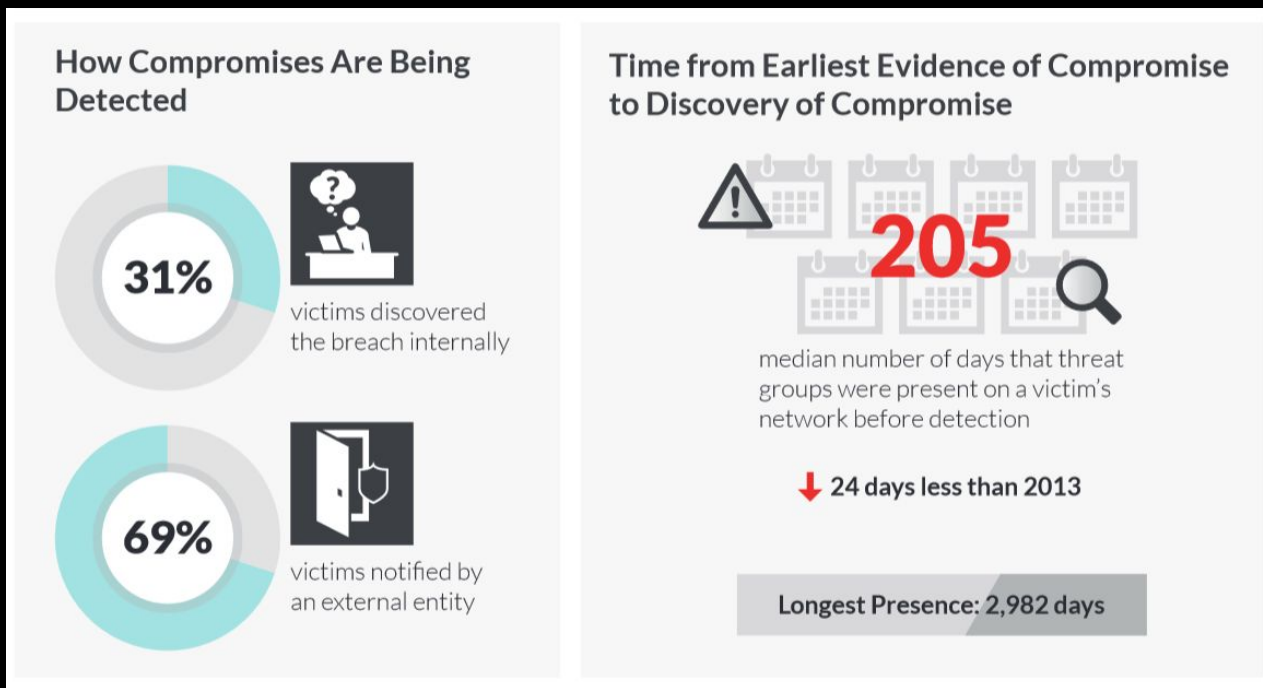# Detection Testing

Because penetration testing dosn't stop the bad guys

The average company dosn't even know when it's been breached!!

How Compromises Are Being Detected

31% victims discovered the breach internally

69% victims notified by an external entity

Time from Earliest Evidence of Compromise to Discovery of Compromise

205 median number of days that threat groups were present on a victim's network before detection

↓ 24 days less than 2013

Longest Presence: 2,982 days

According to Mandiant's 2014 M-Trends report, the average company doesn't know it's been breached for more than 205 days! With 'Detection Testing', guidance, training, and metrics drive those numbers down!!

To quote Sun Tzu.....

Mature IR Team

Developing IR Team

New or bad IR Team

- "If you know the enemy and know yourself, you need not fear the result of a hundred battles.

- If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

- If you know neither the enemy nor yourself, you will succumb in every battle."

Simulated cyber kill chains give your incident responders real practice

Reconnaissance	• Harvesting Email Addresses, Social Networking, Passive Search, IPs, Port Scans
Weaponization	• Developing Exploit with Payload Creation, Malware, Delivery system, Decoys
Delivery	• Spear Phishing, Infected Website, Service Provider, USB
Exploitation	• Activation, Execute Code, Establish Foothold, 3rd Party Exploitation
Installation	• Trojan or Backdoor, Escalate Privileges, Root Kit, Establish Persistence
Command & Control	• Command Channel, Lateral Movement, Internal Recon, Maintain Persistence
Actions on Target	• Expand Compromise, Consolidate Persistence, Identify Targets, Data Ex-filtration

We can help novice to advanced SOCs consistently decrease the time to contain a wide array of threat models