CYBOTS

ADVANCED MANAGED DETECTION AND RESPONSE (AMDR)

FAST | ACCURATE | SIMPLE | THOROUGH

F Our lightweight agent continuously detects, eradicates and remediates issues, drastically reducing your MTTD and MTTR to prevent security incidents from evolving into business-altering events—all provided by the collaboration between our expert analysts, virtual forensic analyst AI and our attacker behavior modeling technology.

A We provide automated forensic analyses not just across multiple levels of contexts but also into the intricate relationships between each of those levels of context

S Receive regular in-depth reports on the current state of your entire network. Cybots AMDR Services Team is available to walk you through your fully-actionable reports step by step, explaining each step simply and clearly.

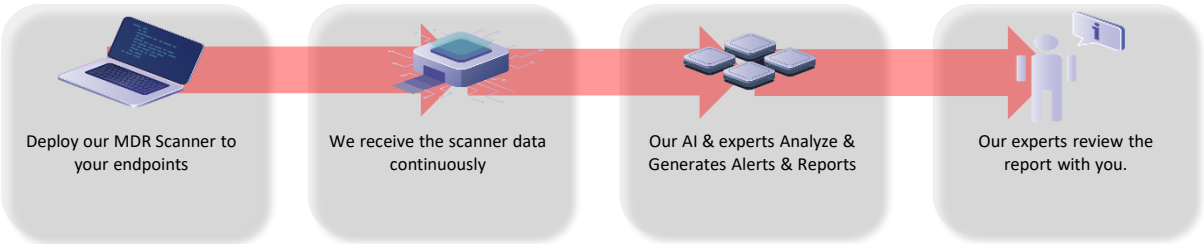
T We rescan and confirm eradication with cyber threat intel from multiple major proprietary sources and organizations across the globe, as well as the rigorous AI-driven vetting process of our Cyber Threat Intelligence

ADVANCED MANAGED DETECTION AND RESPONSE (AMDR)

Cybots Advanced MDR is unique in its accuracy in detecting malicious behavior. We are able to continuously monitor and manage the cyber situation of even large-scale enterprises with thousands of endpoints. Unlike other services, we generate fully actionable reports, review them with you step-by-step and confirm eradication of threats.

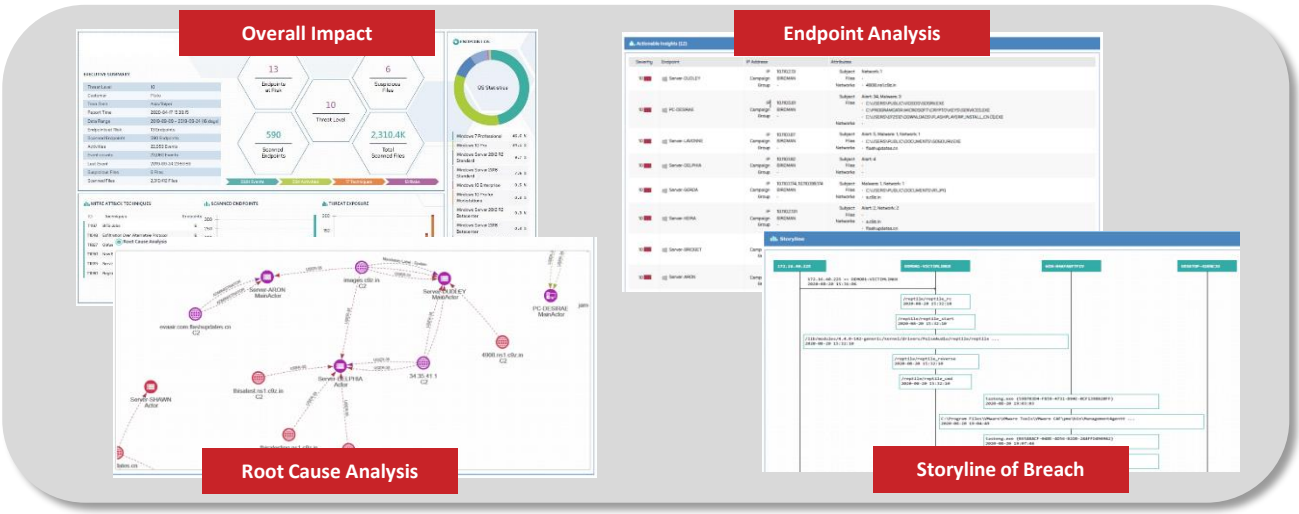
Our Approach - Step 1 and Final Step

Install lightweight Agents on all workstation and servers



Holistic Response Plan within Minutes

Breach and Full root-cause-analysis done by AI-powered correlation engine within minutes. Complete response plan to eliminate even Advanced Persistent Threats (APTs).



Our Deliverables

- Full storylines of any & all hacker activity
- True global root cause analysis
- Malicious domain, IP, URL analysis
- List & behavior of suspicious user accounts
- Graphs of all affected nodes & executions
- Malware analysis
- A plan for eradication
- Eradication confirmation
- MITRE ATT&CK mapping

Cybots AMDR will provide 24 x 7 threat hunting services and can help you save money on labor. This allows your data security personnel the time to focus on important tasks.

Cybots AMDR vs Other Cyber Security Solutions

	CYBOTS	Normal EDR	AV	SIEM
Time to Get to True Root Cause	<1 day	Days to Weeks	N/A	Days to Weeks
Amount of Querying	Zero	Tons	N/A	Tons
Value to Your Organization	High	Mid	Low	Mid to Low
Ease of Actionability	Easy	Hard	Easy	Hard
Ability to Show Full Situation	High	Mid to Low	Low	Low

Consult our cybersecurity experts today!

The Cybots team is here to be your cybersecurity partner, whether it's the Initial Assessment, Managed Services or Cybersecurity Products.

THE CYBOTS DIFFERENCE

Cybots AMDR Standard vs. Enterprise vs. Premium

Keep pace with continually evolving adversarial tactics and techniques and enjoy the benefits

- 24 x 7 threat hunting of installed endpoints
- Productivity Gains
- Enhanced IT user experience
- Eliminate >90% “false positives”, reducing load of IT security staff dedicated to this area
- Reduce staff fatigue with the power of AI
- Increased compliance

Product Features	Standard	Enterprise	Premium
24x7 Monitoring	Yes	Yes	Yes
Scan every endpoint, process, file	Yes	Yes	Yes
IAM (Identity Access Management) across entire network	Yes	Yes	Yes
Automated investigations triggered upon detection of a high severity alert (level 7 – 10)	Yes	Yes	Yes
Delivers full site-wide forensic analysis by AI	Yes	Yes	Yes
Additional analysis by human security analysts	No	No	Yes
Link each step of the attack	Yes	Yes	Yes
Provide full context for each step of the attack	Yes	Yes	Yes
Report that informs which processes to stop	Yes	Yes	Yes
Identify files to delete	Yes	Yes	Yes
Identify Malware to remove	Yes	Yes	Yes
List of infected user accounts	Yes	Yes	Yes
List of URLs, IP addresses, domains to block	Yes	Yes	Yes
Threat Hunting Alerts			
Detection time for cyber threat	90 mins	45 mins	15 mins
Cyber Situation Reports*			
Auto Generated Actionable Report	Yes	Yes	Yes
Generation time for Cyber Situation Report	24 hours	12 hours	6 hours
Full storylines of any & all malicious activity	Yes	Yes	Yes
Malicious domain, IP, URL analysis	Yes	Yes	Yes
Malware analysis	Yes	Yes	Yes
Graphs of all affect nodes and executions	Yes	Yes	Yes
Step-by-step plan for eradication	Yes	Yes	Yes
Eradication confirmation	Yes	Yes	Yes
Root cause analysis	NA	NA	Yes
Global Cyber Threat Intelligence	NA	Yes (Monthly)	Yes (Weekly)
MITRE ATT&CK mapping	NA	NA	Yes
Analyst Recommendation & Interpretation on report	Chargeable man hour	Limited support	Full support
Sample Report	**EDR Threat Hunting Alert Cyber Situation Report (AI)**	**Asset Analysis Report Cyber Situation Report (AI)**	**Asset Analysis Report Cyber Situation Report**

*action report only available when cyber situation arises