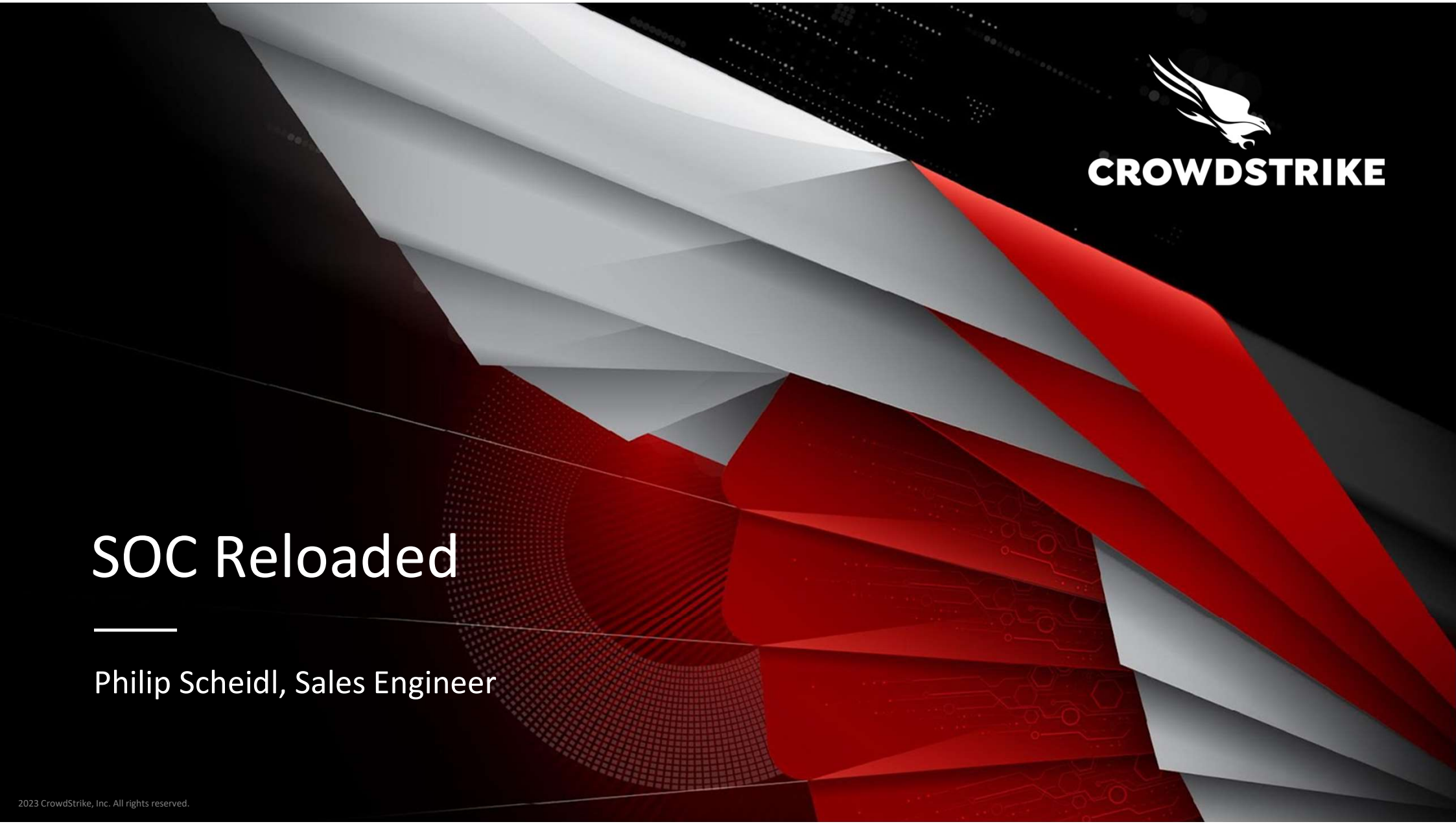
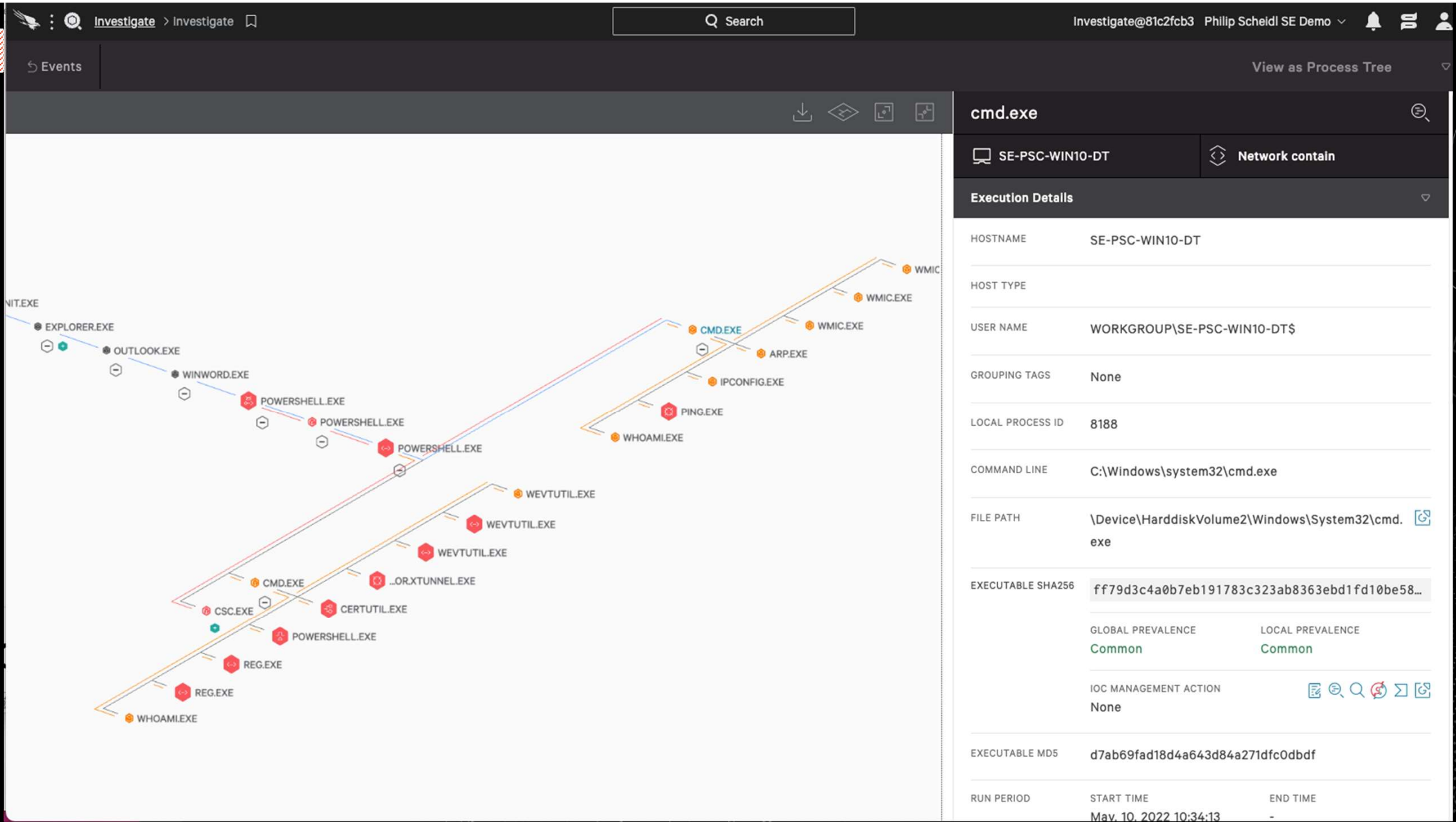
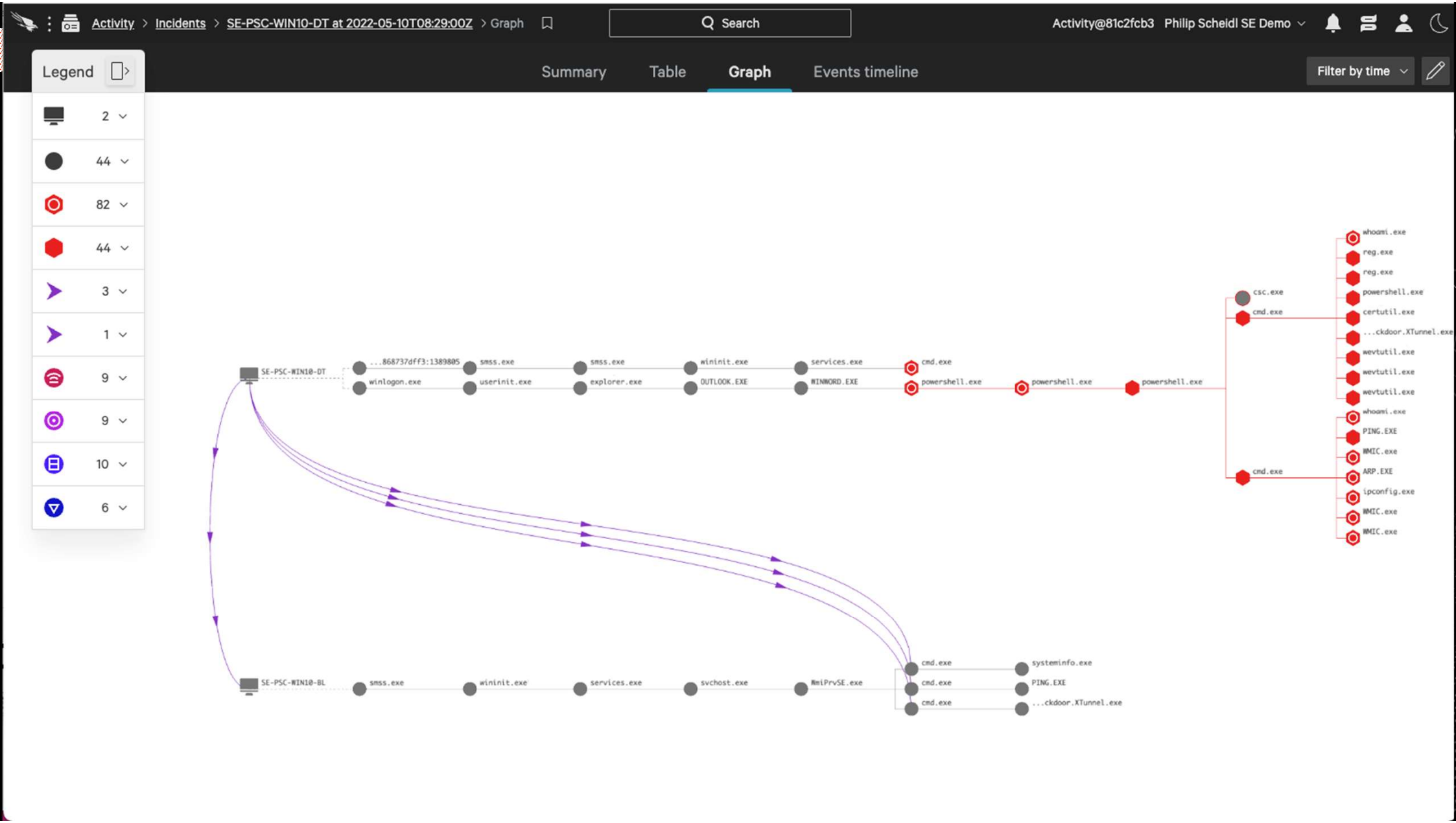


SOC Reloaded

Philip Scheidl, Sales Engineer


Investigate > Investigate
Search
Investigate@81c2fcb3 Philip Scheidl SE Demo
Events
View as Process Tree
NIT.EXE
EXPLORER.EXE
OUTLOOK.EXE
WINWORD.EXE
POWERSHELL.EXE
POWERSHELL.EXE
POWERSHELL.EXE
CMD.EXE
CSC.EXE
CERTUTIL.EXE
POWERSHELL.EXE
REG.EXE
REG.EXE
WHOAMI.EXE
WEVTUTIL.EXE
WEVTUTIL.EXE
WEVTUTIL.EXE
...OR.XTUNNEL.EXE
CMD.EXE
WMIC
WMIC.EXE
WMIC.EXE
ARP.EXE
IPCONFIG.EXE
PING.EXE
WHOAMI.EXE
cmd.exe
SE-PSC-WIN10-DT
Network contain
Execution Details
HOSTNAME
SE-PSC-WIN10-DT
HOST TYPE
USER NAME
WORKGROUP\SE-PSC-WIN10-DT$
GROUPING TAGS
None
LOCAL PROCESS ID
8188
COMMAND LINE
C:\Windows\system32\cmd.exe
FILE PATH
\Device\HarddiskVolume2\Windows\System32\cmd.exe
EXECUTABLE SHA256
ff79d3c4a0b7eb191783c323ab8363ebd1fd10be58...
GLOBAL PREVALENCE
Common
LOCAL PREVALENCE
Common
IOC MANAGEMENT ACTION
None
EXECUTABLE MD5
d7ab69fad18d4a643d84a271dfc0dbdf
RUN PERIOD
START TIME
May. 10, 2022 10:34:13
END TIME
-


Activity
Incidents
SE-PSC-WIN10-DT at 2022-05-10T08:29:00Z
Graph
Search
Activity@81c2fcb3
Philip Scheidl SE Demo
Legend
Summary
Table
Graph
Events timeline
Filter by time
2
44
82
44
3
1
9
9
10
6
SE-PSC-WIN10-DT
...868737dff3:1389805
winlogon.exe
smss.exe
userinit.exe
smss.exe
explorer.exe
wininit.exe
OUTLOOK.EXE
services.exe
WINWORD.EXE
cmd.exe
powershell.exe
powershell.exe
powershell.exe
csc.exe
cmd.exe
cmd.exe
whoami.exe
reg.exe
reg.exe
powershell.exe
certutil.exe
...ckdoor.XTunnel.exe
wevtutil.exe
wevtutil.exe
wevtutil.exe
whoami.exe
PING.EXE
WMIC.exe
ARP.EXE
ipconfig.exe
WMIC.exe
WMIC.exe
SE-PSC-WIN10-BL
smss.exe
wininit.exe
services.exe
svchost.exe
WmiPrvSE.exe
cmd.exe
cmd.exe
cmd.exe
systeminfo.exe
PING.EXE
...ckdoor.XTunnel.exe

XDR @ CROWDSTRIKE

ENTERPRISE-WIDE VISIBILITY ACROSS ALL KEY SECURITY DOMAINS

CROWDSTRIKE

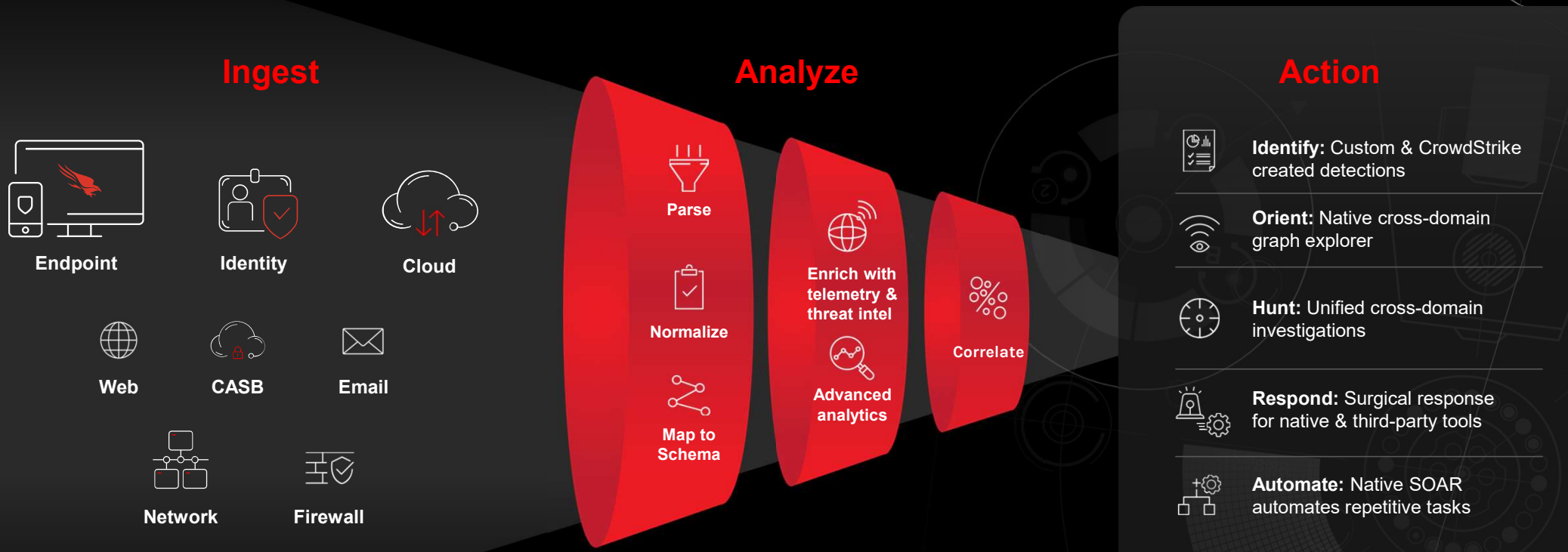
XDR

Definition | **Extended Detection Response**

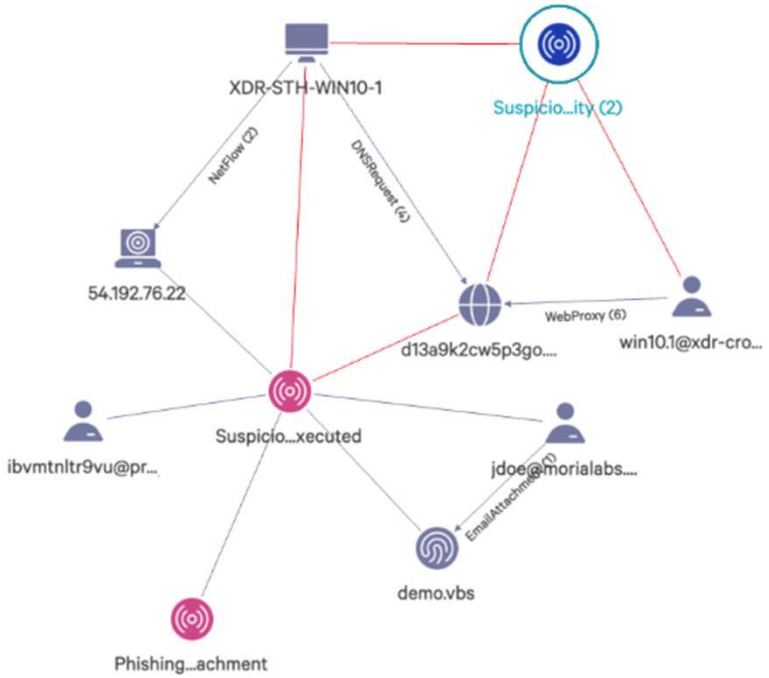
Built on the foundation of EDR, XDR extends enterprise-wide visibility across all key security domains (native & third-party) to speed and simplify near real-time detection, investigation, and response for the most sophisticated attacks

CROWDSTRIKE

UNIFY SIGNALS TO FIND THE MOST SOPHISTICATED ATTACKS ACROSS THE ENTERPRISE



CROWDSTRIKE



Suspicious Web Proxy Allowed Activity (2)

Web indicator

Event time Oct. 27, 2022 03:18:51	Log source Zscaler

Tactic & technique

Command and Control via Application Layer Protocol

Domain
Web

Description
Suspicious allowed web proxy activity observed.

Source IP 172.17.0.26	Destination IP 18.65.229.61
Action Allowed	ApplicationClass General Browsing
ApplicationName General Browsing	ContentType Other
DataDomain Web	EventID 95
HTTPRequestMethod CONNECT	HTTPResponseCode 200
MalwareCategory None	MalwareClass None
Product XDR	Protocol HTTP_PROXY
Reason Allowed	RefererURL None
RemoteAddressIP4 18.65.229.61	RemoteHostname d13a9k2cw5p3go.cloudfront.net

CROWDSTRIKE

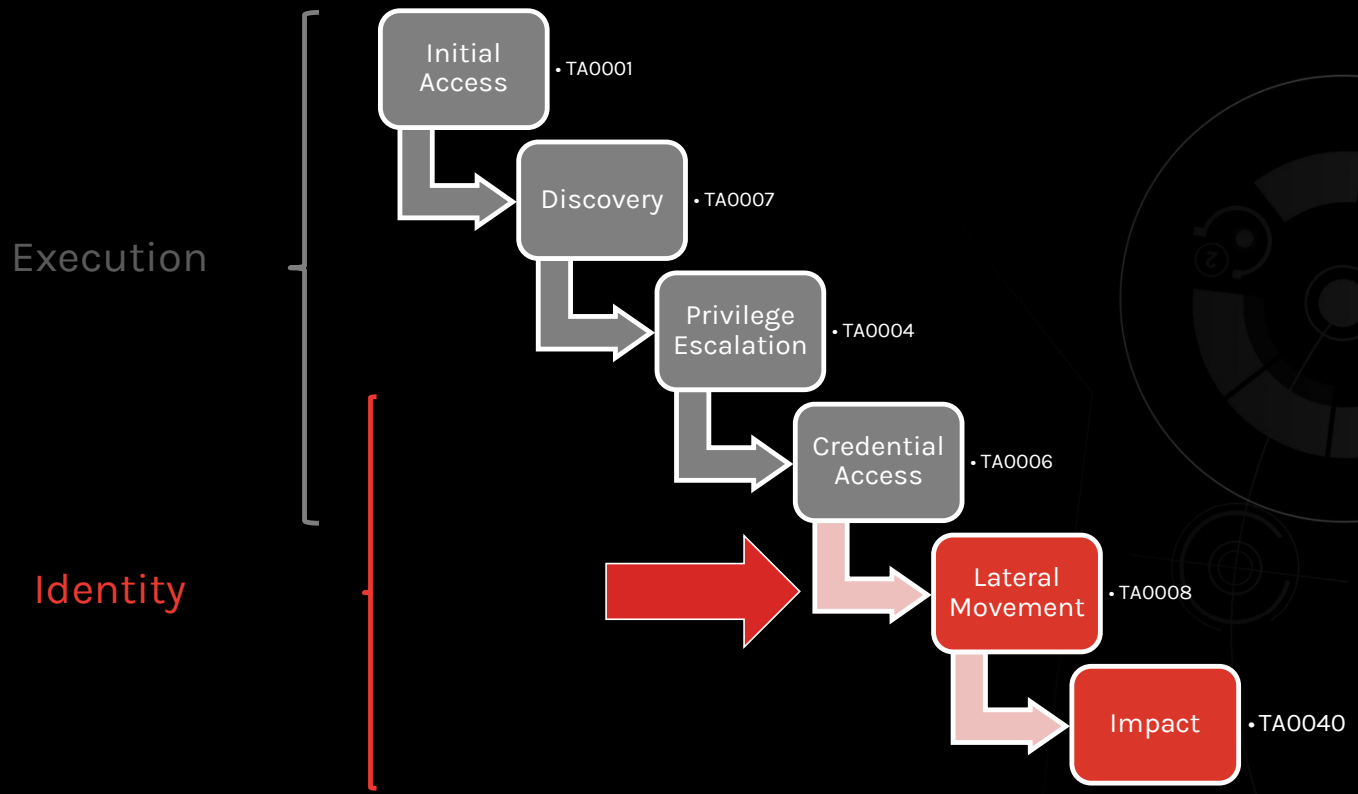
IDENTITIES

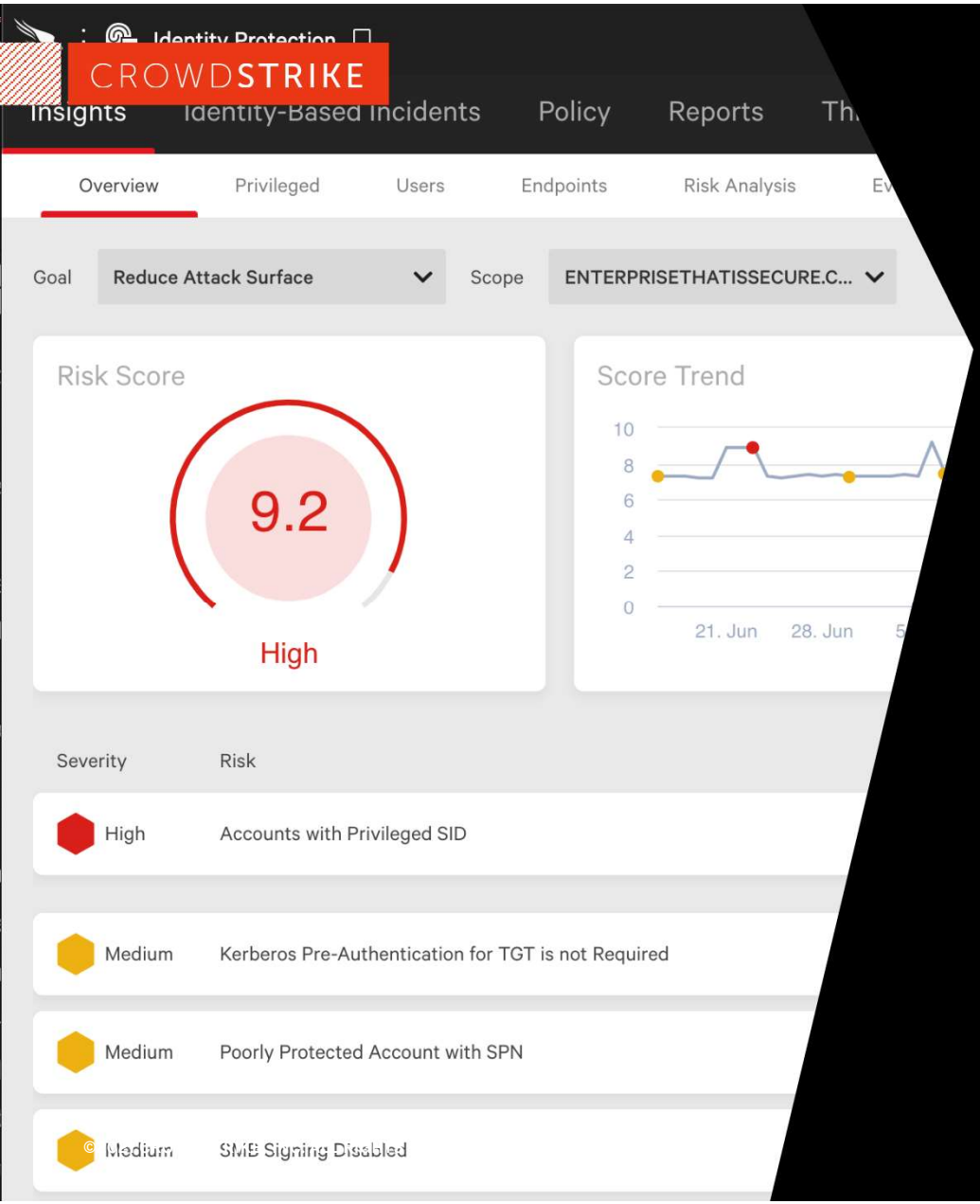
“80% OF DATA BREACHES HAVE A CONNECTION TO COMPROMISED PRIVILEGED CREDENTIALS”

- FORRESTER RESEARCH

CROWDSTRIKE

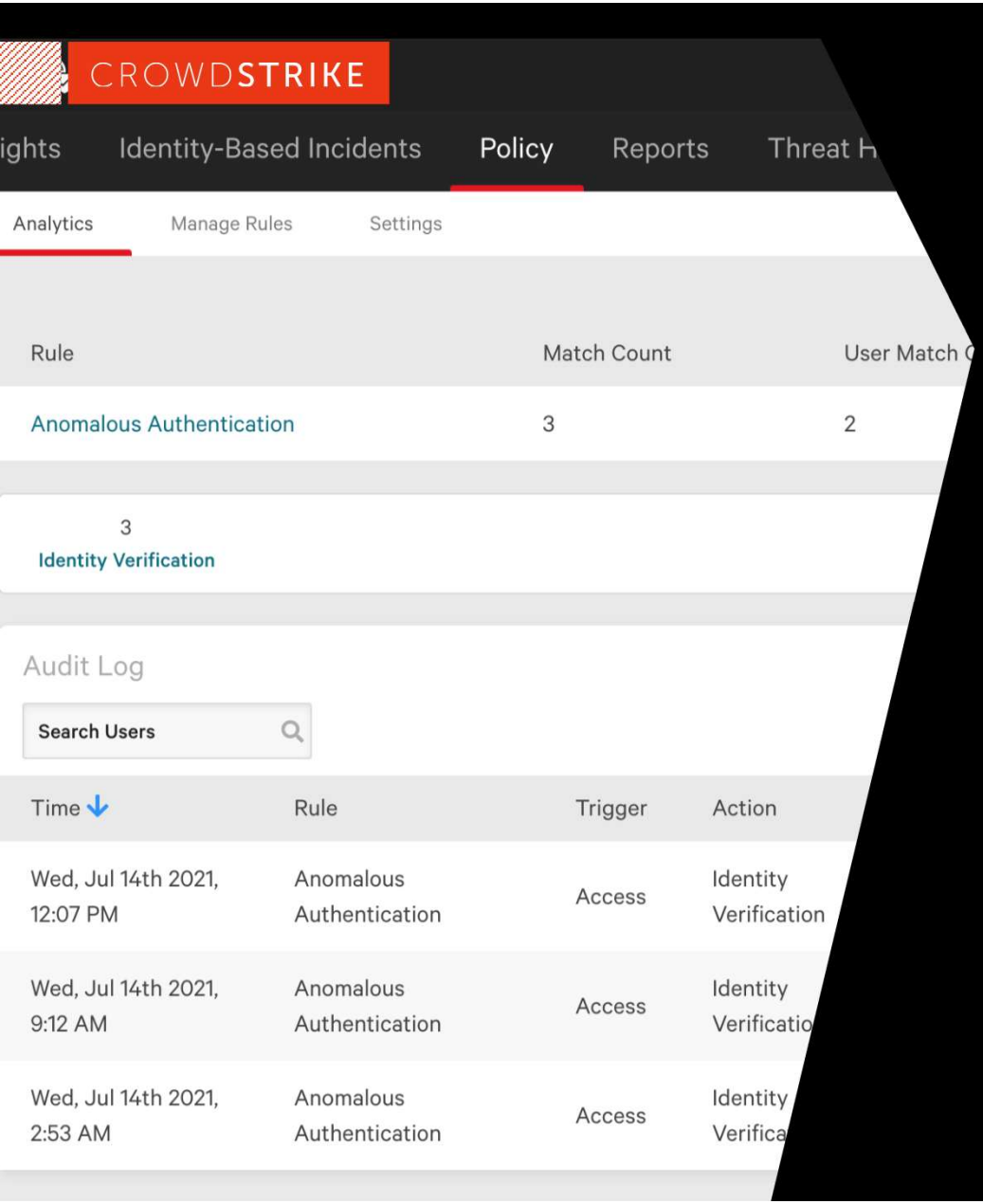
OFTEN, THEY ARE STARTING HERE





FALCON IDENTITY THREAT DETECTION

- Understand what privileged accounts exist
- Understand where privileged accounts are used
- Identify service accounts
- Identify stale accounts
- Assess the risk associated with accounts
- Assess risk associated with account usage
- Identity store stitching and correlation



FALCON IDENTITY THREAT PROTECTION

- Trust... and verify
- Automatically enforce conditional access on anomalous activity
- Create bespoke rules that allow, block, or challenge high-risk identity activity
- Integrate with current identity stores for a zero-friction end-user experience
- Stop adversaries in their tracks

THANK YOU