In partnership with

Responder MDR

Managed detection and response fueled by seasoned IR experts and frontline threat intelligence to deliver unrivaled response

Kroll Responder – Managed Detection and Response

No Holds Barred MDR

Kroll Responder managed detection and response (MDR) merges our frontline threat intelligence and incident response experience, proprietary forensic tools, and rich telemetry from endpoints, network, cloud and SaaS providers to deliver enhanced visibility and rapidly shut down cyber threats.

In Tune with Your Organization and the Threat Landscape

Benefit From Frontline Threat Intelligence Before Anyone Else

Responder consumes direct intelligence from the thousands of incident responses we conduct each year. You benefit from this deep insight before anyone else which means we can detect and contain the latest threats before they impact your organization.

Complete Visibility and Control of your Entire Digital Footprint

We bring together the telemetry from your endpoints, network, cloud and SaaS instances and layer that with our detection and containment capabilities to maximize the benefits of your security technology investments, actively reducing the attack surface of your digital footprint.

Unrivaled Response Capabilities to Protect Your Organization

Our response capabilities are like no other; Kroll Responder is backed by the same team entrusted by global insurers to deal with complex breaches. We extend that service to you so that if the worst happens, we'll stop at nothing to contain and remediate the incident, across any device, anywhere and at any time.

Stop cyberattacks with MDR powered by unrivaled response

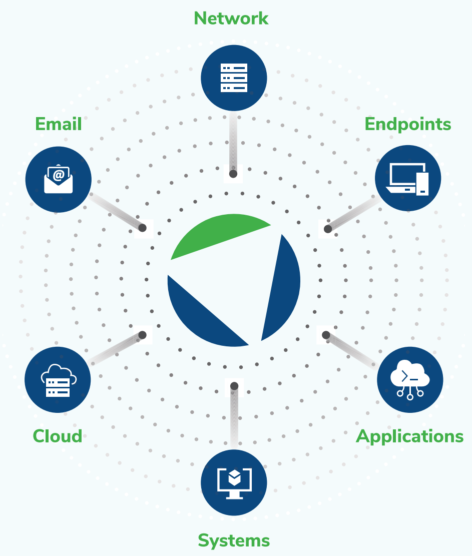
200+
Seasoned Investigators and Threat Hunters

10x
Reduction in Mean Time to Respond

3200+
DFIR Cases Handled Per Year

55+
Leading Endpoint, Network, and Cloud Integrations

Kroll Responder at Work



1

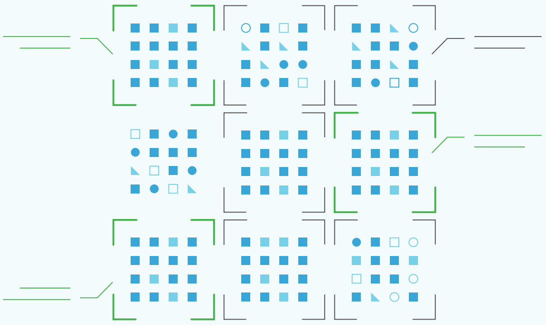
Telemetry & Intelligence

Telemetry is collected from across your networks, endpoints, and cloud environments, analysed using the latest machine learning and behavioural detection engines, then enriched with the latest threat intelligence.

2

Detection & Enrichment

Detections are correlated and then grouped together by common attributes to create 'cases' – providing a more complete overview of security events.



3

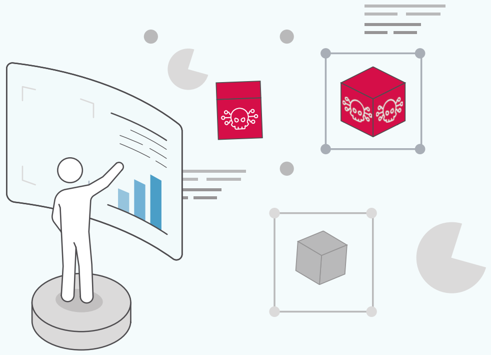
Investigation & Hunting

Cases are triaged by our 24/7 Security Operations experts, using initial findings to hunt deeper before escalating those requiring additional attention to Kroll's elite incident response team.

4

Response & Containment

Automated playbooks and human intelligence provide robust response and remediation capabilities around the clock to disrupt, contain and eradicate threats before they cause costly damages.



Outcome-Driven MDR: Unrivaled Incident Response Expertise Behind Every Alert

Seasoned IR Experts

The same team of Kroll investigators that handles thousands of incident response cases empower Kroll Responder, providing rapid and effective response to threats

Adversary Mindset

Adversary intelligence from hundreds of penetration testing and red team engagements continually improves detection efficacy and hunting, aligned with MITRE ATT&CK

Frontline Intelligence

Real-world cyber threat intelligence from thousands of incident response cases helps Kroll Responder detect even novel attack methods faster and more accurately

Unrivaled Response

World-class incident response experts behind Kroll Responder stop at nothing to contain and remediate the incident, across any device, anywhere and at any time

Limitless Visibility

We can detect even the most elusive adversary by ingesting and enriching telemetry from your networks, endpoints, cloud, SaaS and email platforms

Tech Agnostic Platform

A unified threat management platform enables Kroll Responder to monitor environments, identify and manage security incidents, and deliver the outcomes you need

No-Noise Detections

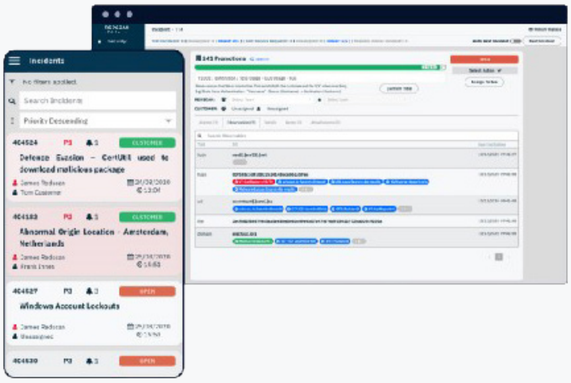
Rapid detection and effective triage is powered by our sophisticated data correlation and enrichment engine, backed by our seasoned investigators

Swift, Precise Playbooks

Threat disruption, isolation, and containment often happens within minutes thanks to automated response playbooks optimized with frontline threat intelligence

Powered by Kroll's Redscan Platform

Kroll Responder is powered by the Redscan platform, able to ingest a variety of sensors capable of monitoring current and legacy versions of Windows, macOS, Linux, as well as network devices and cloud platforms. The Redscan platform helps improve monitoring capabilities to a standard needed to swiftly detect and respond to the cyber threats that target any infrastructure, service or applications.



Incidents

No filters applied

Search Incidents

Priority Descending

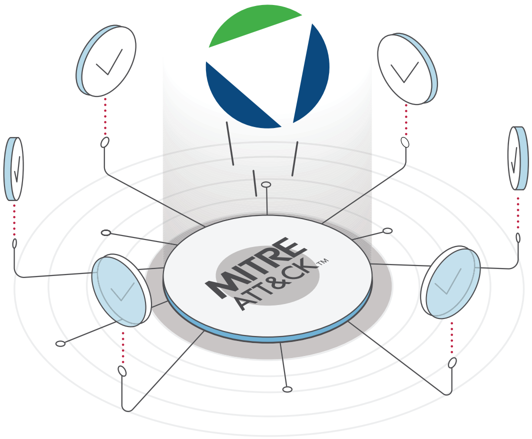
404524 P3 CUSTOMER
Defense Evasion – CertUtil used to download malicious package

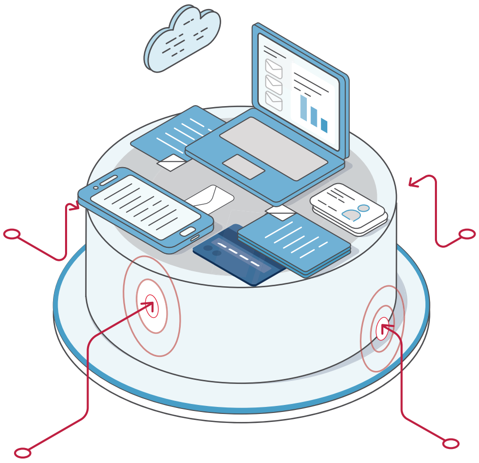
404183 P3 CUSTOMER
Abnormal Origin Location - Amsterdam, Netherlands

404527 P3 OPEN
Windows Account Lockouts

404530 P3 OPEN

Gain a Super-Powered SOC





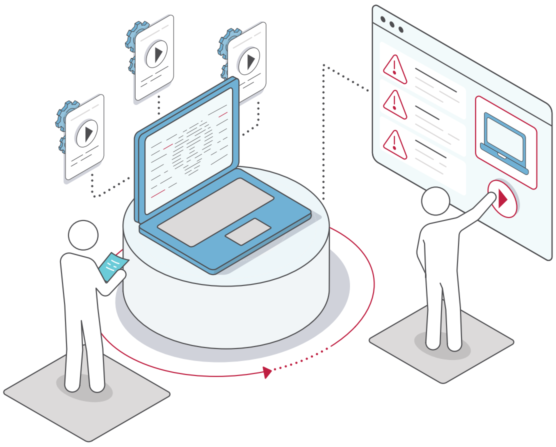
Sophisticated Correlation and Enrichment For No-Noise Detections

Millions of events across your environment are collected, analyzed, and enriched with frontline intelligence from thousands of incident response engagements handled by Kroll every year.

> Get a MITRE ATT&CK observable gap analysis. Talk to one of our experts.

Automated Response Actions Continuously Optimized by Experts

Responder combines the best of human response and threat intelligence with security orchestration, automation and response (SOAR) capabilities to contain and mitigate threats automatically. As both your organization and cyber threats evolve, so do our detections and playbooks, delivering continuous advanced protection.



Unrivaled Response Fueled by Remote Live Forensics

No matter where threats appear in your systems, seasoned incident response investigators behind Kroll Responder are armed with proprietary digital forensics tools like KAPE to dig deeper, at no extra cost. We can:

- Collect additional forensic evidence, including from virtual machines, using proprietary tools
- Enrich findings with extensive intelligence from our cases
- Write custom scripts to purge evil and eliminate persistence
- Reverse engineer suspicious malware
- Validate remediation of threat and “clean” status for impacted systems

Leverage 360-Degree Visibility to See and Stop Cyberattacks. Get a Customized Kroll Responder Demo. Visit kroll.com/responder

KROLL

In partnership with zen

GLOBAL CYBER EXPERTISE

Many of our cyber professionals bring years of unique experience from their former service with large enterprises as well as law enforcement and regulatory agencies:

- Federal Bureau of Investigation (FBI)
- Interpol
- U.S. Department of Justice (DOJ)
- Securities & Exchange Commission (SEC)
- U.K. Intelligence and Policing
- U.S. Department of Homeland Security (DHS)
- U.S. Secret Service (USSS)
- U.S. Attorney's Office

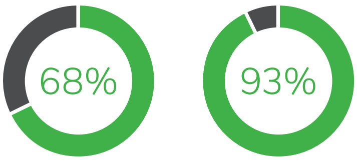
DID YOU KNOW...

Kroll works on ...

3200+

Cyber events per year for clients ranging from Fortune 100 to medium-sized businesses.

Kroll works with over...



of the Fortune 100

of the AM Law 100

Kroll has a dedicated insurance team for insurance and legal channels, with extensive relationships with 60+ cyber insurance carriers and exclusive benefits to insureds.

INDUSTRY RECOGNITION

CREST

CREST has accredited Kroll as a global Penetration Testing provider

PCI Security Standards Council

Kroll is certified as a Global PCI Forensic Investigator (PFI) company

Gartner

Kroll recognized as a Representative Vendor for Digital Forensics and Incident Response (DFIR) and Managed Detection and Response (MDR)

IDC

Kroll named a Global Leader in Incident Response Readiness

TALK TO AN EXPERT TODAY

☎ 01706 902579 ✉ solutionsales@zen.co.uk zen.co.uk/business

About Kroll

As the leading independent provider of risk and financial 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.