

Top 15 **AI** Tools for **CYBERSECURITY PROFESSIONALS**



VECTRA AI

- **Focus:** Hybrid/network threat detection
- **Tech:** Deep learning for detecting privilege escalation, credential misuse
- **Use Case:** SOC threat hunters tracking advanced persistent threats (APTs)



PENTERA

- **Focus:** Automated penetration testing
- **Tech:** AI simulates exploitation chains, lateral movement
- **Use Case:** Red Team validation of exploitable vulnerabilities at scale



BLOODHOUND ENTERPRISE

(WITH AI ANALYTICS)

- **Focus:** Active Directory attack path mapping
- **Tech:** Graph-based AI to model privilege escalation
- **Use Case:** Red Teams & CEH pros testing domain privilege abuse



CAI

(COGNITIVE AI FOR SECURITY)

- **Focus:** Automated bug bounty and pentesting
- **Tech:** Multi-agent AI for recon, scanning, and exploit generation
- **Use Case:** Penetration testing augmentation, vulnerability discovery

CAI[®]



CYLANCE (BLACKBERRY)

- **Focus:** Predictive malware prevention
- **Tech:** AI-driven static analysis, pre-execution blocking
- **Use Case:** CEH labs, SOC malware defense, ransomware mitigation



FORTIAI

- **Focus:** Zero-day malware detection
- **Tech:** Deep neural networks for sample classification & response
- **Use Case:** SOC malware analysis automation, incident containment



RELIAQUEST GREYMATTER

- **Focus:** XDR and detection engineering
- **Tech:** AI-driven log correlation, response playbooks
- **Use Case:** SOC automation, scaling incident response workflows



MALTEGO

(WITH AI ENRICHMENT)

- **Focus:** OSINT + link analysis
- **Tech:** AI plugins to classify entities, detect malicious infra patterns
- **Use Case:** Red Team reconnaissance, CEH investigations



CYBLE VISION

- **Focus:** Dark web and threat intelligence
- **Tech:** AI scrapes and analyzes forums, markets, and paste sites
- **Use Case:** SOC threat intel feeds, early warning of leaked credentials



PURPLE LLAMA (META)

- **Focus:** LLM Security Guardrails
- **Tech:** Input/output filters, adversarial prompt defenses
- **Use Case:** Protects SOC/Red Team using generative AI in engagements

Llama



VASTAV.AI

- **Focus:** Deepfake and synthetic media detection
- **Tech:** AI forensic analysis on image/audio/video metadata
- **Use Case:** SOC fraud detection, Red Team media forensics



DARKTRACE

- **Focus:** AI-driven anomaly detection
- **Tech:** Self-learning ML for baselining network/cloud/email traffic
- **Use Case:** Detects insider threats, lateral movement, and zero-day exploits



IBM QRADAR SUITE

- **Focus:** SIEM + UEBA with AI
- **Tech:** Event correlation + behavioral analytics
- **Use Case:** Reduces SOC false positives, accelerates incident triage



CROWDSTRIKE FALCON

- **Focus:** EDR/XDR platform
- **Tech:** ML-based detection, real-time threat intel, automated containment
- **Use Case:** Endpoint defense, rapid remediation of malware and ransomware



SENTINELONE SINGULARITY

- **Focus:** Endpoint + cloud AI security
- **Tech:** Autonomous detection, storyline-based attack visualization
- **Use Case:** SOC teams handling large-scale endpoint telemetry



KEEP LEARNING WITH



INFOSECTRAIN

Educate. Excel. Empower.



Like



Comment



Share



www.infosectrain.com



sales@infosectrain.com