ITHQ

Incident Detection & Response (IDR)

RAPID7 BRONZE Partner

ADVANCED DETECTION, FOCUSING IN RAPID DATA AGGREGATION, ANALYTICS AND FORENSICS

80% of hacking-related breaches are due to stolen, weak or guessable passwords. While your users are your greatest asset, they can also pose your greatest risk.

Password management solutions are continuing to improve, but having a platform that centralises and analyses your data is still essential if your business is to maximise resilience against intrusion incidents.

Cyber crime can be extremely sophisticated, with breaches going undetected for months. An active approach to defence that incorporates curated threat intelligence from leading security third-parties and machine learning, is the best protection for your corporate data assets.

ITHQ INCIDENT DETECTION AND RESPONSE (IDR)

We deliver a fully configured and managed IDR solution in partnership with Rapid7's InsightIDR.

Our FIRE process: proven to maximise project results

This powerful platform makes it easy to centralise and analyse your data and allows you to detect incidents within hours.

User and attacker behaviour is analysed and, along with curated threat intelligence, is automatically applied. You are able to investigate and respond to attacks up to 20 times faster, while proving compliance.

Alerts automatically flag important behaviour, along with context around any malicious activity. Compromised users and assets are auto-contained, and you can kill malicious processes or quarantine infected endpoints, to immediately lower your risk.

ITHQ's wraparound service and expertise make your business as protected as possible to ever-changing cyber threats.

Configuration and management of Rapid7's InsightIDR

- **User behaviour baselining and analytics**
  Detects attackers masquerading as employees or business-familiar bad actors
- **Advanced attacker behaviour analytics**
  Curated data from leading global security vendors help spot new threats & detect attacks earlier and more accurately
- **Endpoint detection and visibility**
  Unified real-time detection and user endpoint behaviour insights save you time in threat hunting activities
- **Comprehensive centralised log management**
  All logs stored and managed in one place, smooth search, automated compliance and correlation
- **Visual investigation timeline**
  Log search, user behaviours and endpoint data in a single timeline making investigations up to 20x faster
- **Deception technology**
  Craft honeypots, honey users, honey credentials and honey files, to identify attackers much earlier in the attack chain
- **File integrity monitoring**
  Regulation mandated across PCI, HIPAA and GDPR allowing you to flag changes to specified endpoint files or directories
- **Automation for accelerated response**
  Workflows for threat containment, firewall rule changes, integration with ITSM systems and user account suspension
- **Azure cloud environments**
  Our solution integrates with Azure AD, Azure Monitor, Azure Security Centre, Office365 Exchange and Microsoft DNS
- **AWS cloud environments**
  Our IDR platform also integrates with AWS CloudTrail and AWS GuardDuty, to ensure full cloud visibility

"Best external and internal incident threat response with perfect endpoint visibility and monitoring"

G2 Crowd review: ICT Manager

INSIGHTIDR FROM RAPID7

Unify Your Security Data

Detect Behavior Behind Breaches

Respond With Confidence

RAPID7 BRONZE Partner

Using InsightIDR from Rapid7, our fully configured and managed incident detection and response solution includes advanced and sophisticated tools with proven benefits.

Your data is centralised and intuitively visualised to make analysis simple. SIEM is significantly improved, with curated threat intelligence speeding up detection and response times.

Machine learning baselines user behaviour, automatically alerting you if stolen credentials are used or anomalous lateral movement identified.

You can take containment actions across Active Directory, Access Management, EDR, and firewall tools. Your team is empowered to directly contain threats on an endpoint, network, and user level.

ITHQ fully configures the platform to your business and manages everything for you, to ensure you get maximum protection from IDR as part of your cyber resilience program.

ITHQ IDR SOLUTION FEATURES

Consultation, solution plan and reporting included as standard	All network devices and endpoints logging into IDR authenticated as necessary: DCHP, DNS, IDS, Firewalls, AD etc
IDR, response or automation workshops conducted, in line with solution plan - HLD / LLD	Solution is fully configured and managed by ITHQ
Processes	File integrity & monitoring
Running cases	Deceptions
Investigations	Automations

ITHQ

Talent, technology and technique applied to help your business perform better

Suite 127
Churchill Court 3
Manor Royal
Crawley
RH10 9LU

www.ithq.pro
020 3997 7979
transform@ithq.pro

ENGAGE INSPIRE TRANSFORM