Innovation for the future of security

Wolfgang Meert
CrowdStrike

Innovation for the future of security

SCATTERED SPIDER: Tradecraft evolution

Wolfgang Meert
SALES ENGINEERING

Sensitivity: Confidential

We stop breaches

Sensitivity: Confidential

Sensitivity: Confidential

ADVERSARIES ARE ADAPTING FASTER THAN EVER

15+

New Incident Response Investigations Weekly

New Techniques Developed by Scattered Spider Monthly

CROWDSTRIKE

SCATTERED SPIDER: TRADECRAFT EVOLUTION

- Who are SCATTERED SPIDER?
- Initial compromise
- Identity exploitation
- Living in the cloud
- How to prevent the breach

SCATTERED SPIDER

- SCATTERED SPIDER is an eCrime adversary who conducts targeted social-engineering campaigns.

- This adversary focuses on firms specialising in:
  - Customer relationship management ;
  - Business-process; outsourcing
  - Telecommunications;
  - Technology companies.

- SCATTERED SPIDER has adopted extortion and Big Game Hunting (BGH) campaigns for operational monetization.

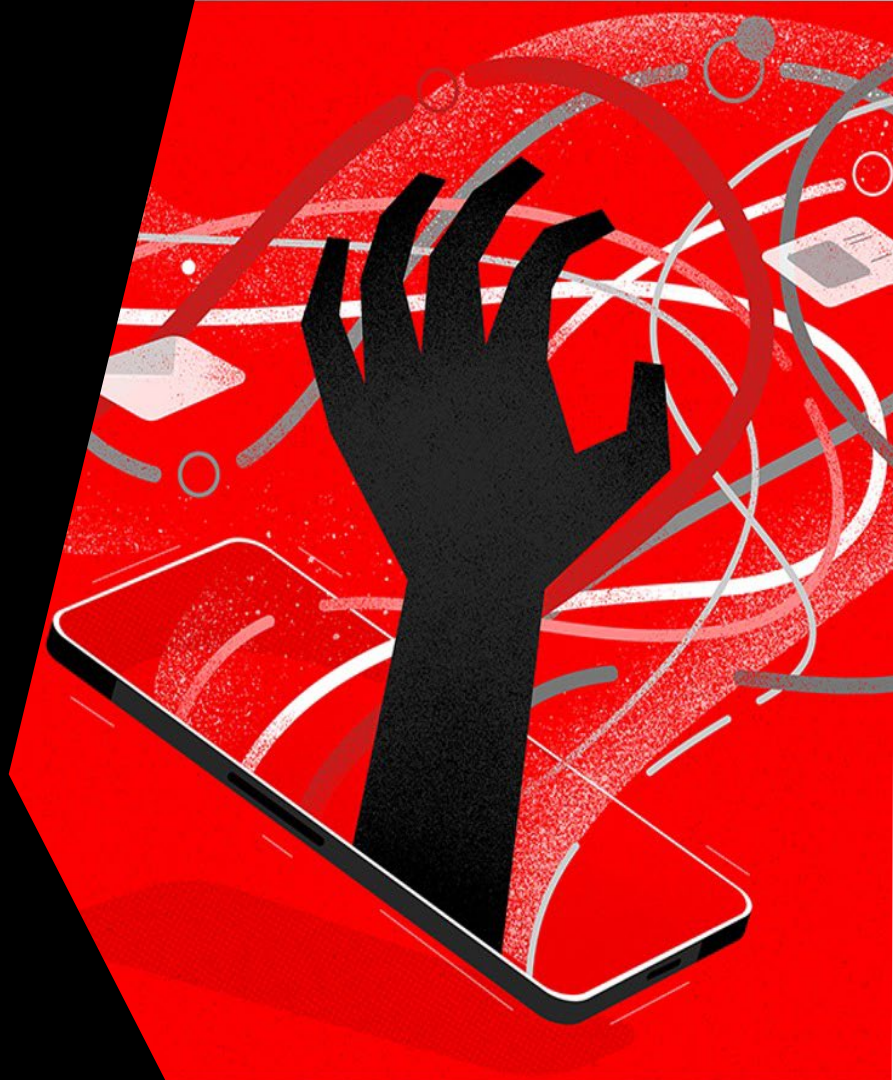
©2023 CrowdStrike, Inc. All rights reserved.

CROWDSTRIKE

INITIAL COMPROMISE

SCATTERED SPIDER combines phishing, smishing, and vishing to compromise targeted companies.

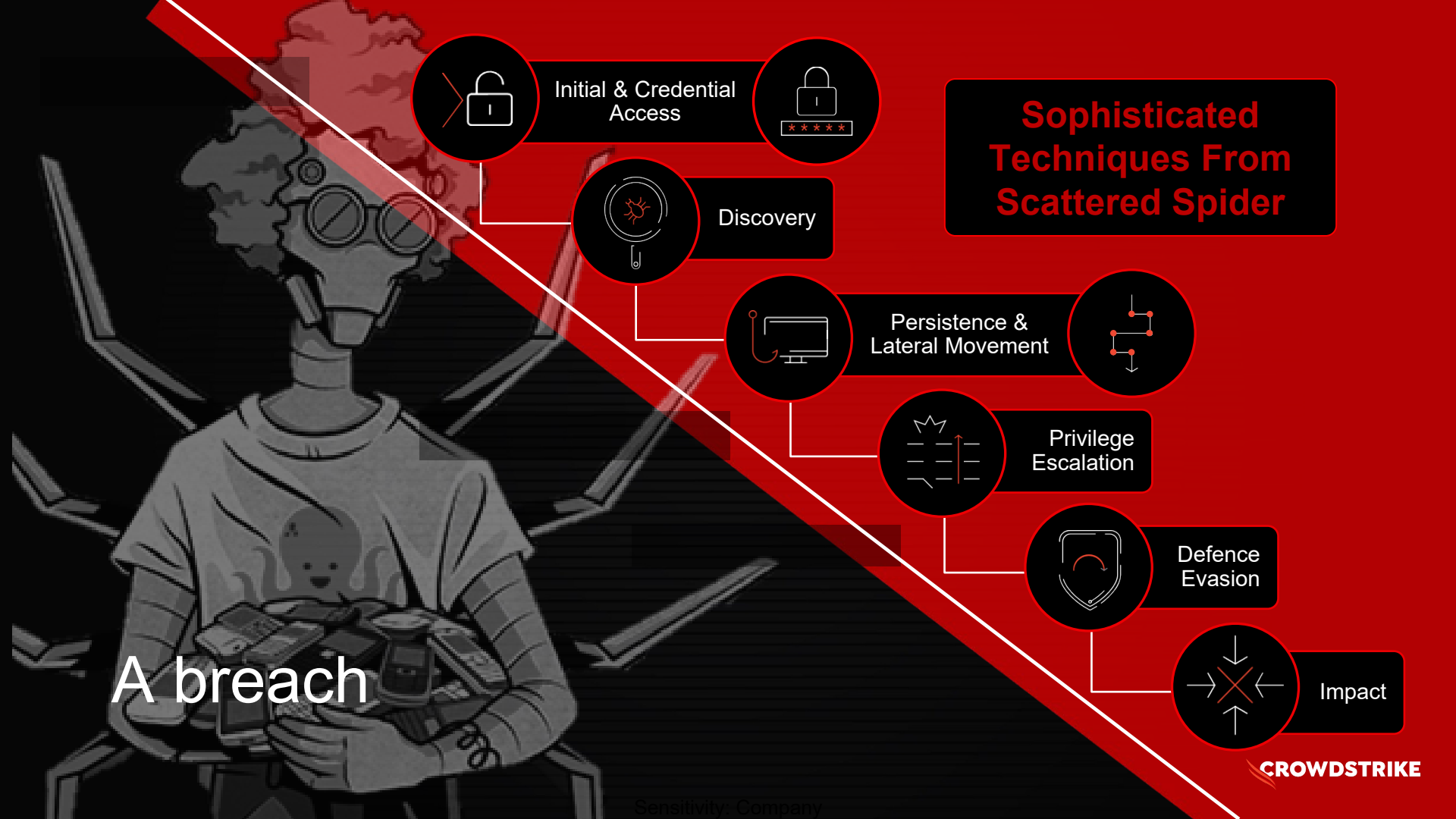
- Campaigns often started with phone calls or SMS messages
- Contact under the guise of an IT or help desk.
- Socially engineers users to share one-time password multifactor authentication (MFA) codes
- Phishing pages to capture authentication tokens
- Overwhelms using MFA notification fatigue



CROWDSTRIKE

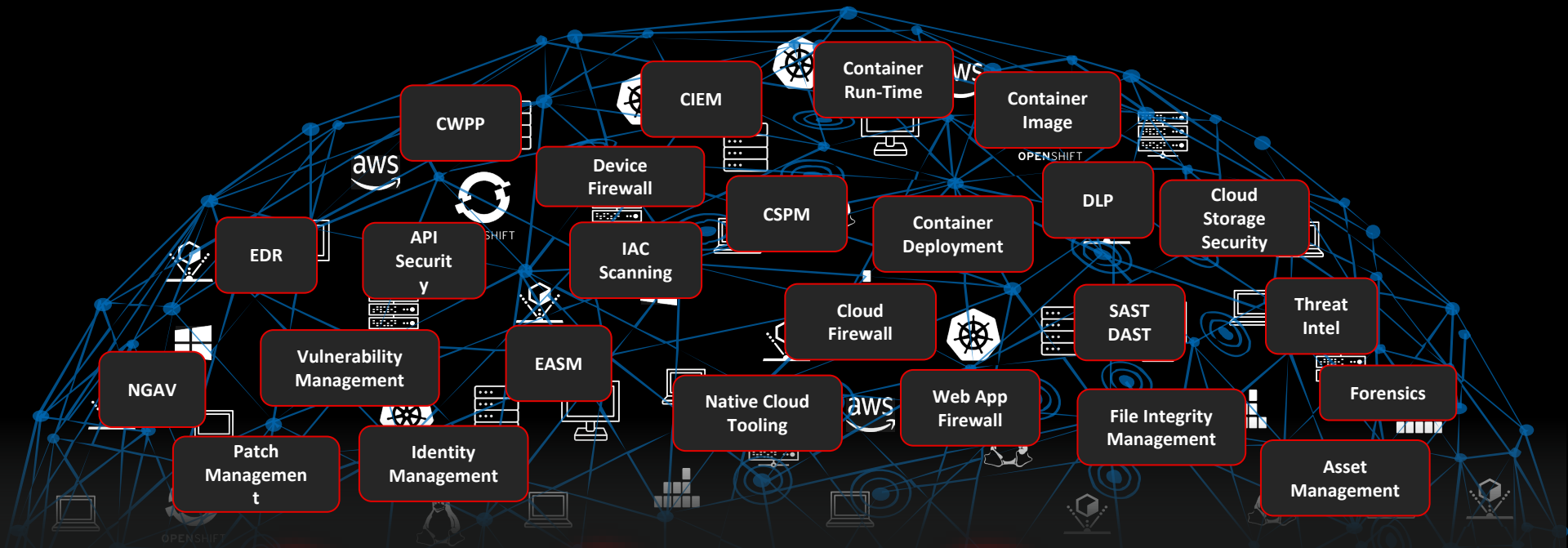
A breach

2023 CrowdStrike, Inc. All rights reserved.



Sensitivity: Company

ADVERSARIES LIVE IN THE GAPS BETWEEN TRADITIONAL POINT PRODUCTS



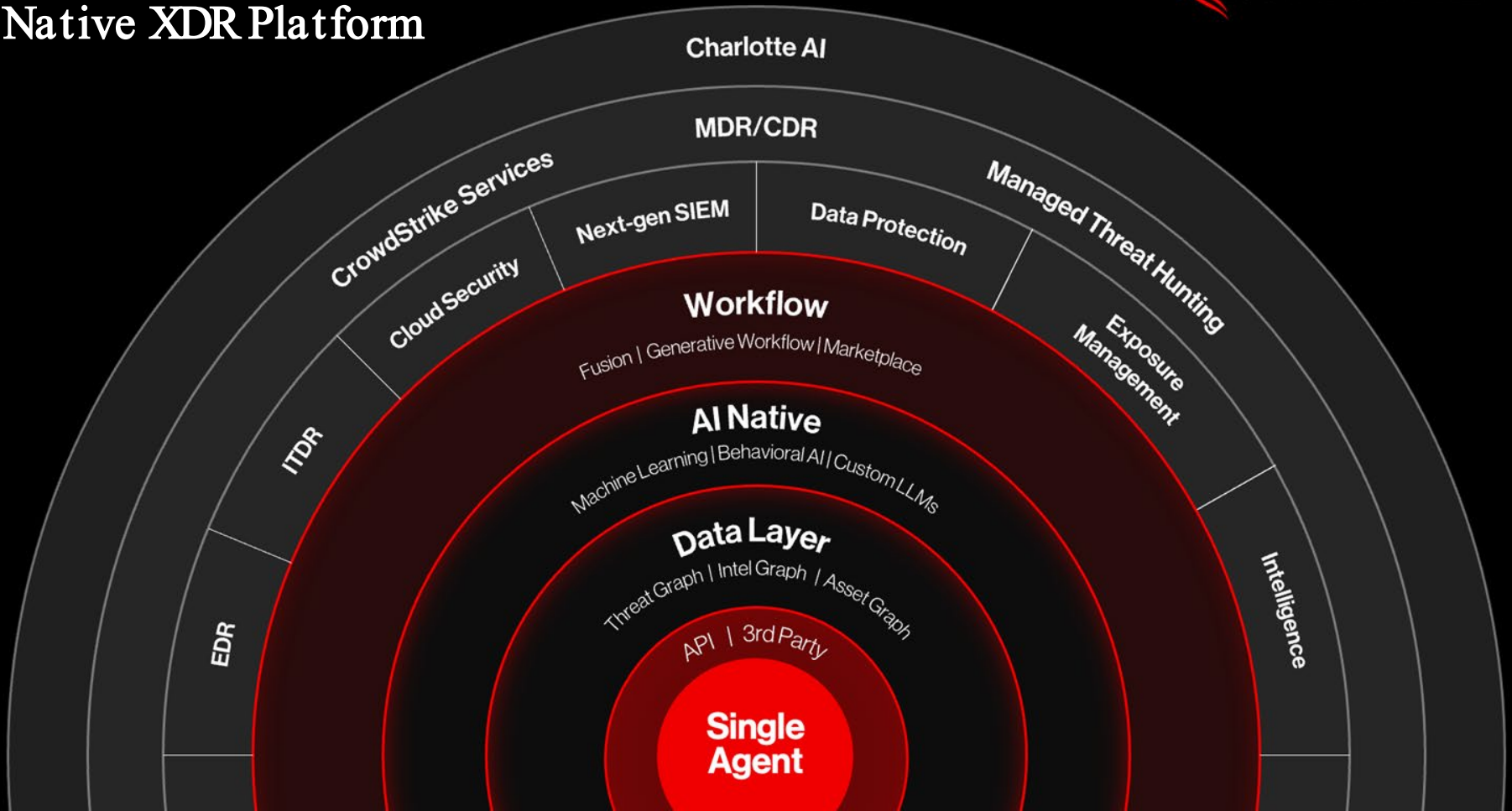
Cost

Complexity

Ease of Deployment & Operations

Cybersecurity's AI-Native XDR Platform

CROWDSTRIKE



CROWDSTRIKE

YOUR ABILITY TO DEFEAT ADVANCED CYBER THREATS RESTS ALMOST ENTIRELY ON YOUR UNDERSTANDING OF THE PROBLEM

CROWDSTRIKE