

A hand holding a wooden gavel over a document, symbolizing security and innovation. The background is dark and blurred, with a teal square in the top right corner. The text is overlaid on a dark blue rectangular background.

Innovation for the future of security

**Wolfgang Meert
CrowdStrike**



Innovation for the future of security

SCATTERED SPIDER: Tradecraft evolution

Wolfgang Meert
SALES ENGINEERING





We stop breaches



CRIMINAL

Alchemist Spider
 Aviator Spider
 Bitwise Spider
 Carbon Spider
 Chariot Spider
 Clockwork Spider
 Cyborg Spider
 Doppel Spider
 Feral Spider
 Graceful Spider
 Hidden Spider
 Hive Spider
 Indrik Spider
 Knockout Spider
 Lunar Spider
 Mallard Spider
 Mummy Spider
 Narwhal Spider
 Night Spider
 Outbreak Spider
 Outlaw Spider
 Percussion Spider
 Pinchy Spider
 Prophet Spider
 Salty Spider
 Samba Spider
 Scully Spider
 Slippy Spider
 Smoky Spider
 Solar Spider
 Sprite Spider
 Traveling Spider
 Venom Spider
 Wizard Spider
 Vice Spider

CHINA

Aquatic Panda
 Circuit Panda
 Emissary Panda
 Karma Panda
 Kryptonite Panda
 Mustang Panda
 Octane Panda
 Pirate Panda
 Puzzle Panda
 Shattered Panda
 Sunrise Panda
 Vixen Panda
 Wicked Panda

NORTH KOREA

Labyrinth Chollima
 Ricochet Chollima
 Silent Chollima
 Stardust Chollima
 Velvet Chollima

IRAN

Charming Kitten
 Chrono Kitten
 Haywire Kitten
 Imperial Kitten
 Nemesis Kitten
 Pioneer Kitten
 Refined Kitten
 Spectral Kitten
 Static Kitten
 Tracer Kitten

INDIA

Hazy Tiger
 Quilted Tiger
 Razor Tiger
 Viceroy Tiger

RUSSIA

Berserk Bear
 Cozy Bear
 Ember Bear
 Fancy Bear
 Primitive Bear
 Venomous Bear
 Voodoo Bear

PAKISTAN

Mythic Leopard
 Fringe Leopard

VIETNAM

Ocean Buffalo

SOUTH KOREA

Shadow Crane

SYRIA

Deadeye Hawk

COLOMBIA

Galactic Ocelot

TURKEY

Cosmic Wolf

HACKTIVISM

Curious Jackal
 Frontline Jackal
 Intrepid Jackal
 Partisan Jackal
 Regal Jackal
 Renegade Jackal
 Thunderbolt Jackal





ADVERSARIES ARE ADAPTING
FASTER THAN EVER

15+

**New Incident Response
Investigations Weekly**

New Techniques Developed by
Scattered Spider Monthly





SCATTERED SPIDER: TRADECRAFT EVOLUTION

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





SCATTERED SPIDER

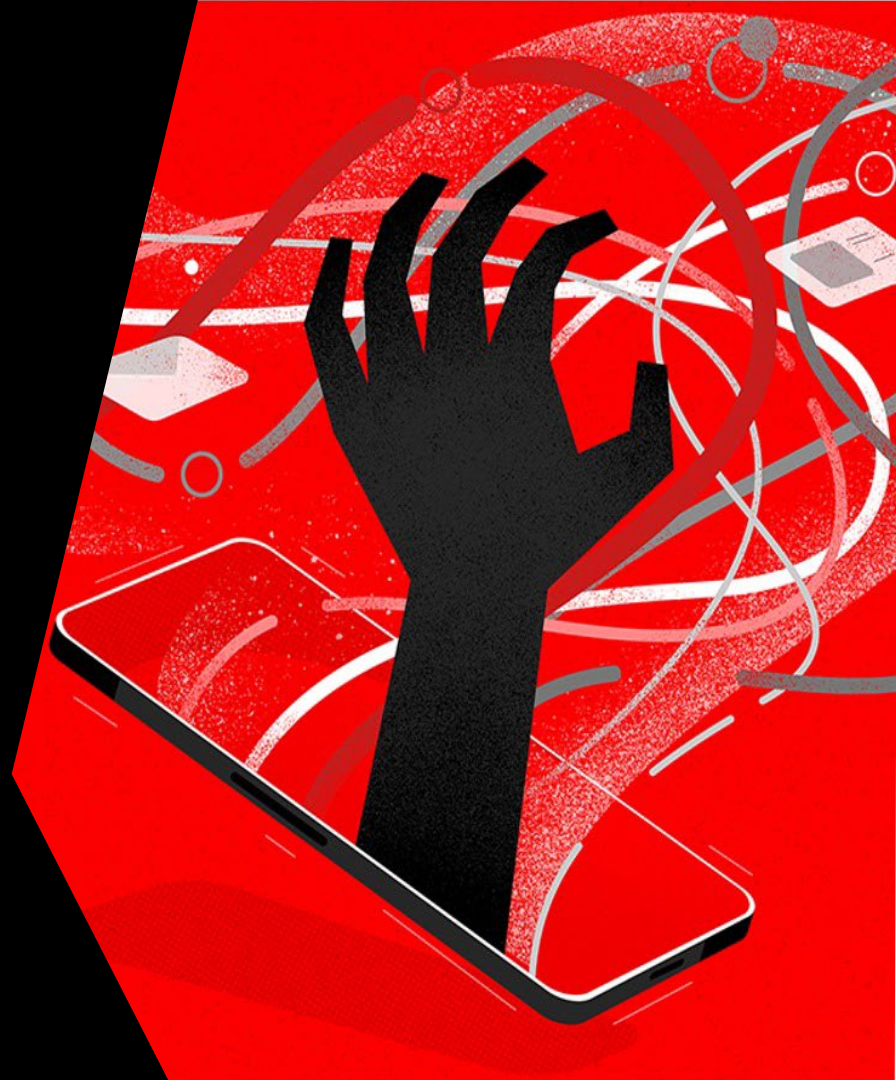
- SCATTERED SPIDER is an eCrime adversary who conducts targeted social-engineering campaigns.
- This adversary focuses on firms specialising in:
 - Customer relationship management ;
 - Business-process; outsourcing
 - Telecommunications;
 - Technology companies.
- SCATTERED SPIDER has adopted extortion and Big Game Hunting (BGH) campaigns for operational monetization.



INITIAL COMPROMISE

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

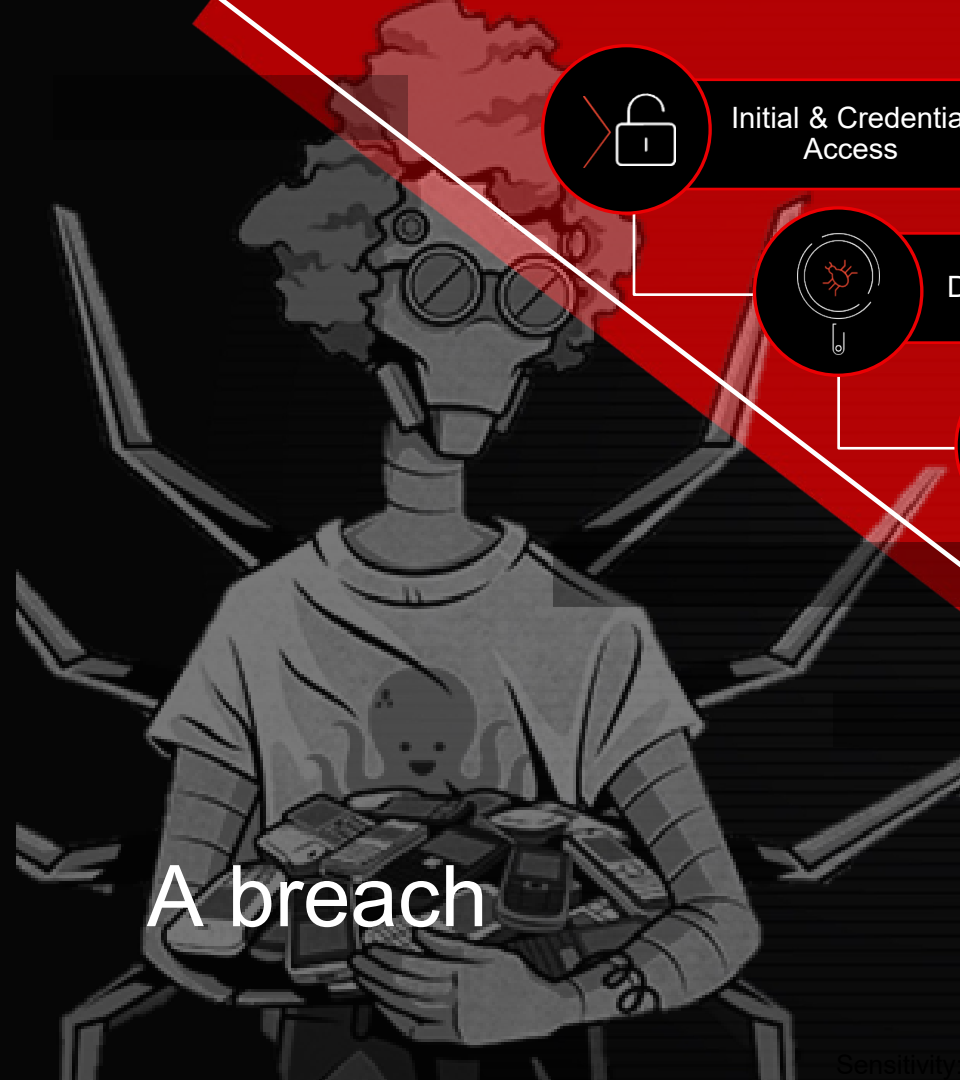
- Campaigns often started with phone calls or SMS messages
- Contact under the guise of an IT or help desk.
- Socially engineers users to share one-time password multifactor authentication (MFA) codes
- Phishing pages to capture authentication tokens
- Overwhelms using MFA notification fatigue



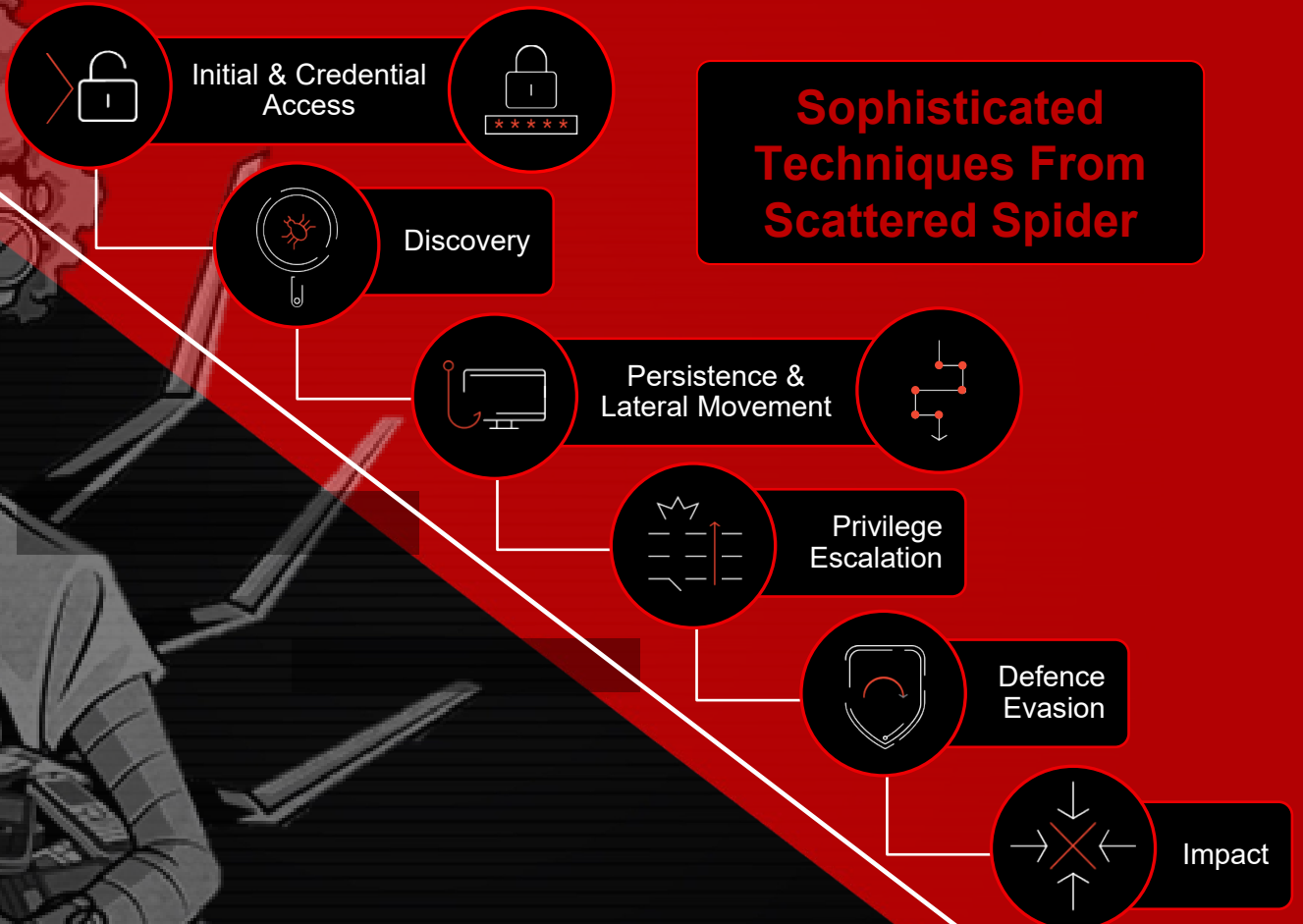


A breach



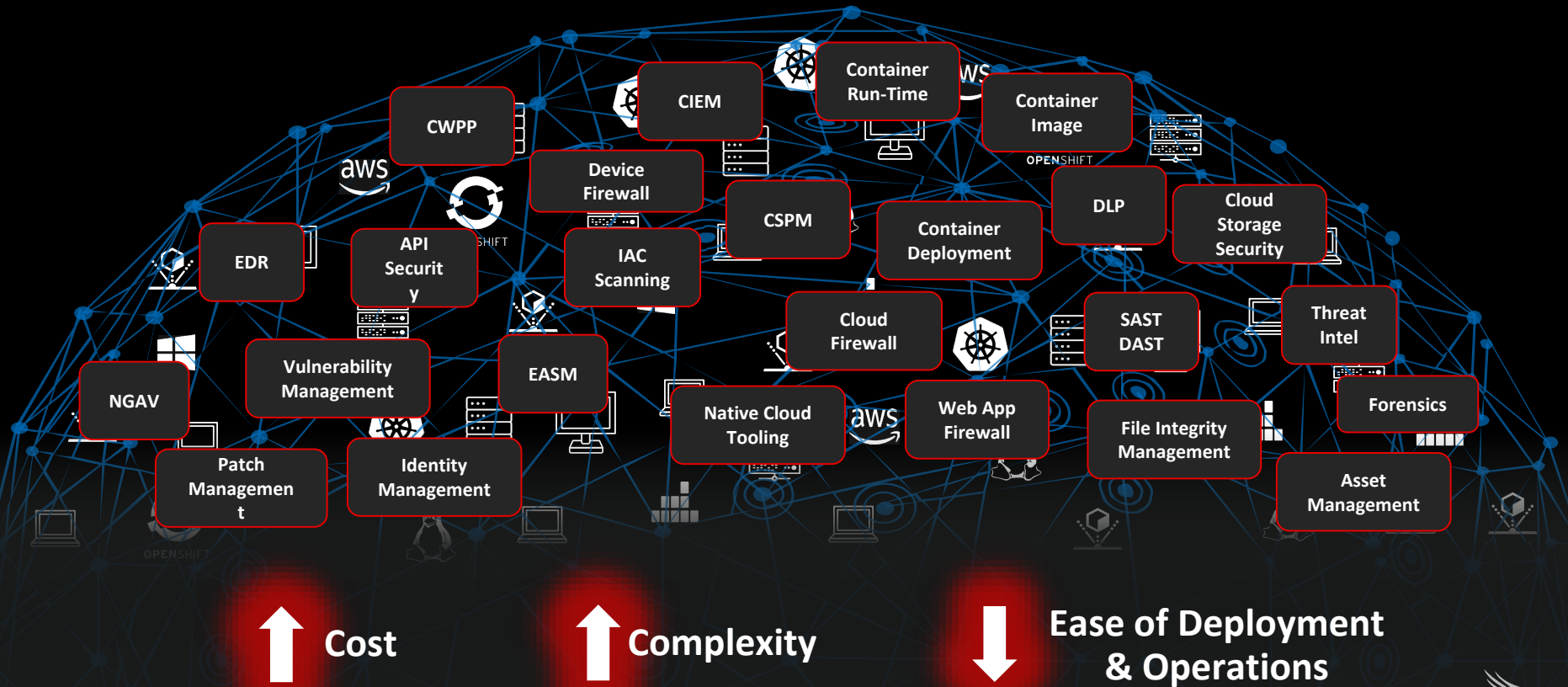


A breach

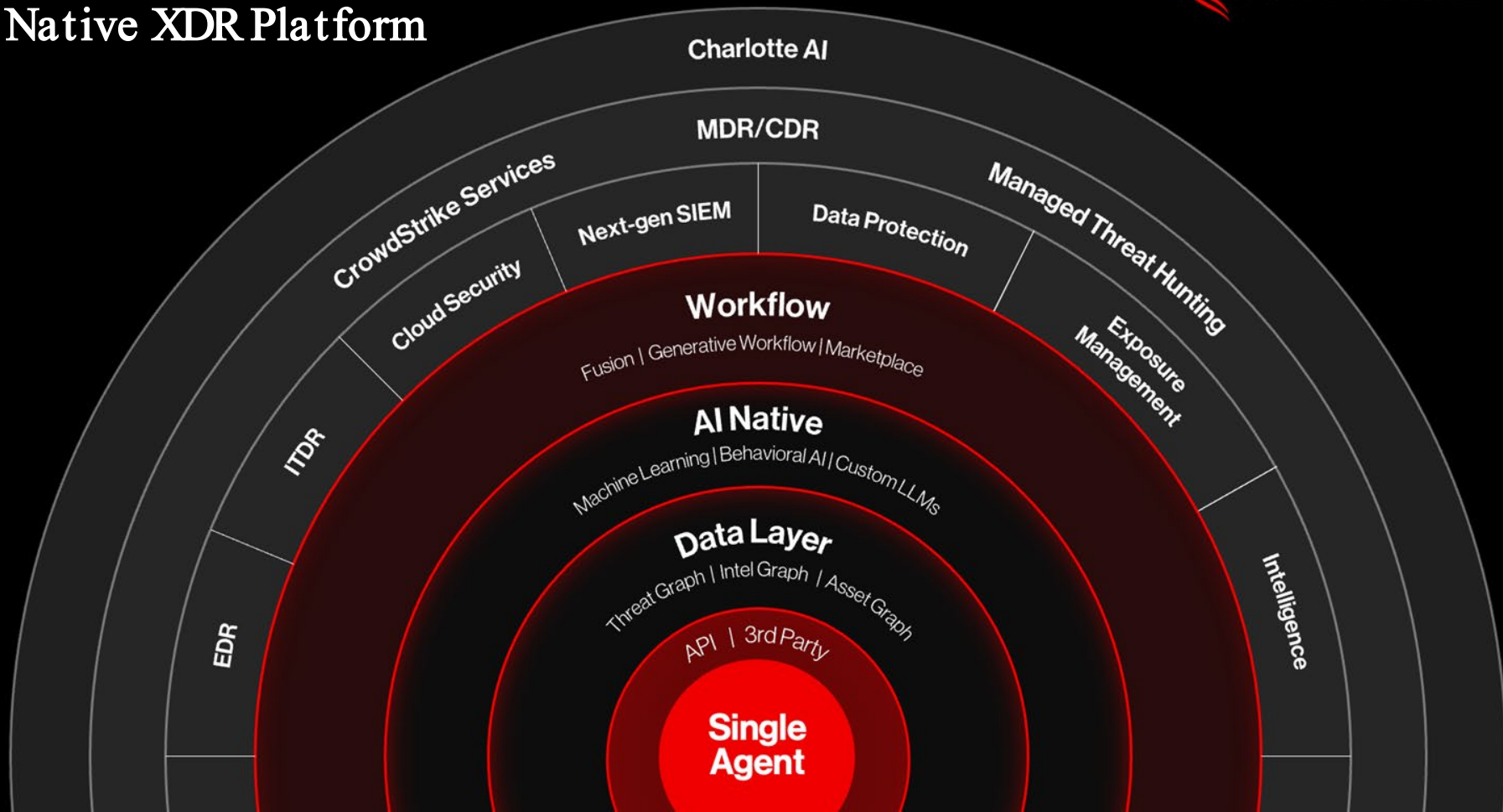


**Sophisticated
Techniques From
Scattered Spider**

ADVERSARIES LIVE IN THE GAPS BETWEEN TRADITIONAL POINT PRODUCTS



Cybersecurity's AI-Native XDR Platform





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





CROWDSTRIKE

