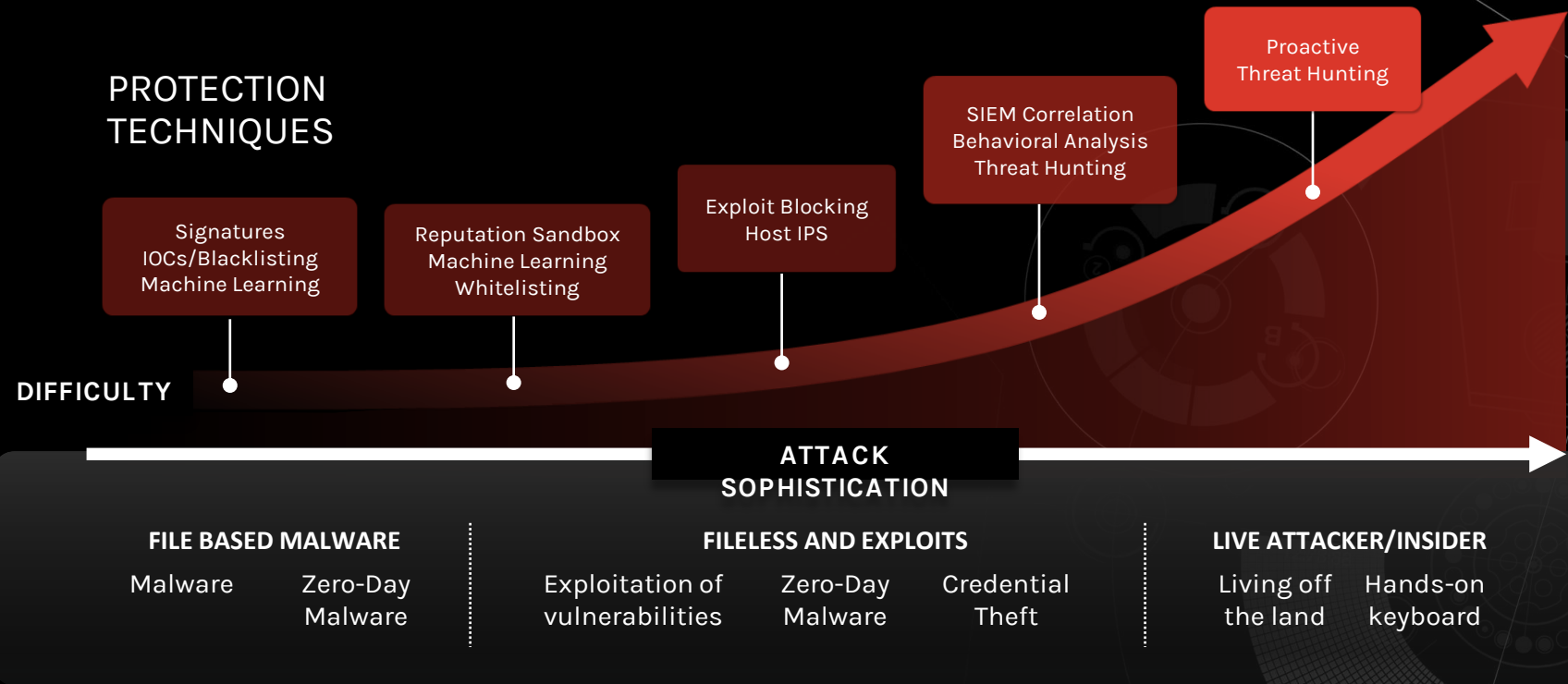**CROWDSTRIKE**

MODERN ENDPOINT SECURITY, NEXT GEN - WARUM EIN UMSTIEG GERADE JETZT WICHTIG IST

PHILIP SCHEIDL
SALES ENGINEER

CROWDSTRIKE

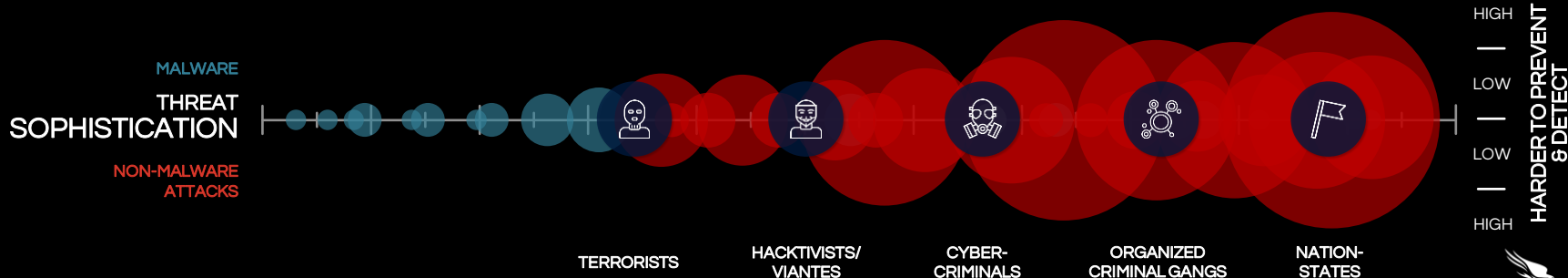# ATTACK SOPHISTICATION

PROTECTION TECHNIQUES

Proactive
Threat Hunting

SIEM Correlation
Behavioral Analysis
Threat Hunting

Exploit Blocking
Host IPS

Signatures
IOCs/Blacklisting
Machine Learning

Reputation Sandbox
Machine Learning
Whitelisting

DIFFICULTY

**ATTACK
SOPHISTICATION**

FILE BASED MALWARE		**FILELESS AND EXPLOITS**			**LIVE ATTACKER/INSIDER**	
Malware	Zero-Day Malware	Exploitation of vulnerabilities	Zero-Day Malware	Credential Theft	Living off the land	Hands-on keyboard

STOPPING MALWARE IS NOT ENOUGH

82%
Increase in ransomware-related data leaks

62%
Of attacks are malware-free

MALWARE

THREAT
SOPHISTICATION

NON-MALWARE
ATTACKS

HIGH

LOW

LOW

HIGH

HARDER TO PREVENT
& DETECT

TERRORISTS

HACKTIVISTS/
VIANTES

CYBER-
CRIMINALS

ORGANIZED
CRIMINAL GANGS

NATION-
STATES

CROWDSTRIKE

THREAT ACTORS AREN'T ALWAYS STARTING FROM HERE

Initial Access • TA0001

Discovery • TA0007

Privilege Escalation • TA0004

Credential Access • TA0006

Lateral Movement • TA0008

Impact • TA0040
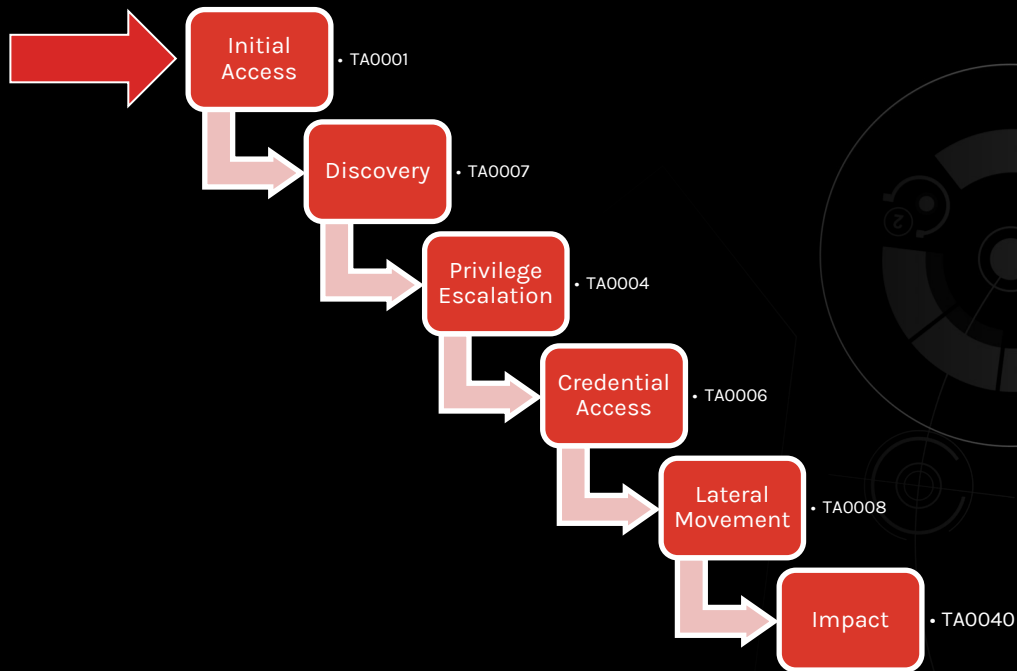
OFTEN, THEY ARE STARTING HERE

Execution

- Initial Access • TA0001
- Discovery • TA0007
- Privilege Escalation • TA0004
- Credential Access • TA0006

Identity

- Lateral Movement • TA0008
- Impact • TA0040
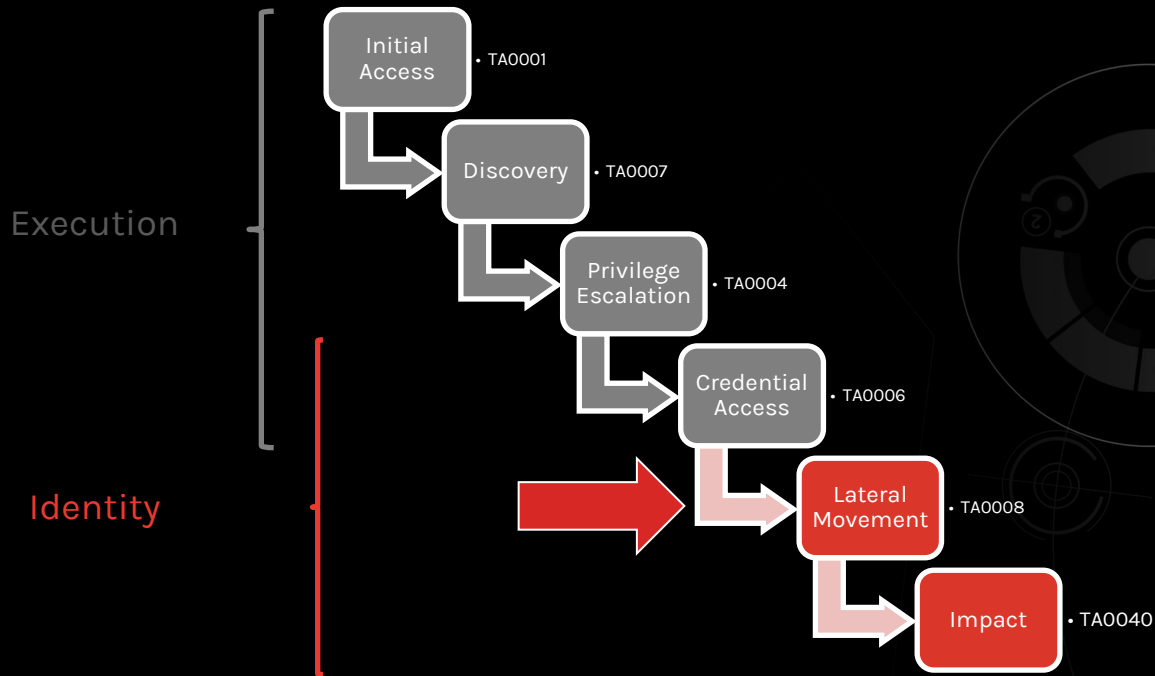
NOW WHAT?

AUTOMATED HUNTING ENGINE
THREAT GRAPH

135 MILLION
IOA DECISIONS/MIN

1 TRILLION+
EVENTS/DAY

160+
ADVERSARIES TRACKED

ENRICHED
DATA

ANALYZED
DATA

AUTOMATED HUNTING ENGINE
THREAT GRAPH

CROWDSTRIKE

135 MILLION
IOA DECISIONS/MIN

1 TRILLION+
EVENTS/DAY

160+
ADVERSARIES TRACKED

ENRICHED
DATA

ACTIONABLE
INSIGHTS

ANALYZED
DATA

65,000

POTENTIAL INTRUSIONS STOPPED

PREVENT
THREATS

HUNT
PROACTIVELY

INVESTIGATE
FASTER

ARTIFICIAL INTELLIGENCE
POWERED BY THREAT GRAPH

Block known and
unknown malware

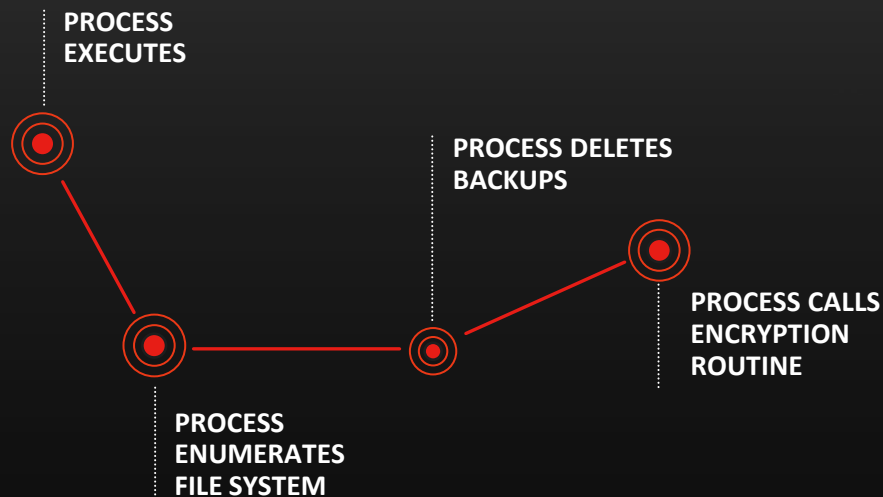Works on-network
or off-network

No signature
updates required

Continuous training,
powered by Threat Graph
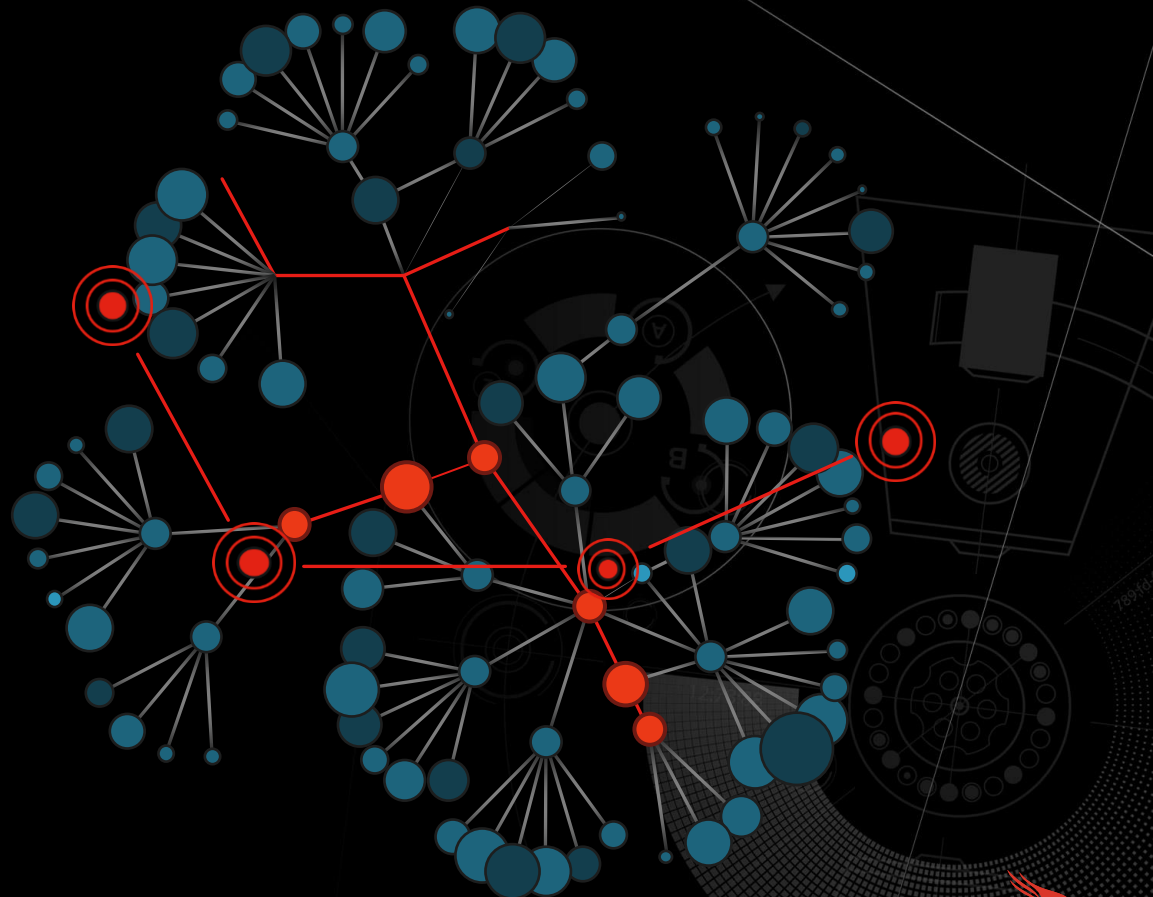
CROWDSTRIKE IDENTITY RISK SECURITY CHECK

Easy, quick & no-risk setup

- Increase cyber resistance by prioritizing and understanding user and system access risks for Active Directory

- Analyze full Active Directory & Show possible Risk factors on Prem, Hybrid, Cloud)

- Detect vulnerable Attack Paths and get recommendations

- Identify suspicious behavior and possible attackers using your Active Directory

EASY TO GET STARTED WITH CROWDSTRIKE

No infrastructure setup

No fine-tuning, rule writing

1 Install the Falcon Agent

2 Verify the installation
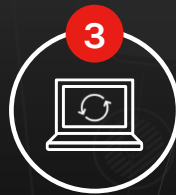
No reboot

No signatures updates

No scan

3 Remove legacy products

Start your free trial today

www.crowdstrike.com/freetrial