Agentic AI-Enabled Managed Detection and Response

Kroll Responder combines Kroll's incident response expertise with CrowdStrike technology and managed services to deliver human-led, AI-enabled detection, response and remediation.

Outpace AI-Powered Threats with AI-Driven Defense

As attackers accelerate using automation, compromised credentials and multi-domain techniques, alert triage alone is no longer enough. Organizations need MDR that delivers speed, scale and intelligence.

Kroll Responder MDR combines CrowdStrike technology with Kroll's incident response expertise, digital forensics and AI-enabled response engineering to help enable faster detection, deeper investigation and more consistent response.

Key Insights on Today's Threat Landscape

- **85% of attack operations are automated:** Attackers are using automation to move faster, increasing the need for AI-enabled response.
- **82% of attacks were malware-free:** Threat actors increasingly use legitimate tools and hands-on-keyboard techniques to evade traditional detection.
- **80% used compromised credentials:** Identity-based attacks allow threat actors to bypass defenses by appearing as trusted users.

Operationalizing Agentic MDR with Kroll Responder and CrowdStrike Falcon Complete

Unify and Optimize Visibility

Establish full attack surface telemetry across endpoint, identity, cloud and SIEM.

CrowdStrike enables: Unified platform visibility across key security domains

Kroll delivers: Agile log source onboarding, mapping and visibility optimization

AI-Driven Detection and Automated Triage

Use Falcon and Charlotte AI to reduce alert noise and focus on high-fidelity signals.

CrowdStrike enables: AI-driven detection, Charlotte AI and managed SOC operations

Kroll delivers: Investigation and triage informed by frontline incident response experience

Response Engineering and Deep Forensics

Build agentic SOAR workflows and conduct deep root cause analysis to improve response.

CrowdStrike enables: SOAR technology, automation and response actions across security domains

Kroll delivers: Agentic workflows, remote digital forensics, root cause analysis and remediation guidance

Strategic Optimization and Value Realization

Communicate service efficacy, security posture and operational value through reporting and dashboards.

CrowdStrike enables: Platform reporting and operational insights

Kroll delivers: Service efficacy reporting, executive-ready insights, continuous optimization, expert delivery and service support

KROLL | CROWDSTRIKE

What Kroll Responder MDR Delivers

A unified MDR service combining CrowdStrike Falcon Complete and Overwatch proactive threat hunting with remote digital forensics, engineered defence, and agentic AI workflows.

24x7 Threat Detection, Investigation and Response
AIways-on detection, investigation and response through CrowdStrike Falcon Complete, supported by Kroll's incident response-informed expertise.

Remote Digital Forensics and Root Cause Analysis
Kroll Response Operations provides remote digital forensics and root cause analysis to help determine how threats entered, moved, and persisted.

AI-Enabled Cross-Domain Response Actions
AI-enabled response actions across endpoint, identity, email and cloud help accelerate containment and reduce manual effort.

Tailored Agentic AI Workflows and Response Engineering
Kroll Engineered Defense supports Fusion SOAR agentic AI workflows, custom playbooks and response engineering.

Integrated Threat Intelligence
Kroll and CrowdStrike threat intelligence enriches investigations with adversary context, helping teams prioritize activity, understand attacker behavior and guide response.

Expert Deployment, Service Management and Platform Support
Kroll supports deployment, platform optimization and ongoing service alignment, with Customer Success Managers providing a consistent point of coordination across onboarding, service reviews, reporting and continuous improvement.

Why Kroll

Kroll delivers MDR with the practitioner expertise, forensic insight and operational support needed to improve detection, response and resilience.

- IR-led delivery informed by real-world breach response
- Forensic depth to investigate threats beyond the initial alert
- Response engineering expertise to operationalize AI-enabled workflows
- Platform guidance to align CrowdStrike capabilities to the customer's environment
- Ongoing optimization supported by Customer Success Managers and Redscan Portal visibility
- Added peace of mind through Kroll's $1M Incident Protection Warranty, where applicable

Key Outcomes

- Faster detection and response supported by 4-minute MTTD and 37-minute MTTR
- Lower breach impact
- Reduced responsibility gaps during incidents
- Improved efficiency through AI-enabled automation
- Stronger visibility across key security domains

Kroll is a Leader in Cyber and Data Resilience

World's largest incident response provider, handling **thousands** of cyber incidents annually

140k+ hours of penetration testing and red teaming annually

Trusted by leading **enterprises, insurers and regulated organizations** worldwide

Experience from **Govt. & Law Enforcement, Industry & Consulting** backgrounds

EUROPOL

700+ experts across 19 countries

100+ certifications

CISM CREST ISO 27001

Expertise in **AI, IAM, Cloud, Data Analytics, OT Security** and **Cyber Risk**

700k+ actively monitored endpoints

Rated as an **industry leader**

FORRESTER 2024 Computing Security Awards WINNER

computing Security Excellence Awards 2023 WINNER

SC 2023 Awards WINNER

AMER Partner Awards 2026

CONTACT US

To learn how Kroll helps organizations operationalize Managed Detection and Response and reduce real-world risk:

Robb Mayeski
Executive Sponsor
Cyber and
Data Resilience

Jim Hardman
Head of Managed
Detection and Response
Cyber and Data
Resilience

Brandon Roberson
Alliance Director
Cyber and
Data Resilience

Contact us via email:
CrowdStrike@kroll.com

Check our website:
kroll.com/crowdstrike

About Kroll

As the leading independent provider of financial and risk advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.