ZDL GROUP

Managed Detection & Response

www.zdlgroup.com

ZDL GROUP

A Proactive Approach to Cyber Security

We live in an era where blind spots in detecting and reacting to early indicators of compromise can be punishing. Without a focus on detecting new and unseen attacks, organisations are left exposed and vulnerable to large scale breaches and the full spectrum of associated potential damage.

The best approach to proactive cyber security requires both technology that can identify potential attacks and skilled cyber security analysts who are armed and ready to investigate and mitigate these threats.

Increased Visibility For Targeted Remediation

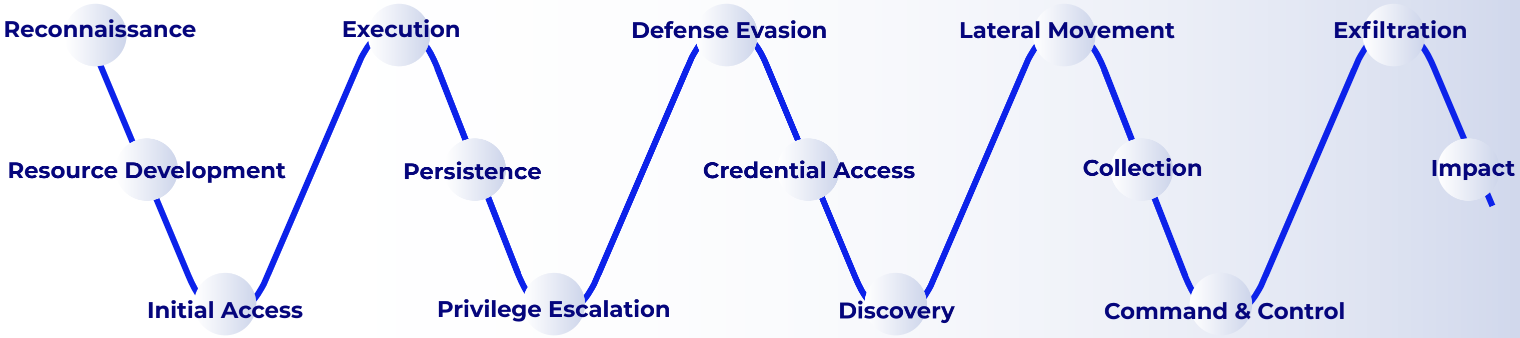
Reduced Mean Time To Respond (MTTR)

Actionable Intelligence For Both Internal And External Threats

Expert Advice To Reduce The Likelihood Of Significant Disruption

Increase Visibility for Targeted Remediation

The ZDL Managed Detection & Response (MDR) Service adopts a ‘Detection-in-Depth’ approach based on the NCSC Good Practice Guide’s 13 controls. Our MDR service pieces together traditional security tools such as firewalls and endpoint AV, merging them into one synergistic solution, providing a single-pane-of-glass view of your estate. Through expanded coverage on the principle of minimum noise maximum signal, we efficiently scale up coverage of the MITRE ATT&CK Framework shown below.



Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact

Reduced Mean Time to Respond (MTTR)

The MDR Service provides proactive alerting and is built around the capability of the expert analysts to take immediate, preventative, and protective measures in the event of a security incident.

- By leveraging the incredibly flexible and versatile Elastic SIEM engine and associated Endgame Endpoint Agent, with a team of expert engineers underpinning the technology, almost any log source can be accommodated.
- In addition to alerting, our analysts work to proactively refine alert criteria based on threat intelligence relevant to your business to continually improve detection coverage across your assets. Minimum noise, maximum signal.
- Our dedicated team will host regular service reviews to refine the service with you and produce curated, handmade monthly reports for feedback to senior stakeholders.

ZDL GROUP

Actionable Intelligence for Both External & Internal threats

- **Deep and Dark Web Monitoring:** Monitors the surface, deep and dark web for instances of usernames & passwords associated with a customer's domains.
- **Threat Intelligence:** Leverages multiple sources to collate information about the threats and threat actors that will help mitigate harmful events.
- **Data Enrichments (e.g GEO-IP):** Leverage trusted external data sources to enrich log data and increase the usability / identifiability (e.g. Geographical enhancement of IP addresses to identify source location).
- **External IP Monitoring:** Get ahead of attackers by identifying the risk areas in your network and taking remedial action to protect against attack before it happens.

Expert Advice to Reduce the Likelihood of Significant Disruption

- **24x7x365 service from the UK based SOC:** Alerting any time; day or night, including weekends and Bank Holidays. Escalation pathways are defined by you during our onboarding process.
- **SIEM:** Collection, indexing, filtering and alerting of suspicious log activity.
- **Security Configuration:** Monitor system and application configurations against security policies.
- **Log Compression at Source:** Reduces the amount of data that needs to be transferred to the SIEM solution.
- **Retroactive Threat Hunting:** Our analysts manually search log data and daily reports, looking for novel or silent signs of intrusion which automated detection logic may miss. This is further augmented with machine learning.
- **Machine Learning / Artificial Intelligence:** Enhance human curiosity with automated elements to accelerate anomaly identification and remediation.

The ZDL Approach

We operate an **ASSET BASED** model allowing organisations to focus on the most important areas of their estate

We recommend a scalable **CRAWL, WALK RUN** approach to allow our clients to grow the coverage provided by our service over time.

We work closely with our clients to understand their needs and never **OVER SELL** the services. If it doesn't need to be covered at this point, then that's fine.

We can provide **RAPID** onboarding meaning your **Return on Investment** is realised much quicker

We provide you with only **HIGH-FIDELITY SECURITY** Alerting to ensure that you are never flooded with false-positives

ZDL
GROUP

Delivering Excellence in Cyber Security

At ZDL, we believe that effective risk management requires a holistic 360° approach. We take a comprehensive view of our clients' cyber security risks andprovide quality services to address those risks.

Our approach to Total Security Management helps make our clients' infrastructure, applications and data more secure in the face of a continually evolving Threat Landscape. Our aim is to build a partnership with our clients, built on a mutual respect and understanding of each other's businesses. We become a part of our clients' team, a valued partner; an intrinsic part of their business.

ZDL's 4 key service areas are designed to focus on our clients' cyber resilience journey. Our unique portfolio of services enables you to build an agile, responsive security infrastructure and strategy.

Our Services

Ethical Hacking

- Broad Security Review
- Red Teaming
- Security Audits
- Penetration Testing
- Cloud Security & Security Ops Testing
- Source Code Review/Coding Standards
- Social Engineering
- Physical Security

Training

- Security Awareness Programmes
- Secure Coding School for Developers
- Bespoke Senior Exec Security Training
- Runbook training/ Scenario Workshops
- Phishing & Resilience Programmes
- Physical Security Awareness
- Online Assessment / CBT Developer Training

Managed Services

- Supplier Evaluation Risk Management (VenDoor)
- Incident Response Preparedness
- Security Training for Developers - Annual Programme
- Managed Detection and Response (MDR)
- Virtual Information Security Manager
- OSINT/Threat Intelligence

Compliance

- Policy Review & Creation
- 360° Assessment
- PCI Remediation Support
- ISO/ NIST/EU GDPR Standards Agreement
- Business Continuity Management
- IR Management Review
- ISO Readiness Programmes
- Office365 Configuration Review

CONTACT US →

www.zdlgroup.com

London | Brighton | Manchester | USA