SafeBreach

Heroes and Villains

Simulating the Adversary

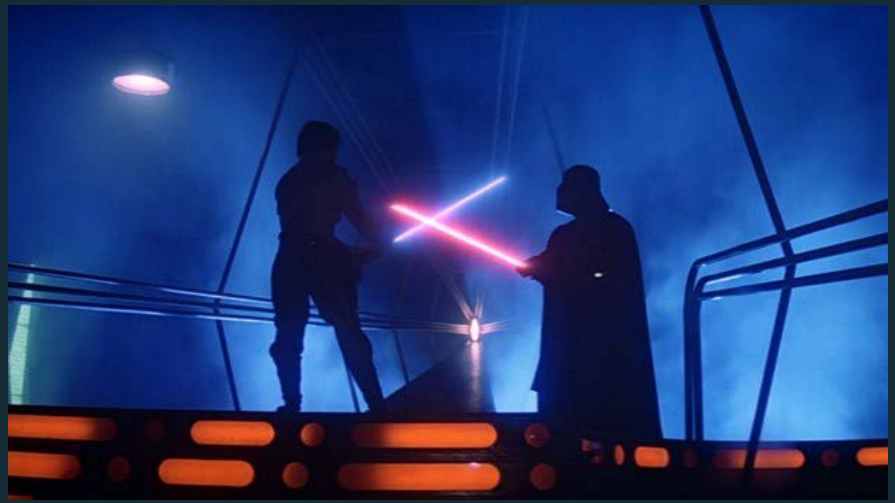
The dark side, and the light…

Security spend is at an all time high

Security controls are at an all time high

“Interest” from BoD is at an all time high

Complexity is at an all time high



I have tons of controls.
I have a smart team.
So… How secure am I?

Every CISO ever

SafeBreach

Best Intentions, But What Results?

- PROXY / URL FILTER / ANTIMALWARE
- FIREWALL
- NGFW
- IDS
- EMAIL FILTER
- WAF
- IAM / MFA
- ENDPOINT

SECURITY TEAMS

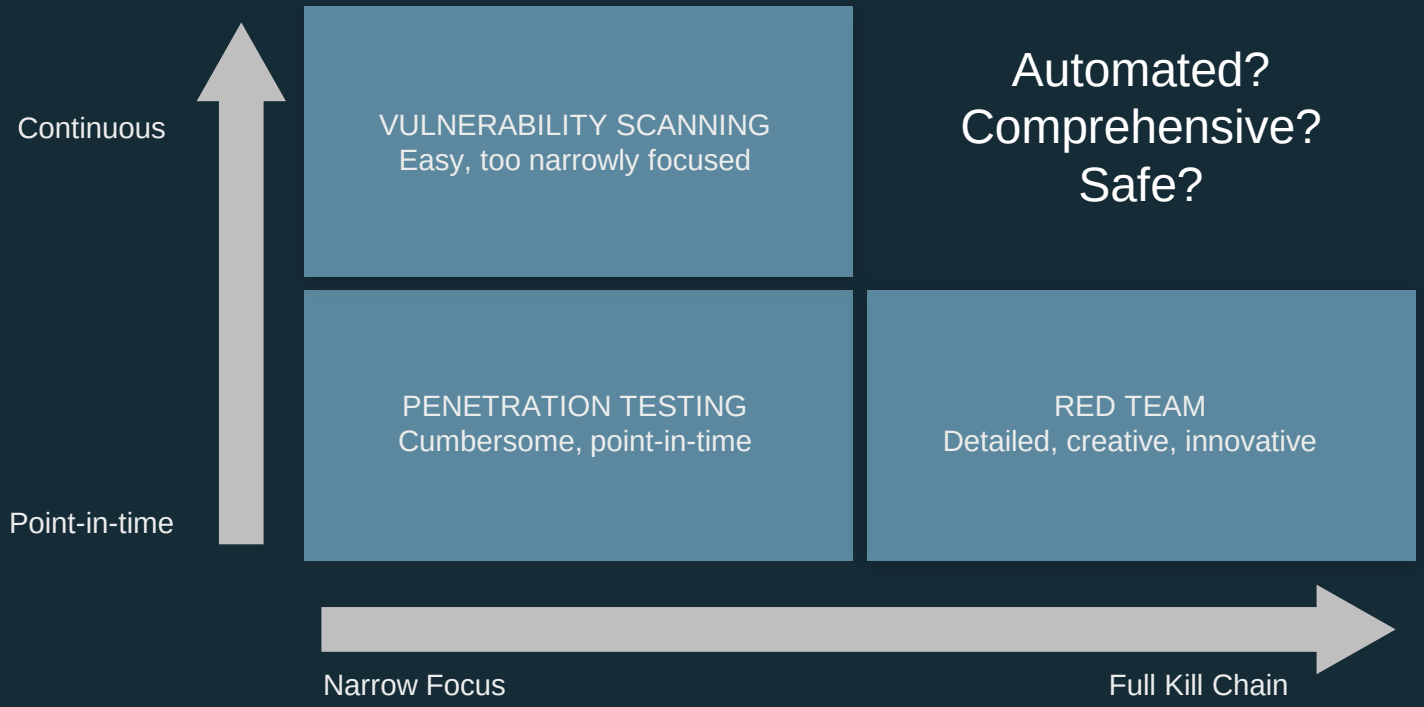
Are these controls working?
What's the IMPACT of attack?

BOARD/EXECS/BUSINESS

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

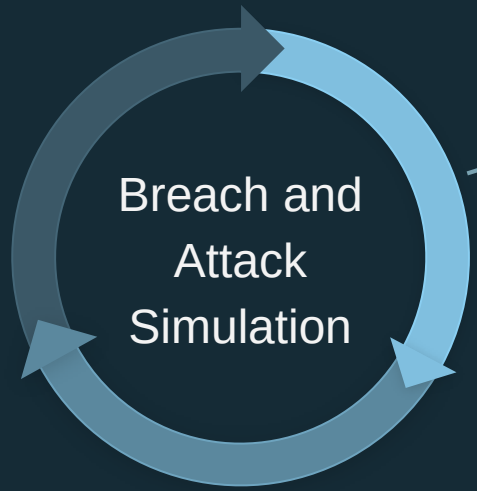
SafeBreach

Legacy Testing Methods



SafeBreach

Breach and Attack Simulation



Remediate

- Initiate automation for immediate fixes
- Send to orchestration/ticketing for ops follow-up

Simulate Attacks

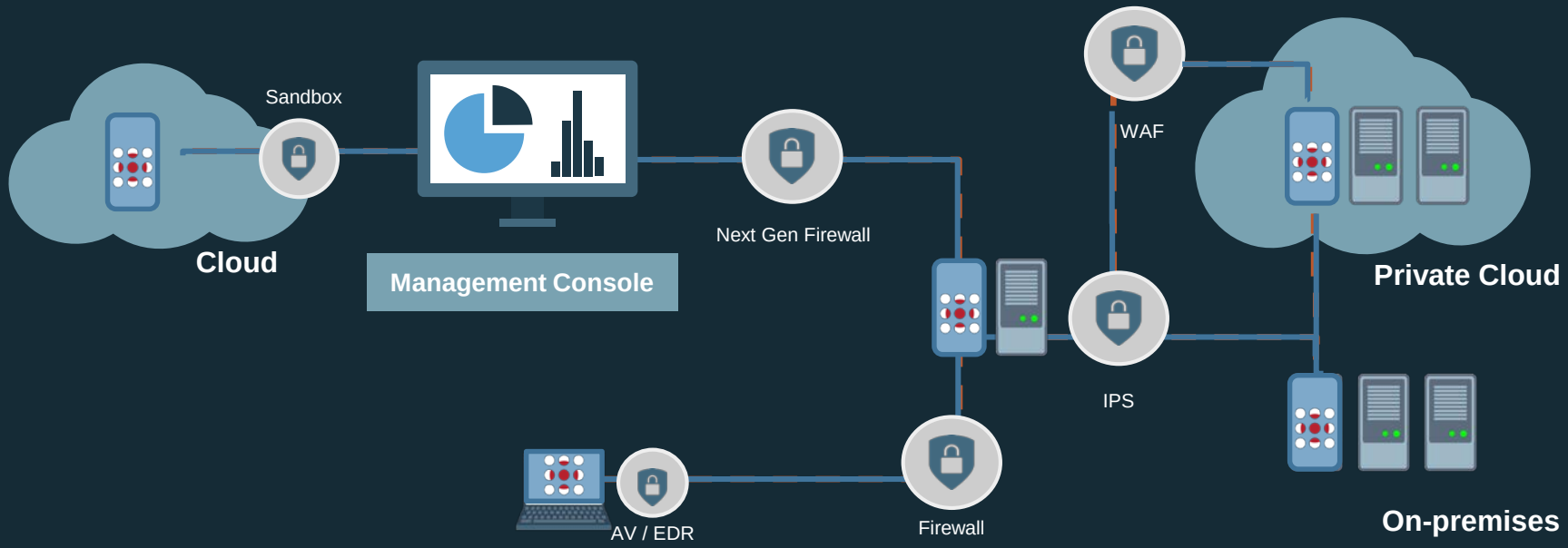
- Cloud, network, endpoint
- Infiltration, lateral movement, exfiltration

Prioritize Results

- Identify and visualize where attacks are successful
- Filter and target critical issues for actionable results

SafeBreach

Breach and Attack Simulation Deployment



SafeBreach

Simulating the Adversary

Continuously validate security with thousands of attacks — safely

Infiltration	Simulated malware drops Executable files Registry entries
Lateral Moves	Brute force Remote code execution Pass-the-hash
Exfiltration	Sample data Direct methods Covert methods

Blocked Methods
Successful Methods
Data Exfiltration Pathways
Recommended Actions

SafeBreach

Breach and Attack Simulation

Validate your controls—with the same techniques attackers use

- **Get more from existing security** by optimizing config and ensuring controls work in concert
- **Minimize security exposure** due to human error, updates, and policy changes
- **Prepare for audits** by validating segmentation and other compliance controls
- **Test alerting and action plans** for SOC or MSSP teams, and provide breach scenario training
- **Get business rationalization for security investment**, prove security against headline attacks

Validate your defenses before the attackers do

SafeBreach

Simulating the Adversary

Do, or do not. There is no try.

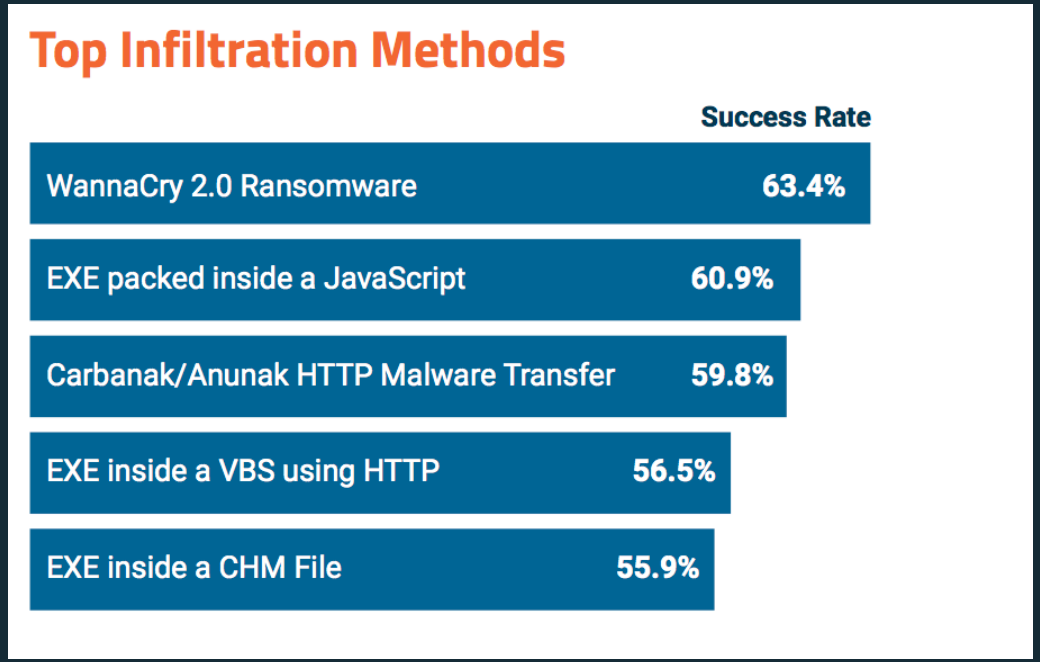
3,400 breach methods executed

11.5 Million simulations

Across verticals and deployment sizes

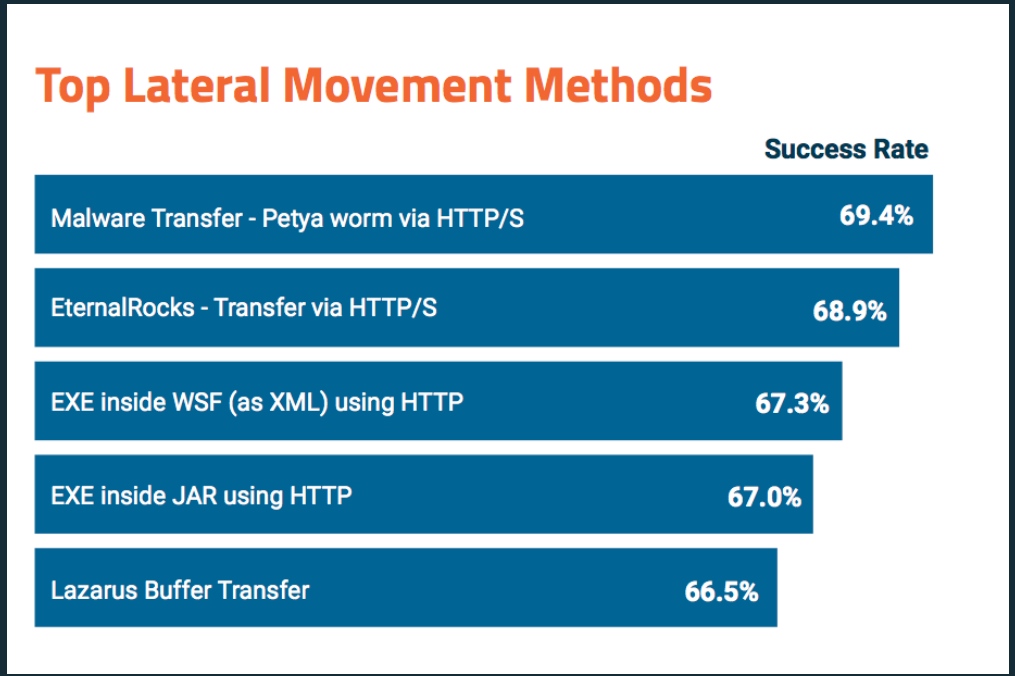
Simulating the Adversary: Results

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



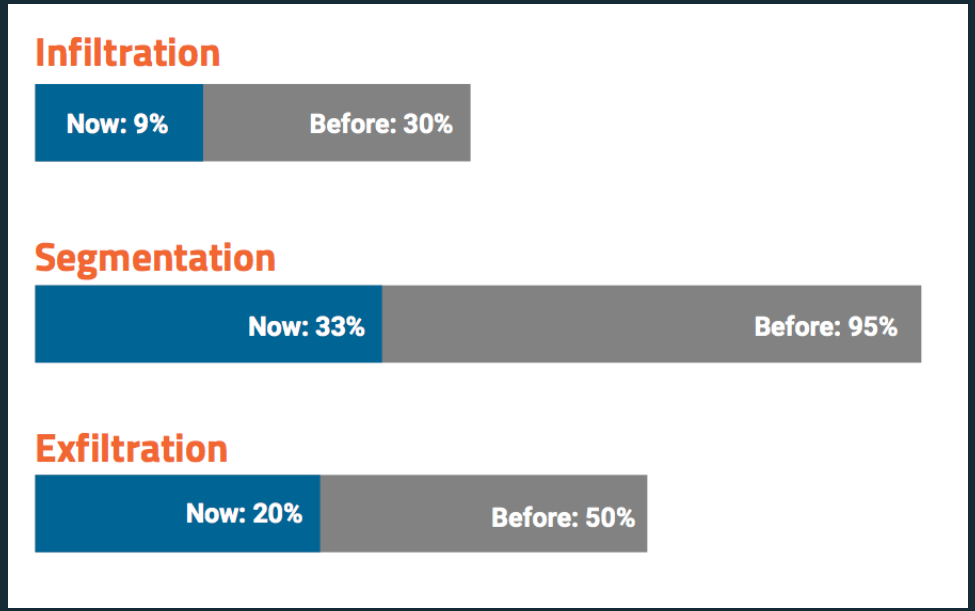
Simulating the Adversary: Results

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



Simulating the Adversary: Remediation

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



SafeBreach

Top Considerations: Breach and Attack Simulation

Safe for production deployment

Continuous validation – not point in time

Actionable, prioritized findings

Complete kill chain, modular, “black box”

Safe | Continuous | Actionable | Thorough

SIMULATE ATTACKS
VALIDATE CONTROLS
HARNESS THE HACKER