs to augment their limited workforce. However, it is a very competitive market and margins are consistently diminishing. MSSPs have to continually improve operational efficiencies, but more importantly, have to aggressively offer innovative solutions as an upsell to existing customers to improve their top-line.

Kognos upsell opportunities

Enterprises are struggling with vendor fatigue, data fatigue, and alert fatigue. Automation and integration are key to solving these problems. With Kognos' suite of autonomous solutions, MSSPs can offer a plethora of offerings as an upsell to existing customers.

- Premium offering for lower MTTD/MTTR
- Autonomous EDR Hunt offering
- Autonomous XDR Hunt offering
- Autonomous Alert Triage/Investigation offering
- Autonomous Incident Response offering

Premium offering for lower MTTD/MTTR (In Minutes)

Most MSSPs still rely heavily on manual or semi-automated investigations. As a result, alerts take longer to investigate, contextualize, and report back to the end-customer. Similarly, some MSSPs offer packaged hunting offerings, but equally suffer from the iterative and time-consuming manual processes. Due to this, adversaries are in the environment for much longer and there is no real-time visibility into attacker activity, ultimately increasing the MSSP's MTTD and MTTR. MSSPs can provide a better MTTD/MTTR offering with the Kognos autonomous solutions, allowing for machine speed detection, investigation, and mitigation. This will drastically reduce the MTTD and MTTR to minutes as threats are continuously being investigated and presented as fully contextualized and pre-investigated visual attack campaign storylines.

KOGNOS
never hunt alone

Kognos for MSSPs

Autonomous EDR Hunting as a service

Enterprises are using Endpoint Detection and Response products to protect their environment that produce hundreds of terabytes of important security telemetry. However, most organizations are not able to make effective use of this telemetry. The data volume is so overwhelming that manual hunting processes are a non-starter. The Kognos autonomous EDR hunt offering understands Carbon Black, CrowdStrike, Sysmon, AuditD, and OpenBSM telemetry, and autonomously hunts for any artifact or behavior without the hunt team having to mine through the telemetry data sets. This can be offered to customers who have these EDR products deployed and be used for hunting suspicious living off the land binaries, suspicious lateral movement tool usage, suspicious persistence mechanisms in use, and more. Kognos then generates and presents these risky activities into pre-investigated visual storylines to your hunting team.

Autonomous XDR Hunting as a service

Enterprises most often have different best of breed products deployed including SIEM, NTA/NDR and EDR products however these products have their own data siloes and hunting can take the hunter from product to product. Kognos XDR hunt solution can seamlessly connect into existing SIEMs, EDR, NDR platforms creating an XDR middleware layer. This allows the system to autonomously hunt for threats across the various platforms generating pre-investigated visual storylines of all risky activities.

Autonomous Alert Triage/Investigations as a service

Alert overload is faced by most enterprises and this is handled by the MSSP or by the enterprise security team depending on the SLA. In the latter case, the Kognos autonomous XDR investigator can be provided to the customers which will ingest alerts from different alert sources and do a fully autonomous investigation for each alert. This removes all manual effort from alert triage and investigations, doing fully autonomous investigations at machine speeds contextualizing the alert at and generating pre-investigated visual storylines in real-time.

Autonomous Incident Response as a service

Incidents do happen from time to time in an enterprise environment and MSSPs often participate in quick incident resolution. Most often the collected evidence needs to be

documented and an Incident report generated for legal/compliance reasons. Kognos XDR investigator can be used to do forensic investigations at machine speeds and generate incident reports without the MSSP or the enterprise having to do it manually.

Kognos MSSP Margin Improvements

Depending on the SLA with customers, some or all of the above functions can be done by the MSSP. In which case all the cost associated with alert overload, heterogeneity of security appliance, volume of telemetry and lack of effective automation multiplied by the number of customers become a hit on the MSSP margins. All above offerings can be applied internally to improve and up level the MSSP practice.

The main operational improvements for an MSSP includes alert investigations and response which can be a major hit into the MSSP margins if the SLA includes alert triage and monitoring. With Kognos XDR Investigator MSSPs can:

1. Reduce triage/investigation time for alerts by 90%
2. Reduce false positives by 95%
3. Reduce post-breach investigation from days/weeks to hours
4. Agnostic to underlying tools as Kognos provides single pane of glass across all MSSP customers giving a simplified and unified layer for the MSSP analysts.
5. Enable junior analysts to do complex analysis using the Kognos autonomous offerings

All of the above functions allow the same MSSP team to add many more customers as the automation suite provides an order of magnitude more of analyst to customer ratio. Also provides 24/7 x 365 hunting and investigations without having to man the SOC with multiple shifts.

KOGNOS
never hunt alone

Kognos for MSSPs

MSSP Features

- Cloud and On-premise options
- Multi-tenant Deployment
- Elastic and Scalable Solution
- Supports Multi-Geography Sources
- Federated Intelligence
- Extensible AI & Investigation Queries
- Extensible Data source Integrations

Integrations

Kognos Autonomous XDR Investigator supports the following integrations and more in the roadmap. Please reach out if you have a specific integration request.

Data sources	**EDR**	**Network Data**	**Application/ Cloud Logs**	**Threat Intelligence**
Splunk	Carbon Black	BRO	AWS Cloud Trail Cloud watch	VirusTotal
Elastic	CrowdStrike	Snort Suricata SecurityOnion	Azure Audit Events Azure Security Events	ThreatCrowd
NetWitness	Sysmon	NetWitness	Nginx, Apache, IIS	ThreatMiner
File Logs	AuditD	FW Logs	Domain Controller Logs	Carbon Black
Rest API	OpenBSM	IDS/IPS logs	DNS Logs	Integrations with custom feeds
SQL DBs Rocks DB MySQL Amazon S3 Buckets			Proxy Logs	Cymru

KOGNOS
never hunt alone

Kognos for MSSPs

Become a Partner Today

Please request a demo via our website at https://www.kognos.io/book-a-demo/.