Operationalize the MITRE ATT&CK Framework with Breach Attack Simulation (BAS)
Steve Roesing
President, CEO
ASMGi

Mansoor Raza
Senior Solutions Engineer
SafeBreach
AGENDA

- Introductions
- What is the Reality of Enterprise Security?
- What is Breach Attack Simulation (BAS)?
- How do Enterprises Best Leverage Breach Attack Simulation?
- What is the Architecture of SafeBreach?
- Demo
- Q&A
What are you seeing in the marketplace as it relates to attacks?
97% of breaches are at companies which have already deployed the right controls

99% of attacks are known and have been for years

95% of firewall breaches are due to misconfiguration
What is Breach Attack Simulation?
Simulate attacks

**Safely and continuously** run thousands of known threat indicators and attack behaviors to validate and improve your security controls.

- Content: 18,000+ Methods
- Tactics, Techniques and Procedures
- Malware Types
- Custom Build Attacks
- Threat Groups
How do Enterprises best leverage Breach Attack Simulation?
Mitigate
- Remediate issues
- Track your progress
- Report back and make the case

Simulate Attacks
- Cloud, network, endpoint, email
- Infiltration, lateral movement, host level, exfiltration
- Any US-CERT, any emerging threat with 48 hours SLA

Prioritize Results
- Associate with overall risk
- Visualize attack path
- Filter and target critical issues for actionable results

Continuous Security Validation
What is the Architecture of SafeBreach?
SafeBreach Deployment Options

SaaS
Fully managed and continuously updated
Based on AWS infrastructure

Virtual Appliance
Supports VMware ESX 5.x, 6.x, XenServer 6.5 SP1
Managed by customer, connected or disconnected

Software Agent
Supports all major Windows, Mac and Linux OS
Supports network and host level simulations

Virtual Appliance
Supports VMware ESX 5.x, 6.x, XenServer 6.5 SP1,
Amazon EC2 AMI (64-bit)
Supports network simulations

Management Console

Simulators
SafeBreach Deployment

Management Console - Hosted by SafeBreach

On All Platforms

- Public Cloud Environment
  - AWS
  - GCP
  - Azure

- On-Premises Environment
  - Palo Alto FW
  - Carbon Black
  - Firewall

- Private Cloud
  - Fortinet FW
  - Blue Coat IPS

Unique Playbook

External Attacker (SB Simulator)
Automated & Continuous

**Breach & Attack Simulation**

- Continuous validation of security posture
- Making data-driven decisions
- Shortening the exposure time and reducing the attack surface
Steve Roesing
President, CEO
ASMGi

Mansoor Raza
Senior Solutions Engineer
SafeBreach

Q & A