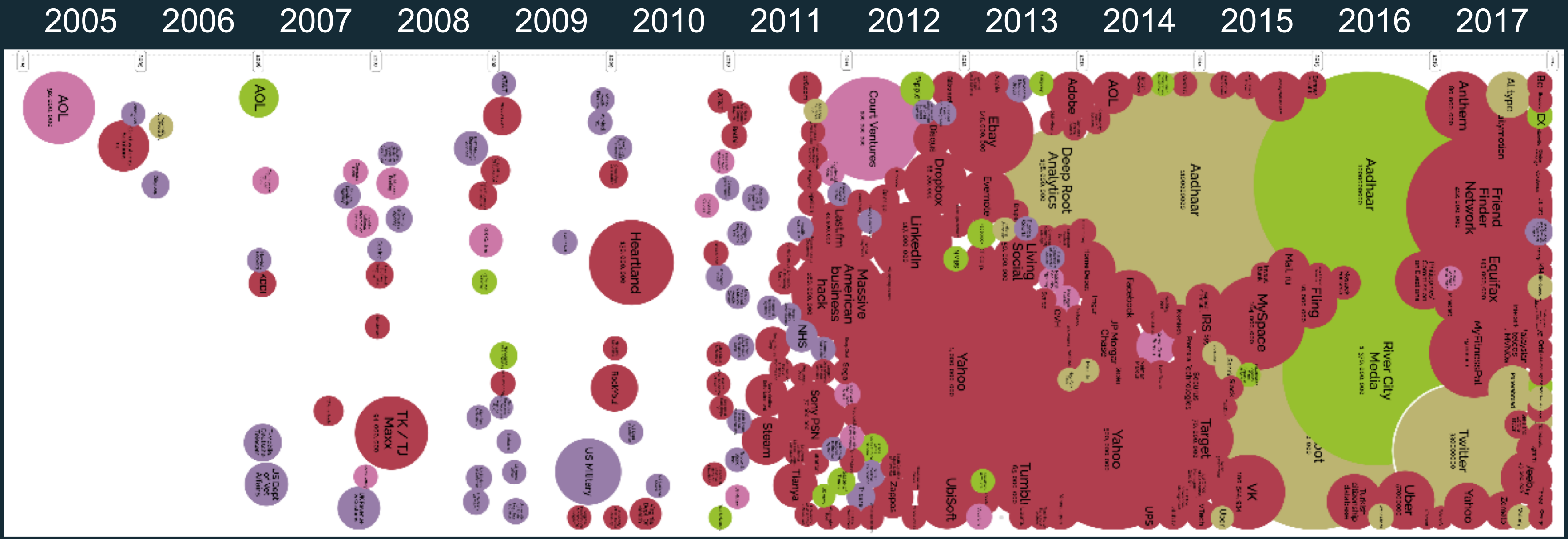
SafeBreach

Build Smarter Defenses

Simulate the Adversary

The Odds are Against Us



And Defenders Keep Investing

PROXY / URL FILTER / ANTIMALWARE

FIREWALL

NGFW

IDS

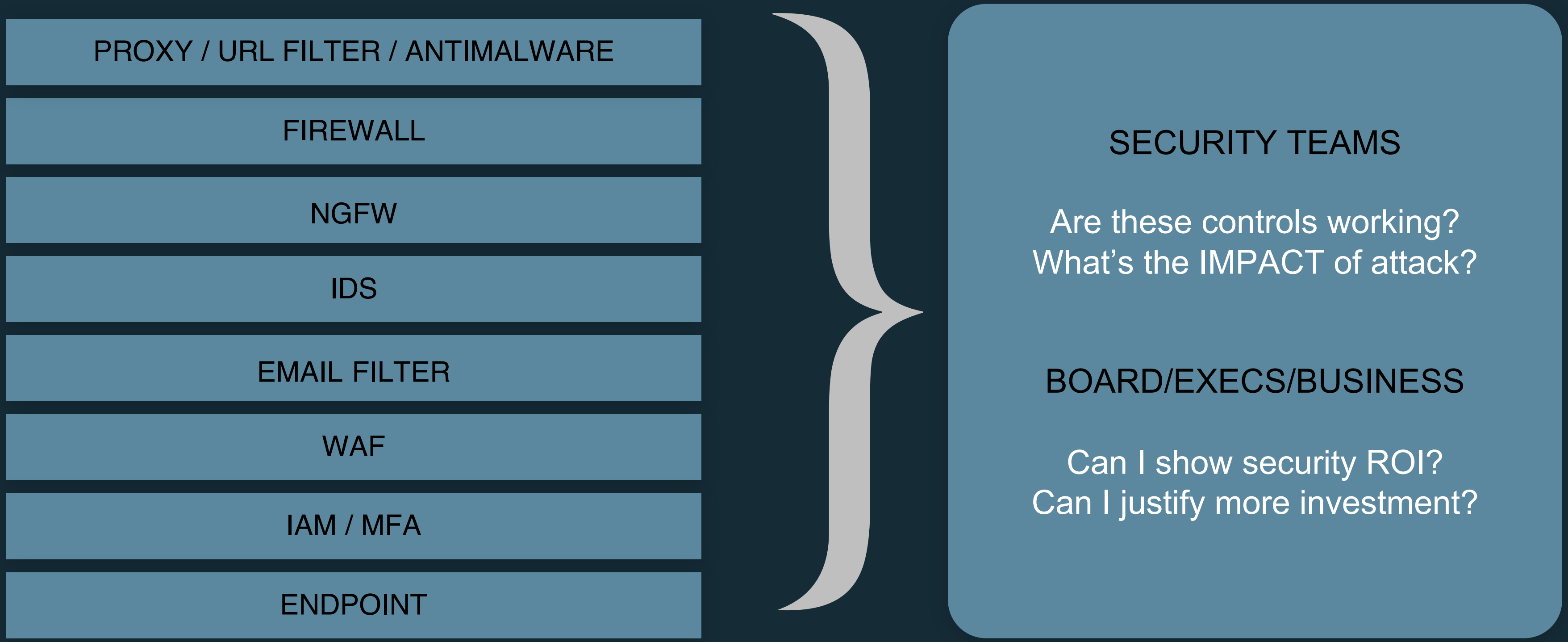
EMAIL FILTER

WAF

IAM / MFA

ENDPOINT

But Still Cannot Answer Critical Questions



PROXY / URL FILTER / ANTIMALWARE

FIREWALL

NGFW

IDS

EMAIL FILTER

WAF

IAM / MFA

ENDPOINT

SECURITY TEAMS

Are these controls working?
What's the IMPACT of attack?

BOARD/EXECS/BUSINESS

Can I show security ROI?
Can I justify more investment?

What Got us Here, Won’t Take us There

1. Build defenses
2. Scan and patch quarterly
3. Run pen tests annually
4. Buy more tools
5. Get breached
6. Get publicized
7. *Hire investigator to *identify where attacks were successful*

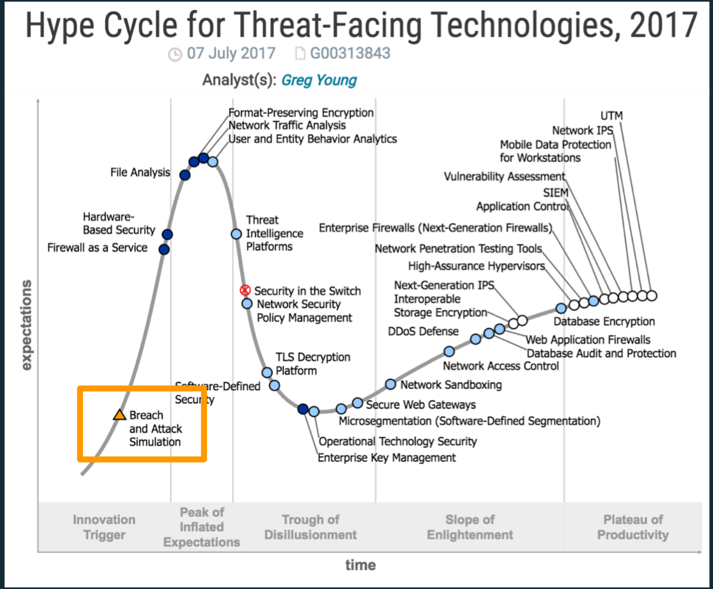
It’s Time to Turn Security Upside Down

1. Unleash thousands of attacks, safely
2. *Identify where attacks are successful*
3. Prioritize blue team efforts based on risk
4. Remediate critical issues
5. Continuously ensure no new gaps
6. Stay ahead of emerging campaigns
7. Fix what *will* happen, before it’s too late

A New Category: Breach and Attack Simulation

"...Shifting to a more proactive risk prevention model can offer valuable data that security and risk managers can use to reduce their risk profiles."

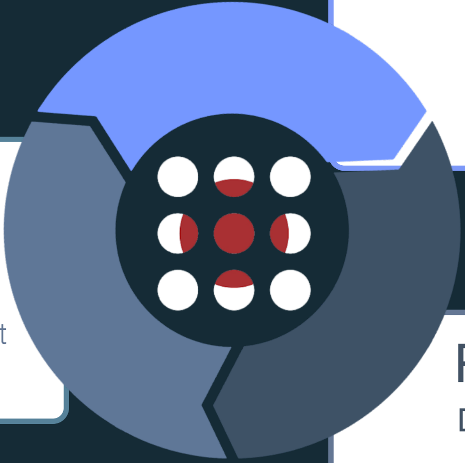
- Gartner



Source: Cool Vendors in Monitoring and Management of Threats to Applications and Data, 2017
Published: 08 June 2017 ID: G00326801

Source: Hype Cycle for Threat-Facing Technologies, 2017
Published: 07 July 2017 ID: G00313843

Simulation: Automated, Comprehensive, Continuous



Simulate Attacks

Eliminate bias with full automation

- Industry’s largest set of attacks
- Uncover security blind spots
- Proven, emerging, never-before seen

Prioritize Results

Drive results with no false positives

- Visualized kill chain
- Simple filters based on critical asset risk
- SIEM and Business Intelligence integration

Remediate Issues

Get more from security investment

- Send to automation and orchestration
- Ensure fixes have no negative security effect
- Maximize outage windows and ops time

100% Real Techniques – All Safe for Production

Relentless attacks, across the entire kill chain, without risk

Infiltration

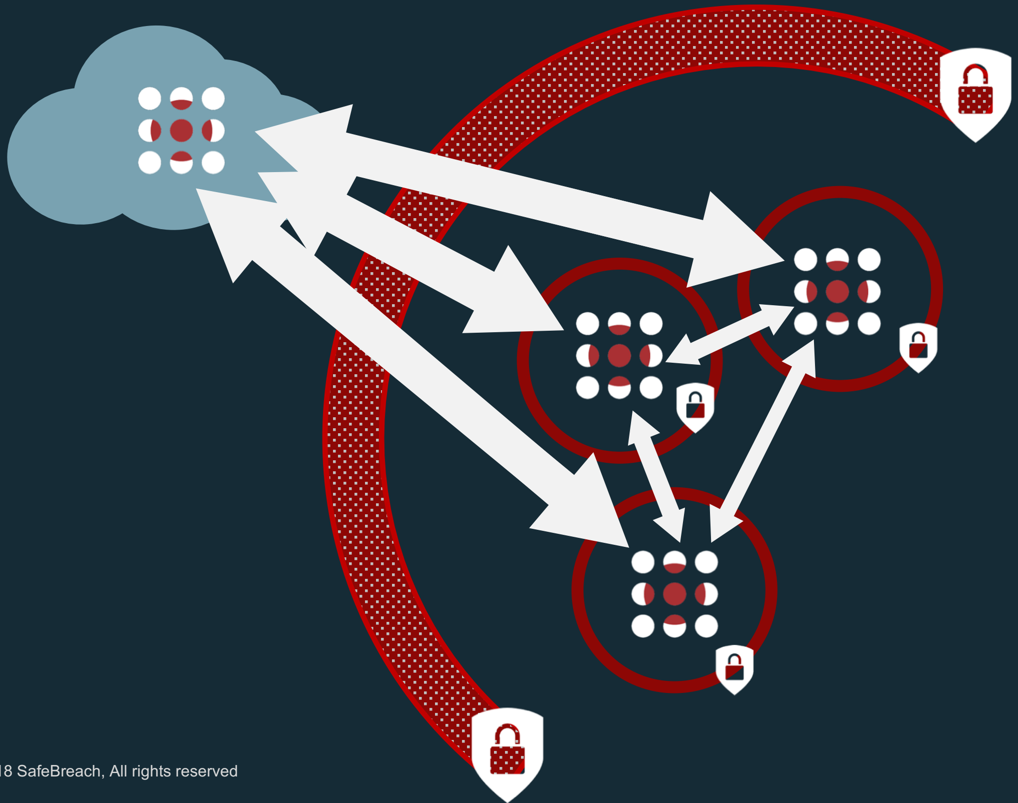
Simulated phishing
Malware download
Drop to disk

Lateral Moves

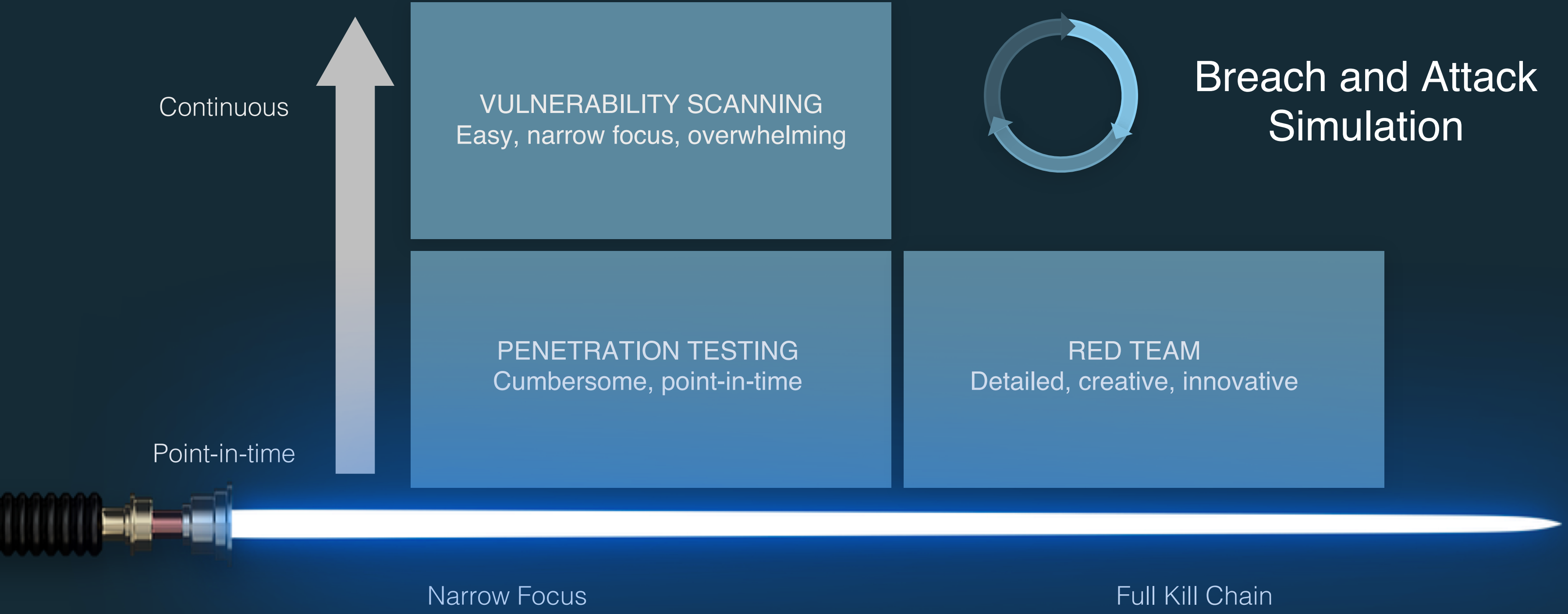
Brute force credentials
Remote code execution
Transfer over SMB

Exfiltration

Header stuffing
DNS tunneling
Malicious ICMP



How is BAS Different from… Everything else?



Continuous

Point-in-time

VULNERABILITY SCANNING
Easy, narrow focus, overwhelming

PENETRATION TESTING
Cumbersome, point-in-time

RED TEAM
Detailed, creative, innovative

Breach and Attack Simulation

Narrow Focus

Full Kill Chain

The Benefits of Playing the Hacker

Minimize security exposure

Get more from existing security

Prepare for audits

Test alerting and action plans

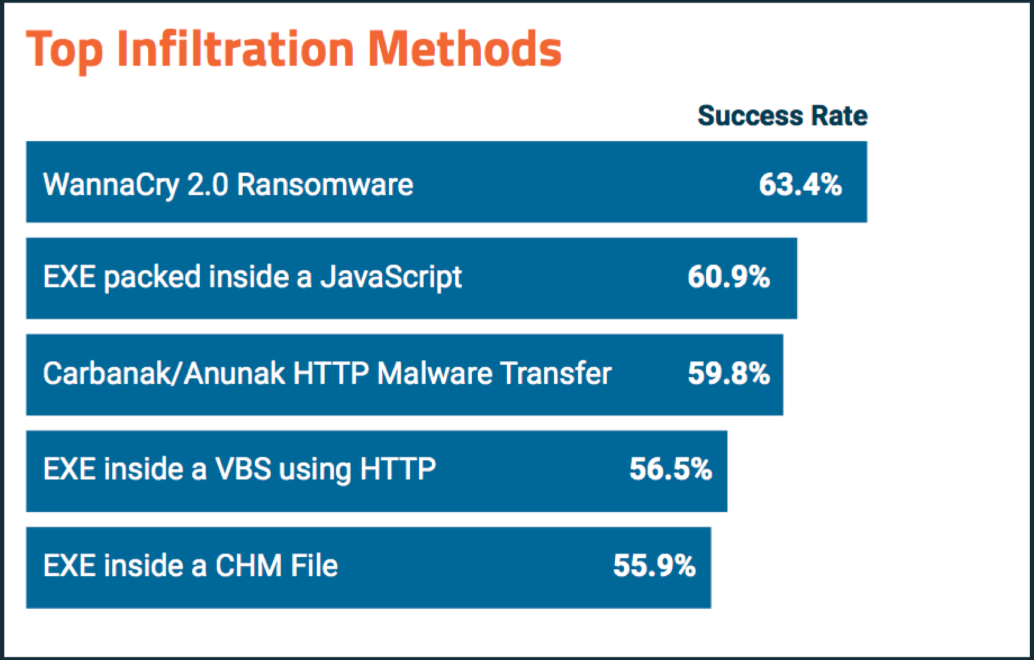
Rationalize security investment

Mergers and acquisitions

Validate your defenses before the attackers do

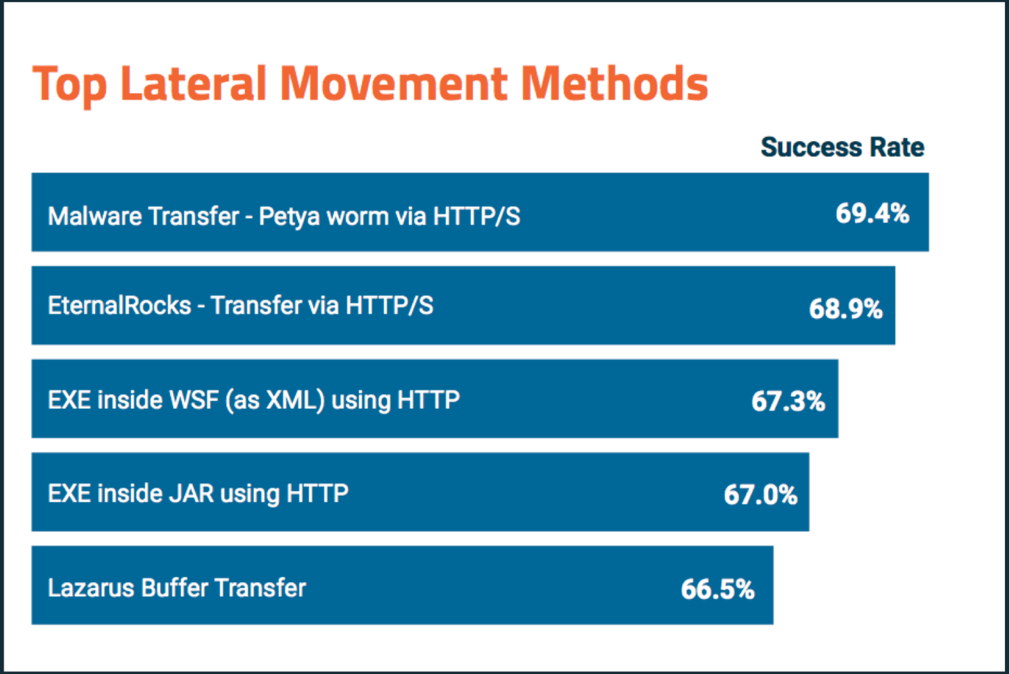
Simulating the Adversary: Results

- Malware manages to evade perimeter defenses
- Encrypted files not scanned
- Leaving it up to the endpoint



Simulating the Adversary: Results

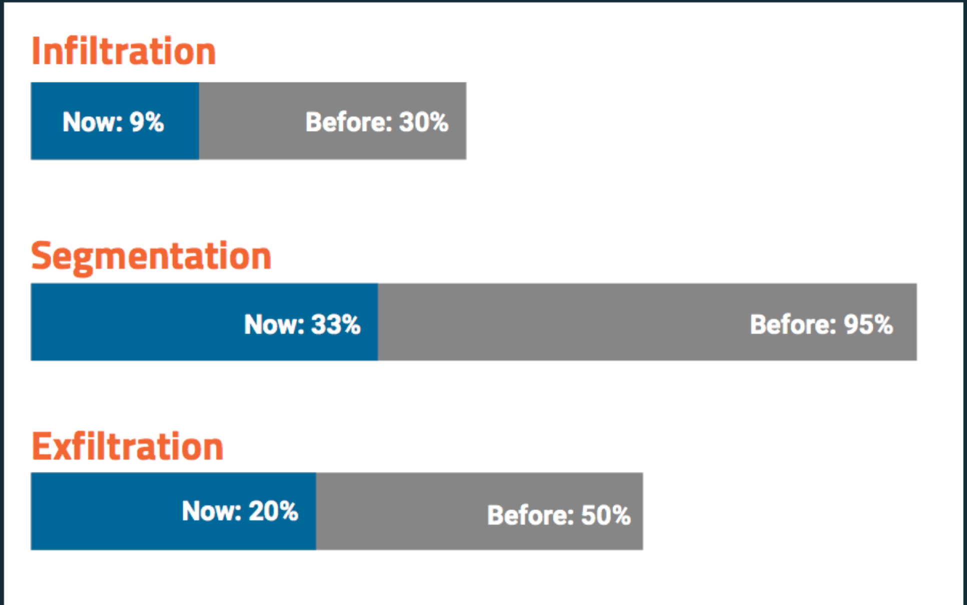
- Lateral moves looked like infiltration
- LAN trust is too high
- Is internal traffic safer than Internet traffic?



Top Lateral Movement Methods

Simulating the Adversary: Remediation

- Dramatically increased security in three weeks
- No new investment
- Conflicting rules, misconfiguration, underutilization



SIMULATE ATTACKS
VALIDATE CONTROLS
HARNESS THE HACKER

SafeBreach