Deception – A Cyber-Defence Strategy For The Next Normal

Taking an ‘Active Defence’ approach to tackling adversaries in real-time with lean security teams
The Anatomy Of An Attack
The Anatomy Of An Attack
The Anatomy Of An Attack
03

Reasons Organisations Get Hacked
01. Low Visibility
02. Constantly Changing Attack Tactics
03. Too Many False Positives

Monitoring team faces
- Event fatigue
- Data paralysis
- Missed alerts
**The Attacker’s View of a Work From Home World**

- **25%** Increase in perimeter threats
- **50%** Attacks target VPN and webmail systems
- **62%** Attacks originated from cloud providers
- **50%** Attacks only are from known-bad sources
Why Deception?

- Lean and overworked security teams
- Limited budgets, high risk-perception
- Too many complex solutions
Detect With Confidence

**FULL KILL-CHAIN COVERAGE**

**PRIVILEGE ESCALATION #1**
- Credential Decoys
- Application Lures

**PRIVILEGE ESCALATION #2**
- Active Directory Decoys

**RECONNAISSANCE**
- Private Threat Intel Decoys

**EXPLOITATION**
- Phone Decoys
- Spear Phishing Decoys

**LATERAL MOVEMENT**
- Network Decoys
- Hi-interaction application decoys
- MITM Decoys
- Cloud Decoys

**DATA THEFT**
- File Decoys