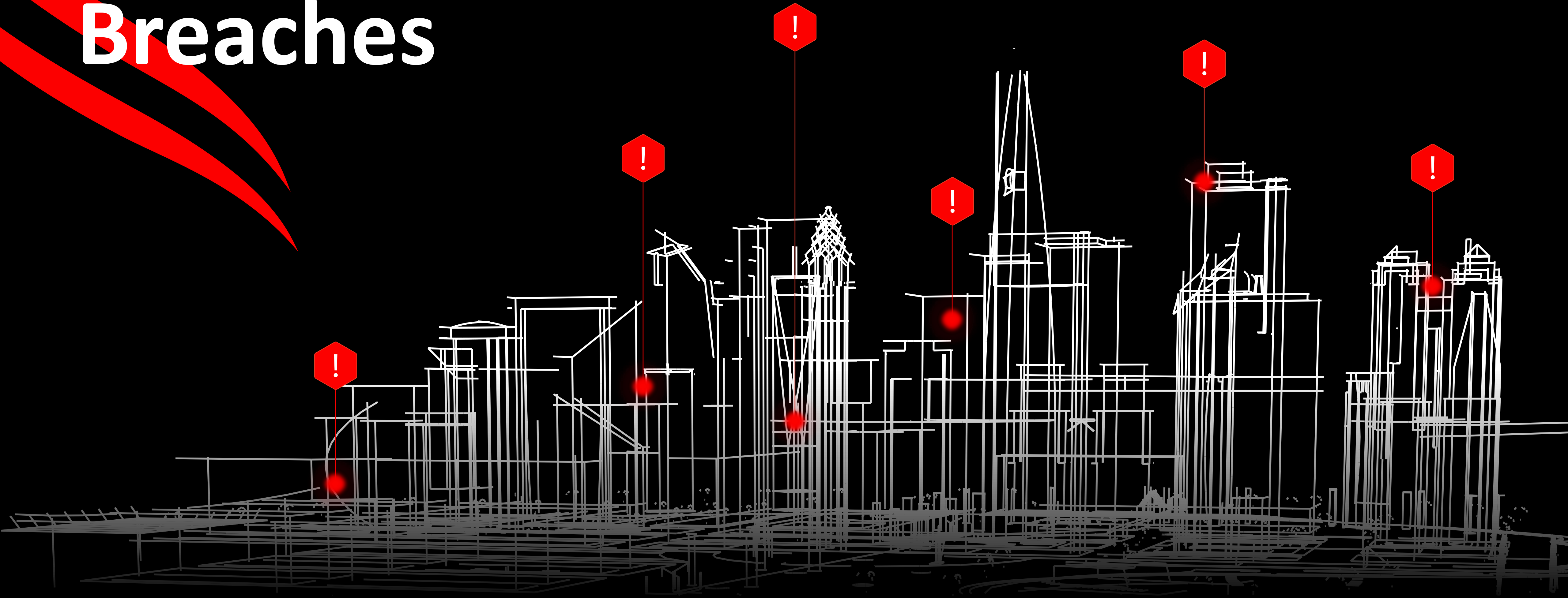
CROWDSTRIKE

Sehen wie ein Angreifer

und was NIS2 damit zu tun hat

Wolfgang Schwed, Regional Sales Manager Österreich

We Stop Breaches

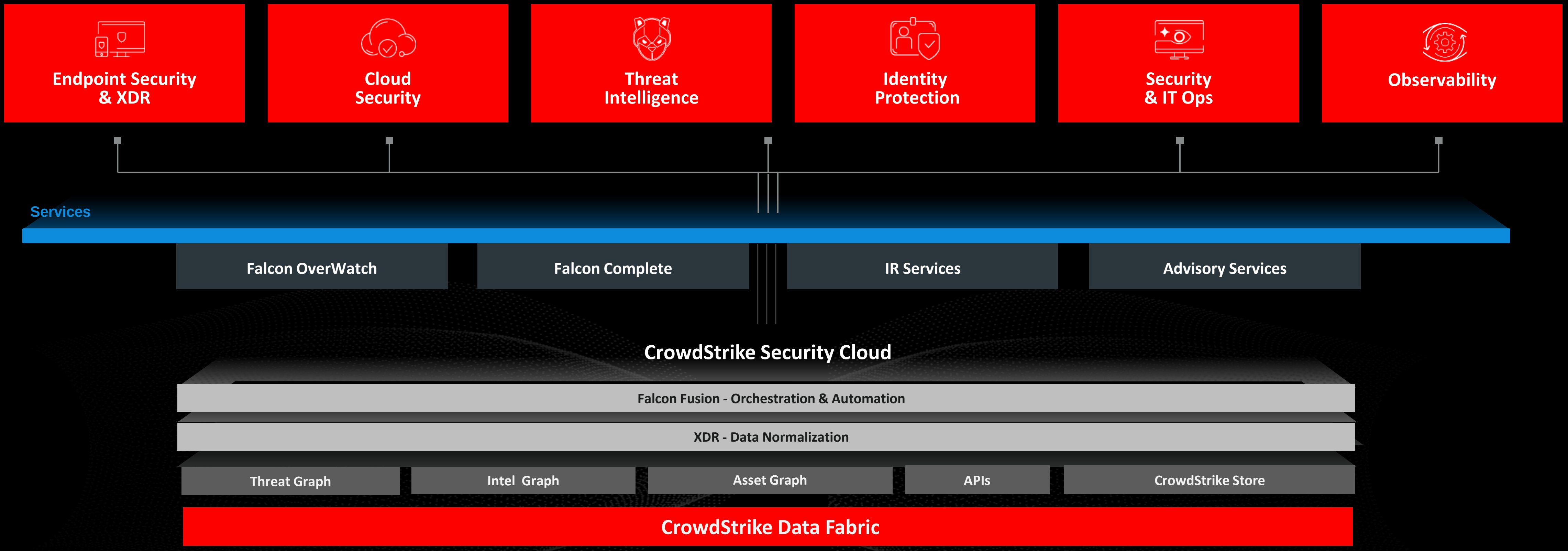


CROWDSTRIKE

NIS 2 - are you ready?

- Artikel 21, (1): “… geeignete und verhältnismäßige **technische**, operative und organisatorische **Maßnahmen** ergreifen…”
- Artikel 21, (2), a): “Konzepte in Bezug auf **Risikoanalyse und Sicherheit für Informationssysteme**”
- Artikel 21, (2), b): “Bewältigung von Sicherheitsvorfällen”
- Artikel 21, (2), e): “**Sicherheit der Lieferkette**…”
- Artikel 21, (2), f): “Konzepte und Verfahren zur **Bewertung der Wirksamkeit von Risikomanagementmaßnahmen**…”
- Artikel 21, (3): “Die spezifischen Schwachstellen der **einzelnen unmittelbaren Anbieter und Dienstanbieter** […] berücksichtigen”

THE CrowdStrike Falcon Platform



Endpoint Security & XDR

Cloud Security

Threat Intelligence

Identity Protection

Security & IT Ops

Observability

Services

Falcon OverWatch

Falcon Complete

IR Services

Advisory Services

CrowdStrike Security Cloud

Falcon Fusion - Orchestration & Automation

XDR - Data Normalization

Threat Graph

Intel Graph

Asset Graph

APIs

CrowdStrike Store

CrowdStrike Data Fabric

UNDERSTANDING THE THREAT LANDSCAPE

Motivations

NATION STATE

ECRIME

HACKTIVISM

Nation State Goals

CHINA

ECONOMIC ESPIONAGE
INTELLIGENCE COLLECTION

North Korea

CURRENCY GENERATION
ECONOMIC ESPIONAGE

IRAN

GEOPOLITICAL CAMPAIGNS
TELECOM FOCUSED

RUSSIA

INFORMATION OPERATIONS
CRITICAL INFRASTRUCTURE

Sophisticated & Symbiotic E-Crime Ecosystem

SERVICES

CAPABILITIES ENABLING CYBER CRIMINAL ACTIVITY

DISTRIBUTION

VEHICLES LEVERAGED FOR DELIVERING TO VICTIMS

MONETIZATION

CAPITALIZING ON SUCCESSFUL EXECUTION

THREAT INTELLIGENCE FOCAL POINTS

THREAT ADVERSARY INTELLIGENCE

Finished & actionable Intelligence

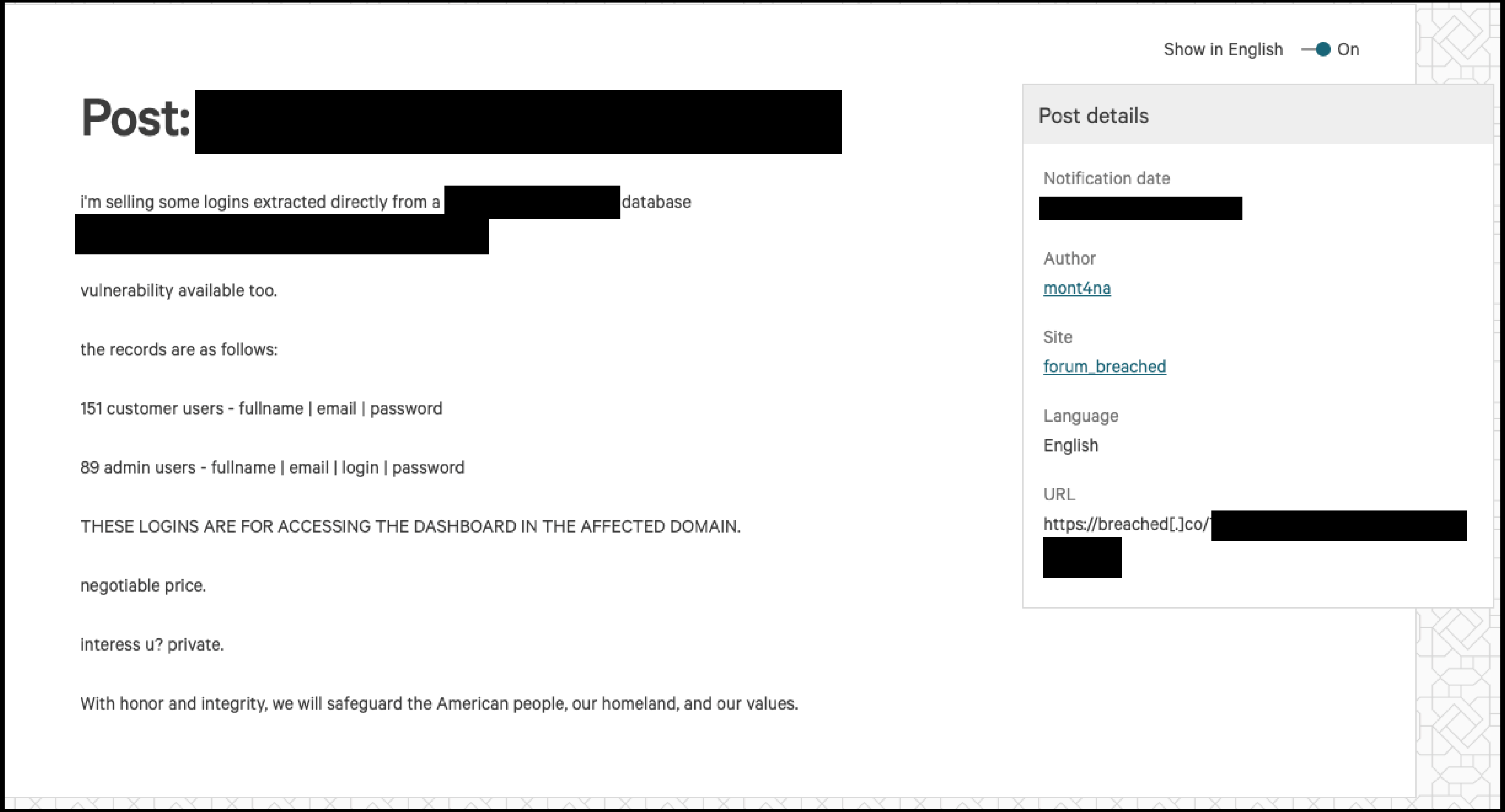
INSIDE your organization

DIGITAL RISK MONITORING

Raw Intelligence

OUTSIDE your organization

THREAT INTELLIGENCE – OUTSIDE YOUR ORGANISATION



Show in English ● On

Post: [redacted]

i'm selling some logins extracted directly from a [redacted] database [redacted]

vulnerability available too.

the records are as follows:

151 customer users - fullname | email | password

89 admin users - fullname | email | login | password

THESE LOGINS ARE FOR ACCESSING THE DASHBOARD IN THE AFFECTED DOMAIN.

negotiable price.

interess u? private.

With honor and integrity, we will safeguard the American people, our homeland, and our values.

Post details

Notification date
[redacted]

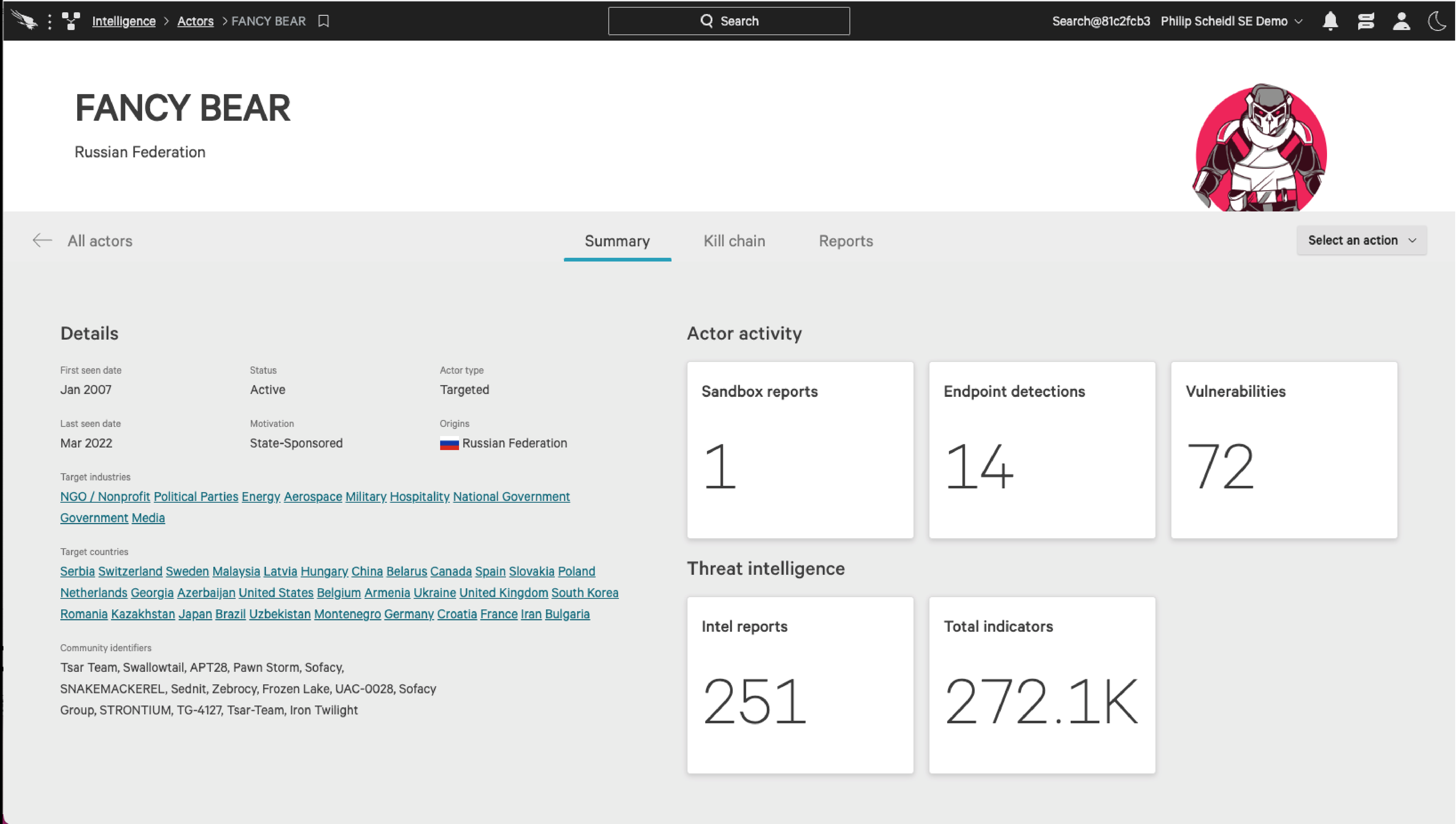
Author
mont4na

Site
forum_breached

Language
English

URL
https://breached[.]co/[redacted]

CROWDSTRIKE


Intelligence > Actors > FANCY BEAR
Search
Search@81c2fcb3 Philip Scheidl SE Demo
All actors
Summary
Kill chain
Reports
Select an action

FANCY BEAR

Russian Federation

Details

First seen date
Jan 2007

Status
Active

Actor type
Targeted

Last seen date
Mar 2022

Motivation
State-Sponsored

Origins
Russian Federation

Target industries
NGO / Nonprofit Political Parties Energy Aerospace Military Hospitality National Government Government Media

Target countries
Serbia Switzerland Sweden Malaysia Latvia Hungary China Belarus Canada Spain Slovakia Poland Netherlands Georgia Azerbaijan United States Belgium Armenia Ukraine United Kingdom South Korea Romania Kazakhstan Japan Brazil Uzbekistan Montenegro Germany Croatia France Iran Bulgaria

Community identifiers
Tsar Team, Swallowtail, APT28, Pawn Storm, Sofacy, SNAKEMACKEREL, Sednit, Zebrocy, Frozen Lake, UAC-0028, Sofacy Group, STRONTIUM, TG-4127, Tsar-Team, Iron Twilight

Actor activity

Sandbox reports
1

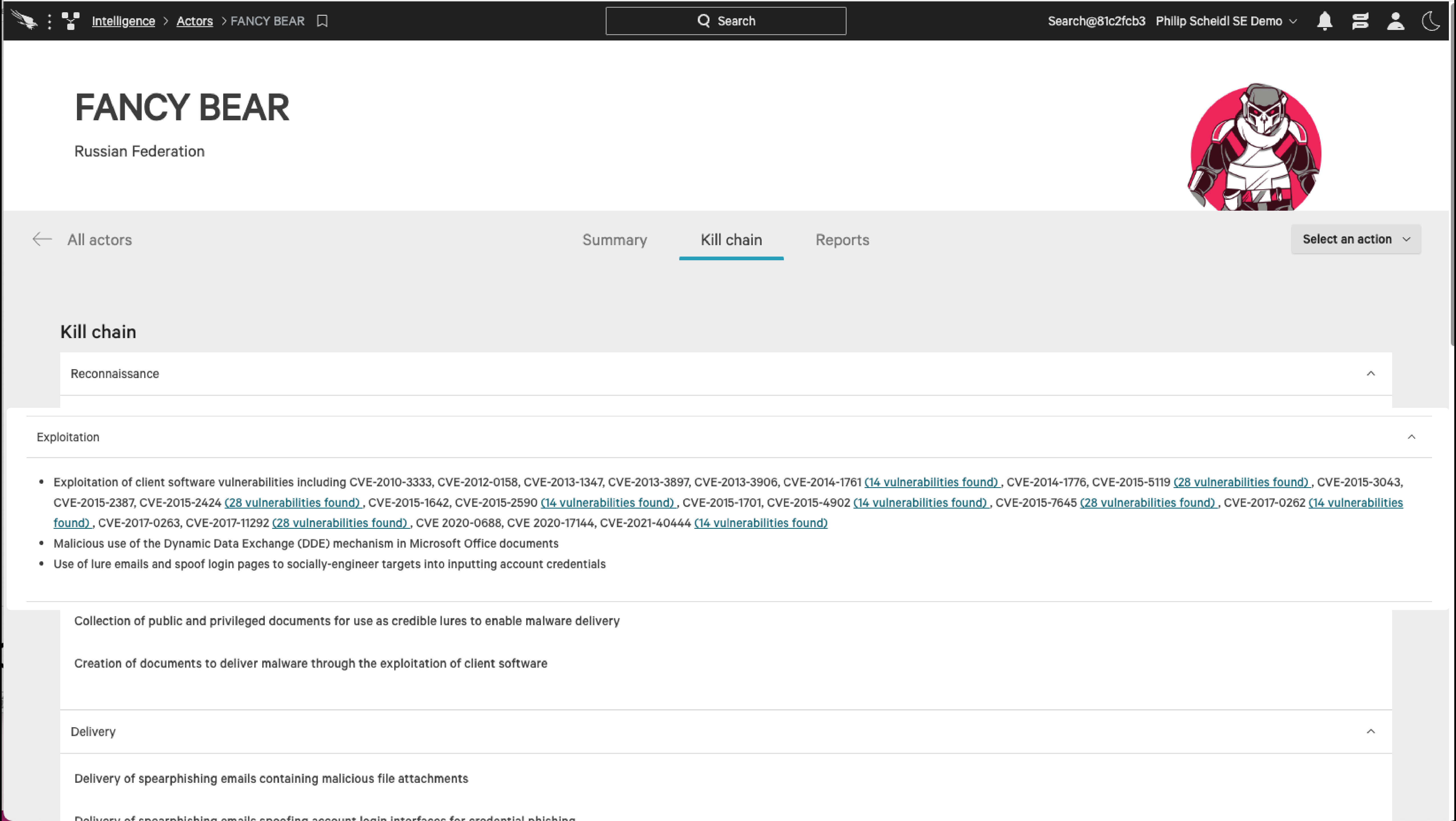
Endpoint detections
14

Vulnerabilities
72

Threat intelligence

Intel reports
251

Total indicators
272.1K


Intelligence > Actors > FANCY BEAR
Search
Search@81c2fcb3 Philip Scheidl SE Demo
All actors
Summary
Kill chain
Reports
Select an action

FANCY BEAR

Russian Federation

Kill chain

Reconnaissance

Exploitation

- Exploitation of client software vulnerabilities including CVE-2010-3333, CVE-2012-0158, CVE-2013-1347, CVE-2013-3897, CVE-2013-3906, CVE-2014-1761 (14 vulnerabilities found) , CVE-2014-1776, CVE-2015-5119 (28 vulnerabilities found) , CVE-2015-3043, CVE-2015-2387, CVE-2015-2424 (28 vulnerabilities found) , CVE-2015-1642, CVE-2015-2590 (14 vulnerabilities found) , CVE-2015-1701, CVE-2015-4902 (14 vulnerabilities found) , CVE-2015-7645 (28 vulnerabilities found) , CVE-2017-0262 (14 vulnerabilities found) , CVE-2017-0263, CVE-2017-11292 (28 vulnerabilities found) , CVE 2020-0688, CVE 2020-17144, CVE-2021-40444 (14 vulnerabilities found)
- Malicious use of the Dynamic Data Exchange (DDE) mechanism in Microsoft Office documents
- Use of lure emails and spoof login pages to socially-engineer targets into inputting account credentials

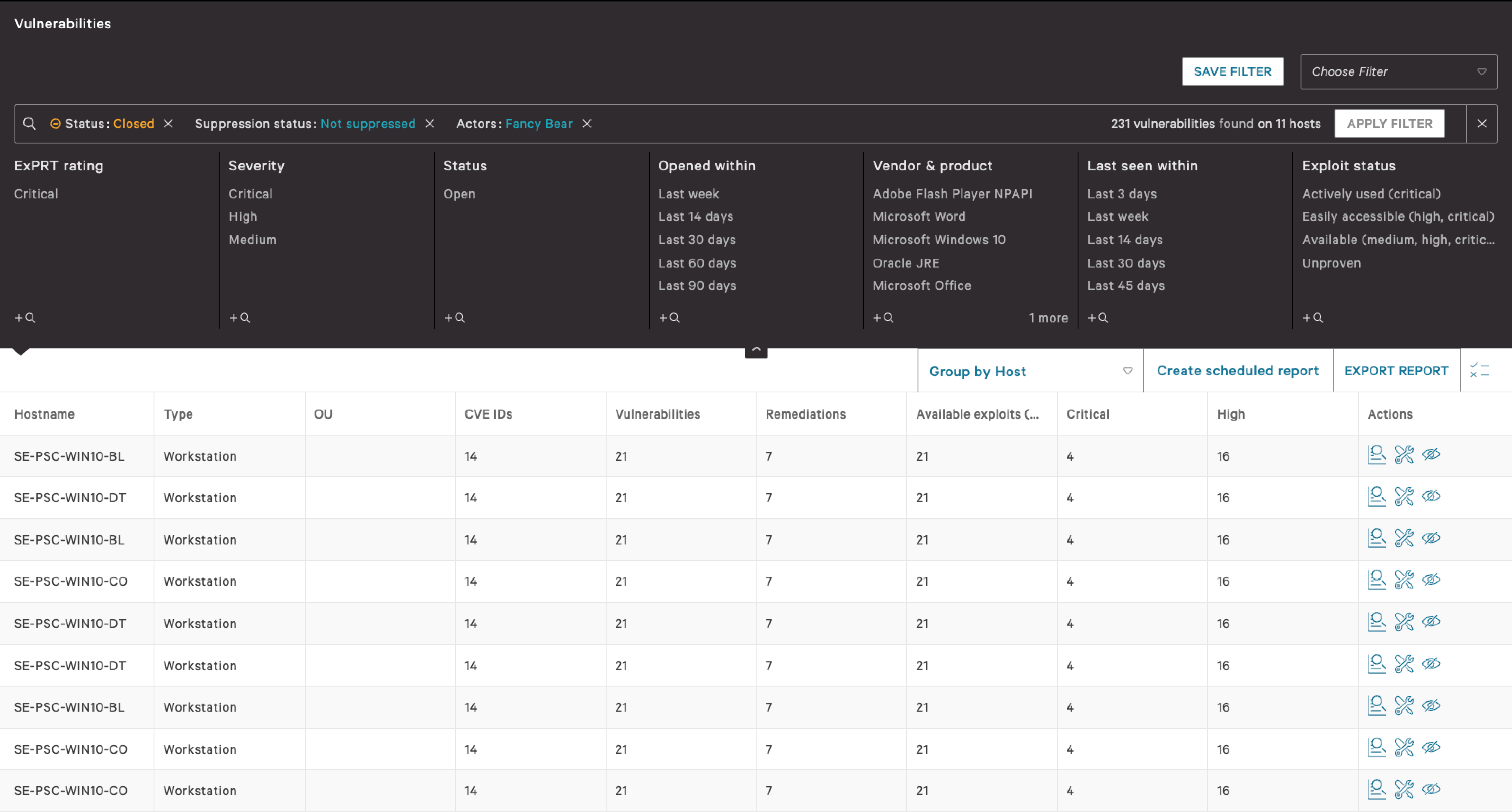
Collection of public and privileged documents for use as credible lures to enable malware delivery

Creation of documents to deliver malware through the exploitation of client software

Delivery

Delivery of spearphishing emails containing malicious file attachments

Delivery of spearphishing emails spoofing account login interfaces for credential phishing



Vulnerabilities

Status: Closed ✕ Suppression status: Not suppressed ✕ Actors: Fancy Bear ✕

231 vulnerabilities found on 11 hosts

ExPRT rating
- Critical

Severity
- Critical
- High
- Medium

Status
- Open

Opened within
- Last week
- Last 14 days
- Last 30 days
- Last 60 days
- Last 90 days

Vendor & product
- Adobe Flash Player NPAPI
- Microsoft Word
- Microsoft Windows 10
- Oracle JRE
- Microsoft Office
- 1 more

Last seen within
- Last 3 days
- Last week
- Last 14 days
- Last 30 days
- Last 45 days

Exploit status
- Actively used (critical)
- Easily accessible (high, critical)
- Available (medium, high, critic...
- Unproven

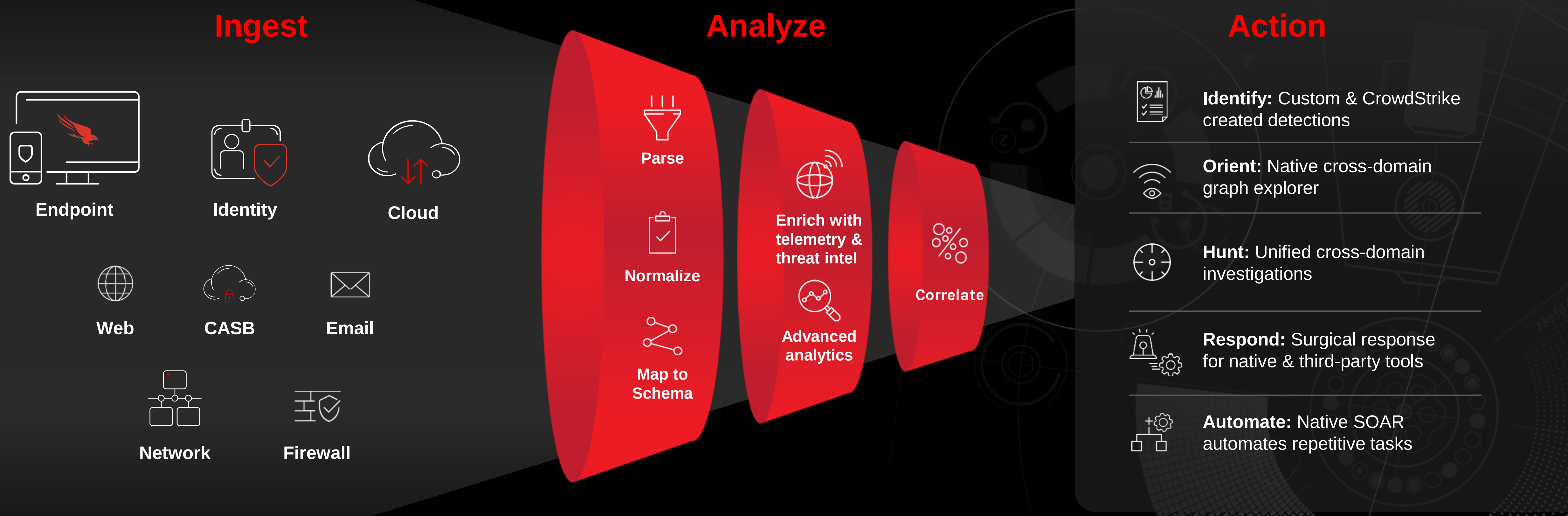
Hostname	Type	OU	CVE IDs	Vulnerabilities	Remediations	Available exploits (...	Critical	High	Actions
SE-PSC-WIN10-BL	Workstation		14	21	7	21	4	16	
SE-PSC-WIN10-DT	Workstation		14	21	7	21	4	16	
SE-PSC-WIN10-BL	Workstation		14	21	7	21	4	16	
SE-PSC-WIN10-CO	Workstation		14	21	7	21	4	16	
SE-PSC-WIN10-DT	Workstation		14	21	7	21	4	16	
SE-PSC-WIN10-DT	Workstation		14	21	7	21	4	16	
SE-PSC-WIN10-BL	Workstation		14	21	7	21	4	16	
SE-PSC-WIN10-CO	Workstation		14	21	7	21	4	16	
SE-PSC-WIN10-CO	Workstation		14	21	7	21	4	16	

SEHEN WIE EIN ANGREIFER –

IM UNTERNEHMEN

CROWDSTRIKE

FALCON XDR: UNIFY SIGNALS TO FIND THE MOST SOPHISTICATED ATTACKS ACROSS THE ENTERPRISE



Ingest

Endpoint

Identity

Cloud

Web

CASB

Email

Network

Firewall

Analyze

Parse

Normalize

Map to Schema

Enrich with telemetry & threat intel

Advanced analytics

Correlate

Action

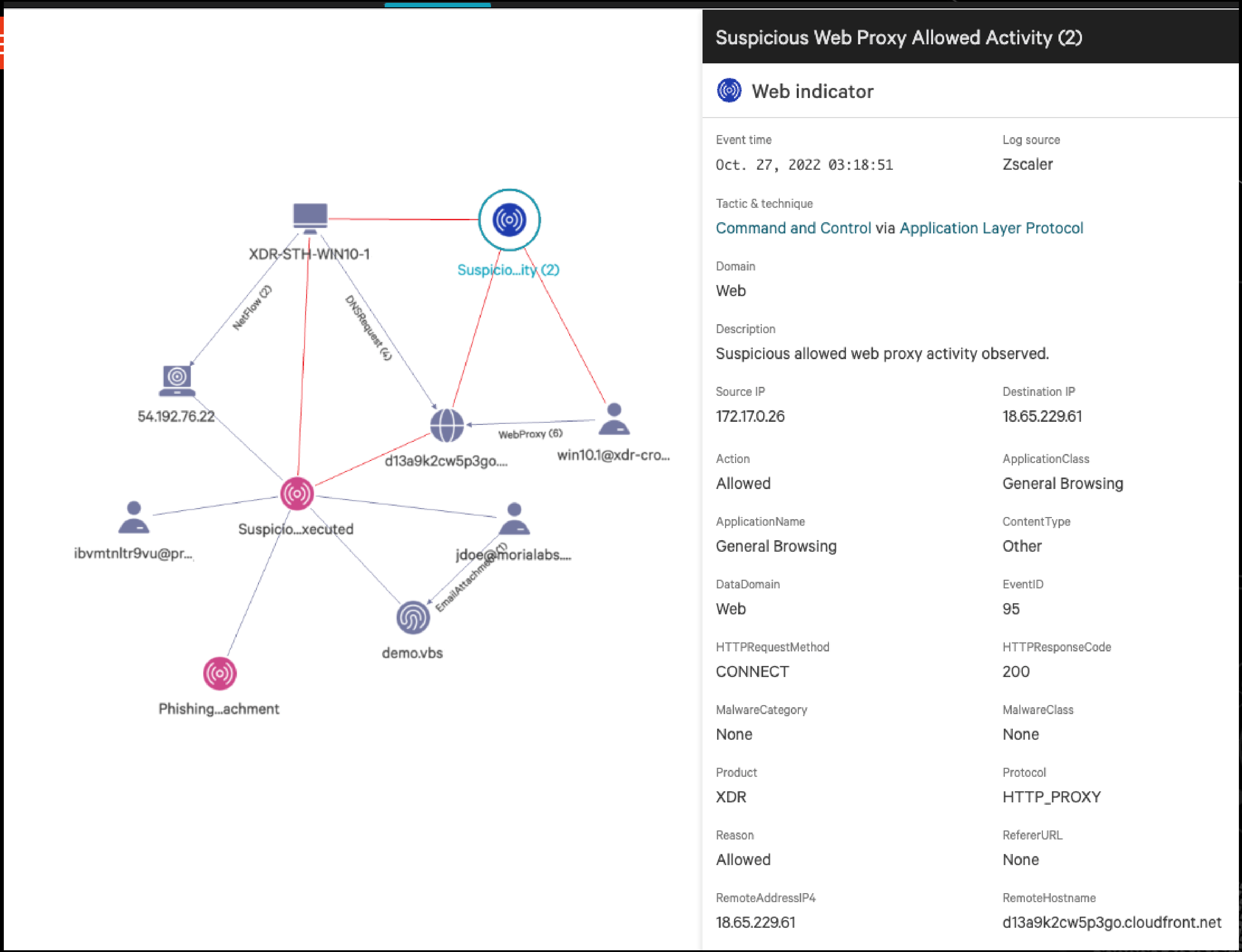
Identify: Custom & CrowdStrike created detections

Orient: Native cross-domain graph explorer

Hunt: Unified cross-domain investigations

Respond: Surgical response for native & third-party tools

Automate: Native SOAR automates repetitive tasks



Suspicious Web Proxy Allowed Activity (2)

Web indicator

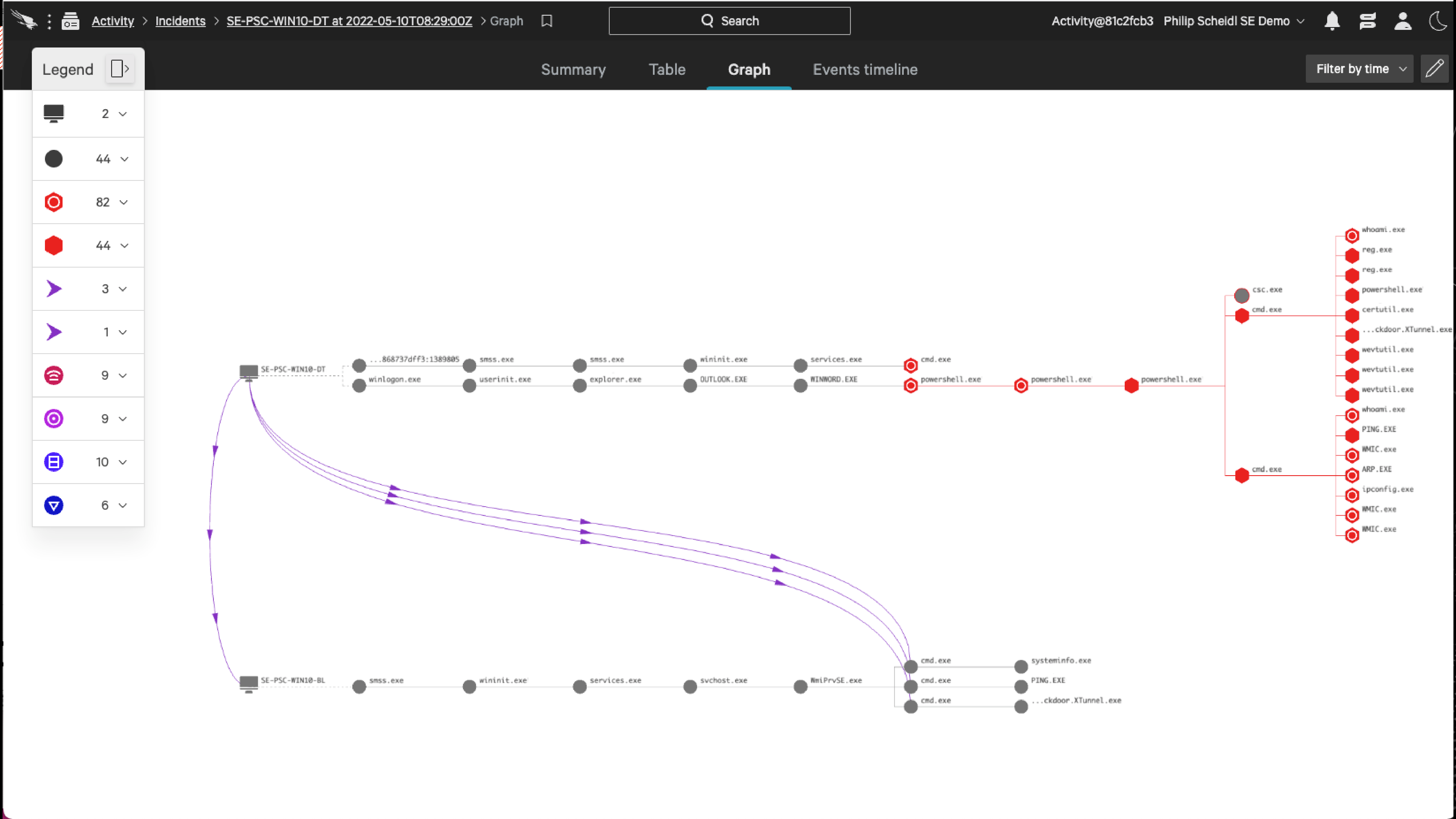
Event time Oct. 27, 2022 03:18:51	Log source Zscaler

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


Activity
Incidents
SE-PSC-WIN10-DT at 2022-05-10T08:29:00Z
Graph
Search
Activity@81c2fcb3
Philip Scheidl SE Demo
Legend
2
44
82
44
3
1
9
9
10
6
Summary
Table
Graph
Events timeline
Filter by time
SE-PSC-WIN10-DT
...868737dff3:1389805
smss.exe
smss.exe
wininit.exe
services.exe
cmd.exe
winlogon.exe
userinit.exe
explorer.exe
OUTLOOK.EXE
WINWORD.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

CROWDSTRIKE

Visibility across all key security domains and leading third-party vendors

Identity/SSO	Web security (SWG)	Cloud access security broker (CASB)	CrowdStrike	Email	Network detection & response (NDR)	Firewall
PingIdentity.	zscaler	zscaler	Falcon Insight XDR with threat intel	mimecast	corelight	FORTINET
okta	CLOUDFLARE	netskope	Falcon Identity Protection	proofpoint.	ExtraHop	paloalto NETWORKS
Microsoft Azure /AD	MENLO SECURITY		Falcon Horizon & CWP	cisco Secure Email Gateway	VECTRA	cisco ASA and Secure Firewall
FORGEROCK			Falcon for Mobile	Microsoft 365 Defender for O365D	cisco Secure Analytics	
			Falcon Spotlight & Discover			

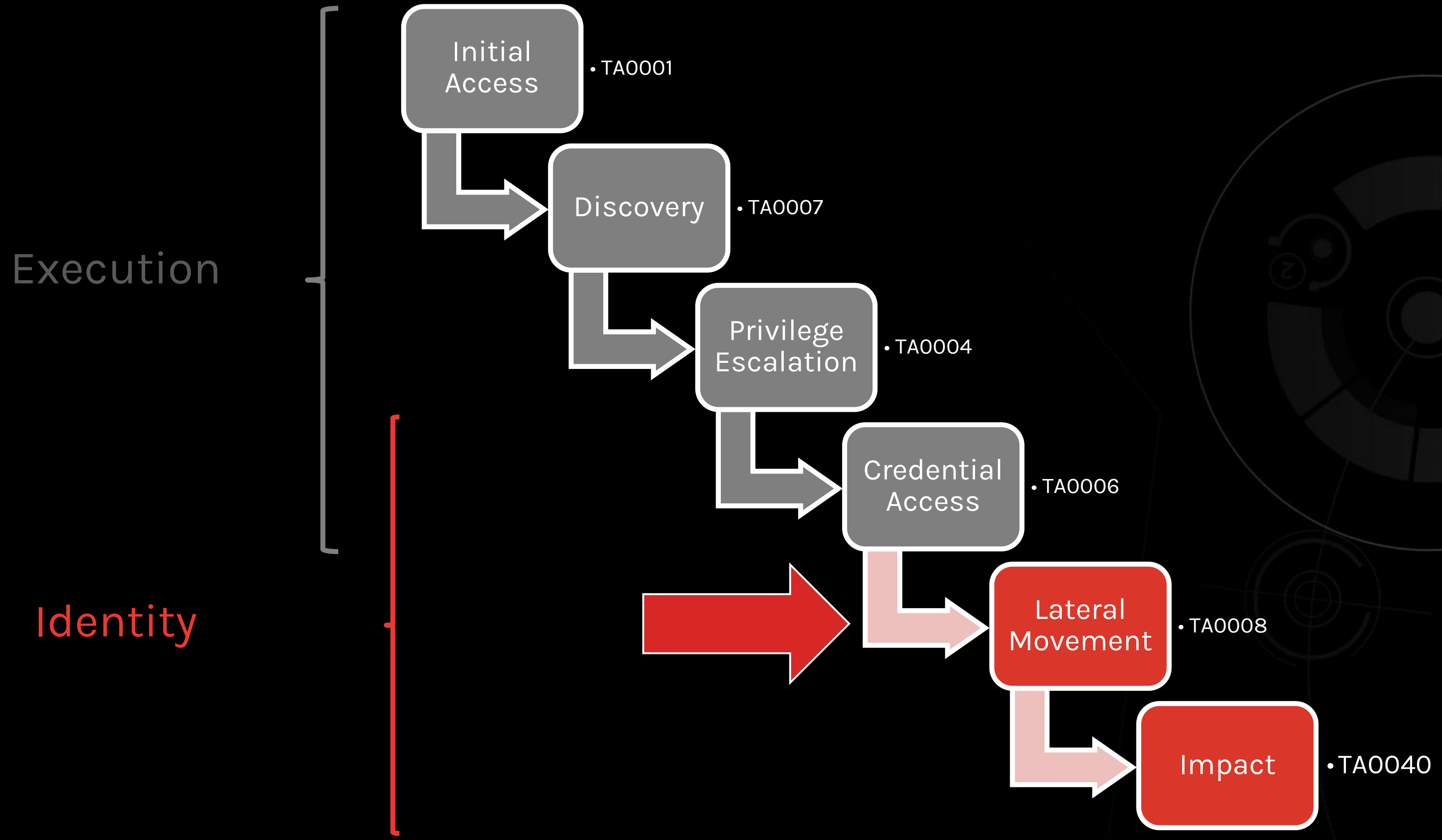
CROWDSTRIKE

SEHEN WIE EIN ANGREIFER – IDENTITIES

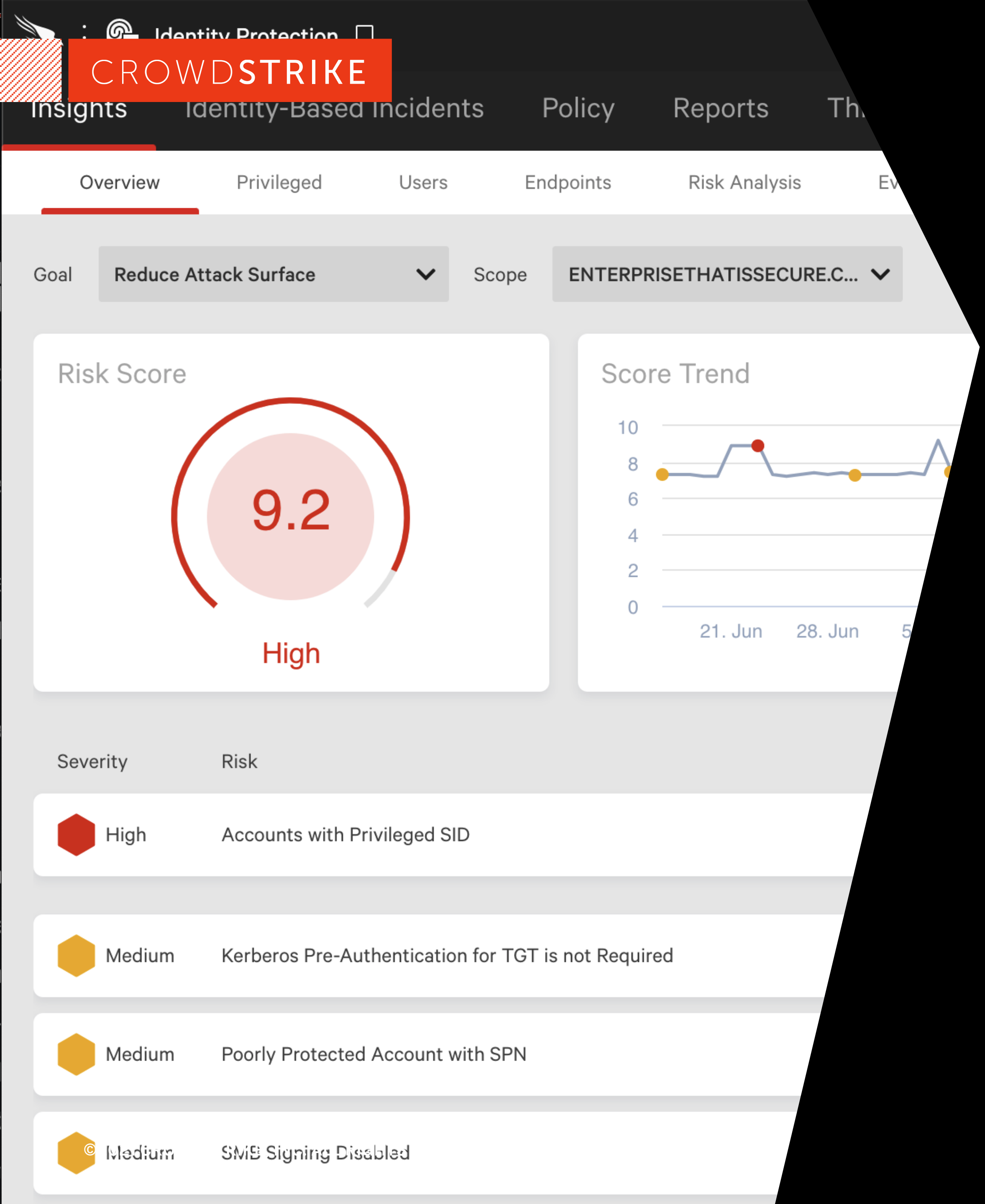
> “80% OF DATA BREACHES HAVE A CONNECTION TO COMPROMISED PRIVILEGED CREDENTIALS”
>
> - FORRESTER RESEARCH

CROWDSTRIKE

OFTEN, THEY ARE STARTING HERE



CROWDSTRIKE

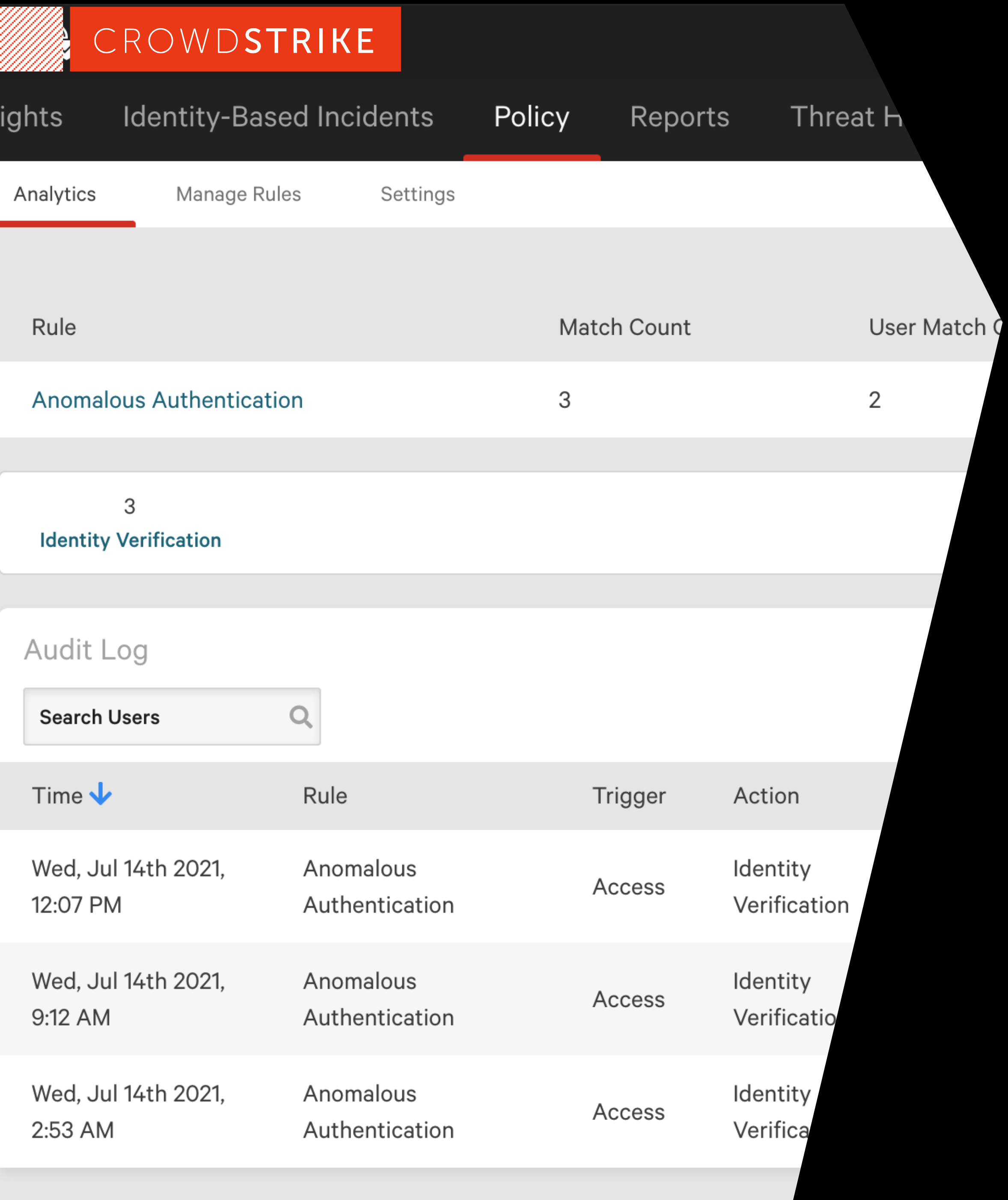


Goal: Reduce Attack Surface
Scope: ENTERPRISETHATISSECURE.C...

Severity	Risk
High	Accounts with Privileged SID
Medium	Kerberos Pre-Authentication for TGT is not Required
Medium	Poorly Protected Account with SPN
Medium	SMB Signing Disabled

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



Rule	Match Count	User Match C
Anomalous Authentication	3	2

3
Identity Verification

Audit Log

Time ↓	Rule	Trigger	Action
Wed, Jul 14th 2021, 12:07 PM	Anomalous Authentication	Access	Identity Verification
Wed, Jul 14th 2021, 9:12 AM	Anomalous Authentication	Access	Identity Verificatio
Wed, Jul 14th 2021, 2:53 AM	Anomalous Authentication	Access	Identity Verifica

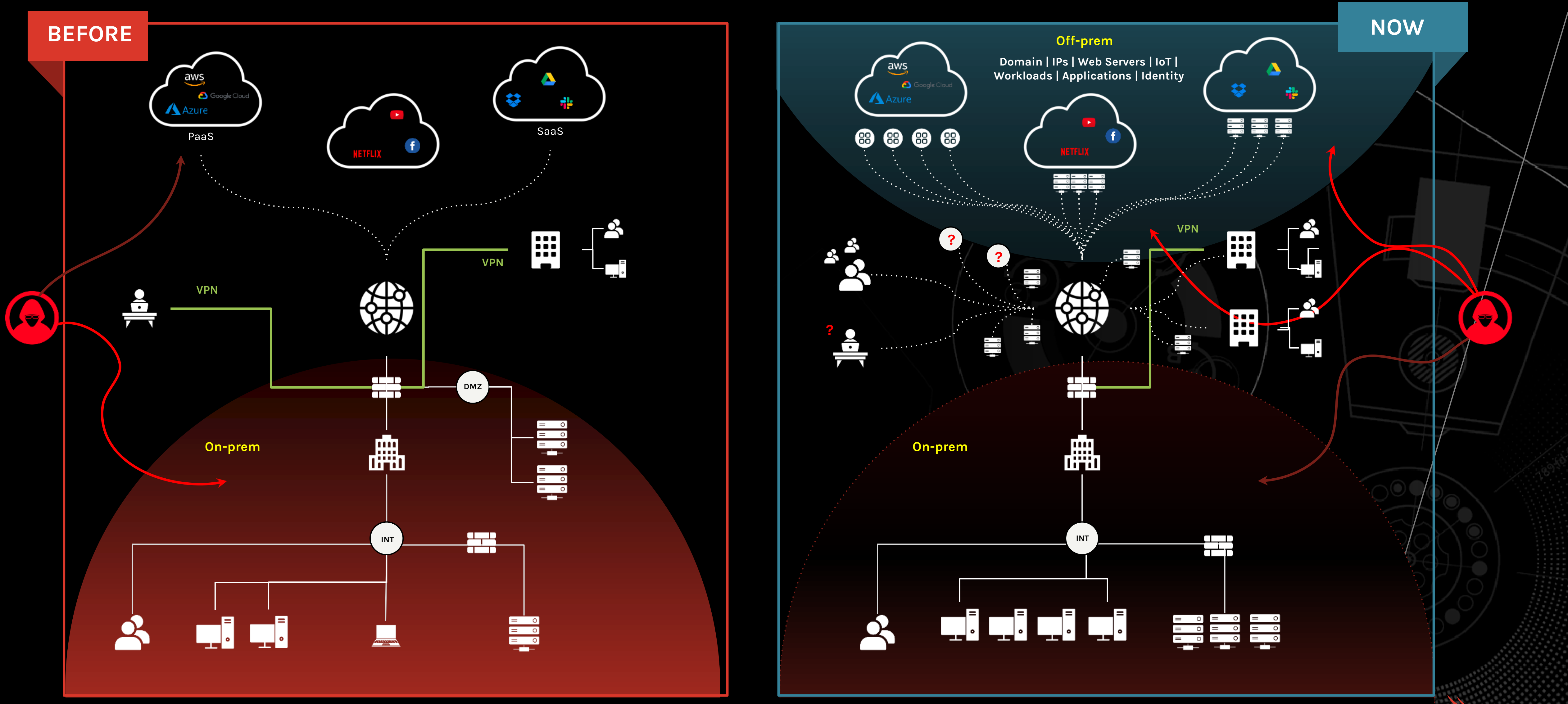
FALCON IDENTITY THREAT PROTECTION

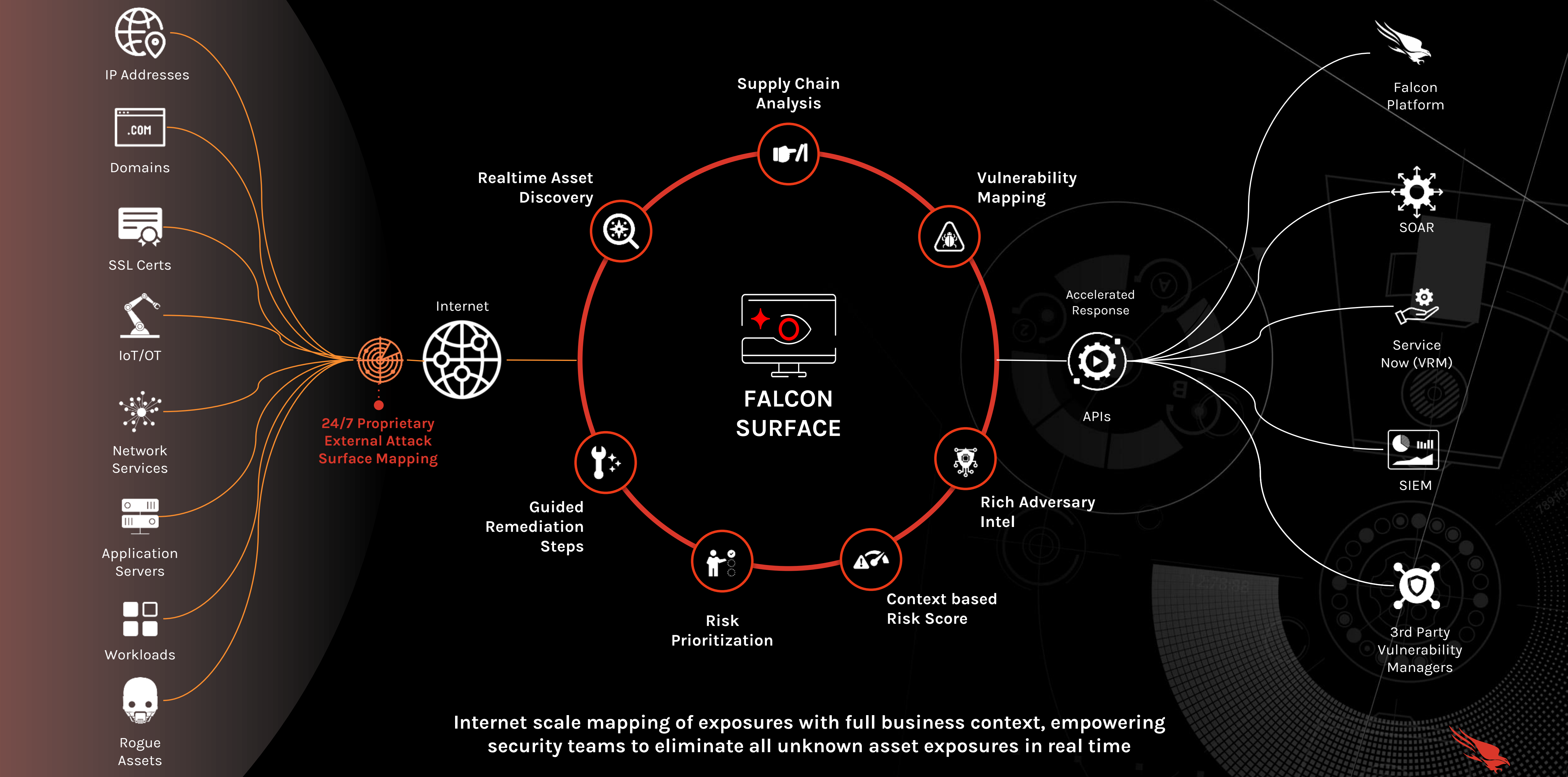
- Trust… and verify
- Automatically enforce conditional access on anomalous activity
- Create bespoke rules that allow, block, or challenge high-risk identity activity
- Integrate with current identity stores for a zero-friction end-user experience
- Stop adversaries in their tracks

SEHEN WIE EIN ANGREIFER – EXTERN

CROWDSTRIKE

Your digital footprint is becoming complex



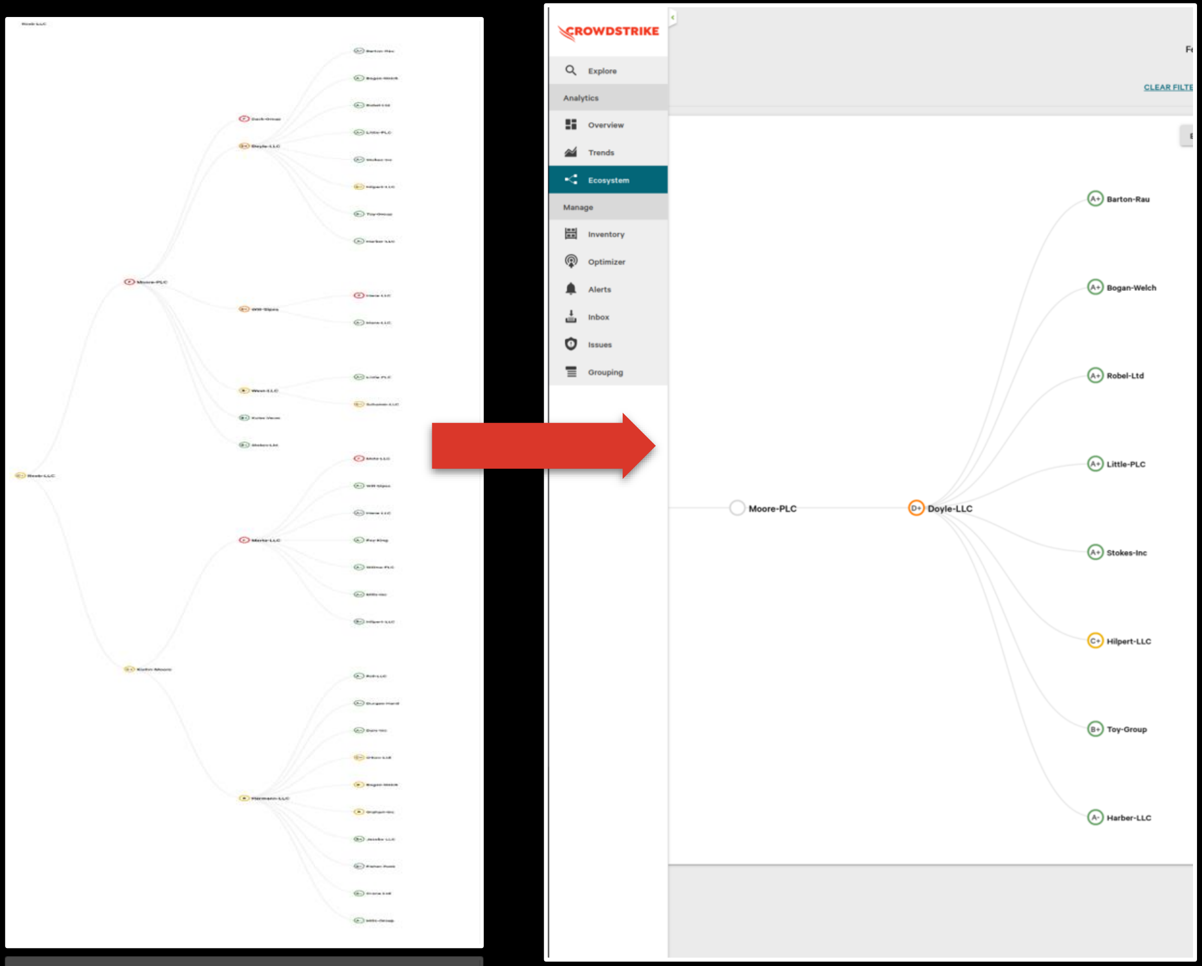


Internet scale mapping of exposures with full business context, empowering security teams to eliminate all unknown asset exposures in real time

CROWDSTRIKE USE CASE

ASSESS MERGERS AND ACQUISITIONS SOLUTION

GAIN COMPLETE VISIBILITY OF SHADOW IT AND UNKNOWN RISKS RELATING TO YOUR SUBSIDIARIES.

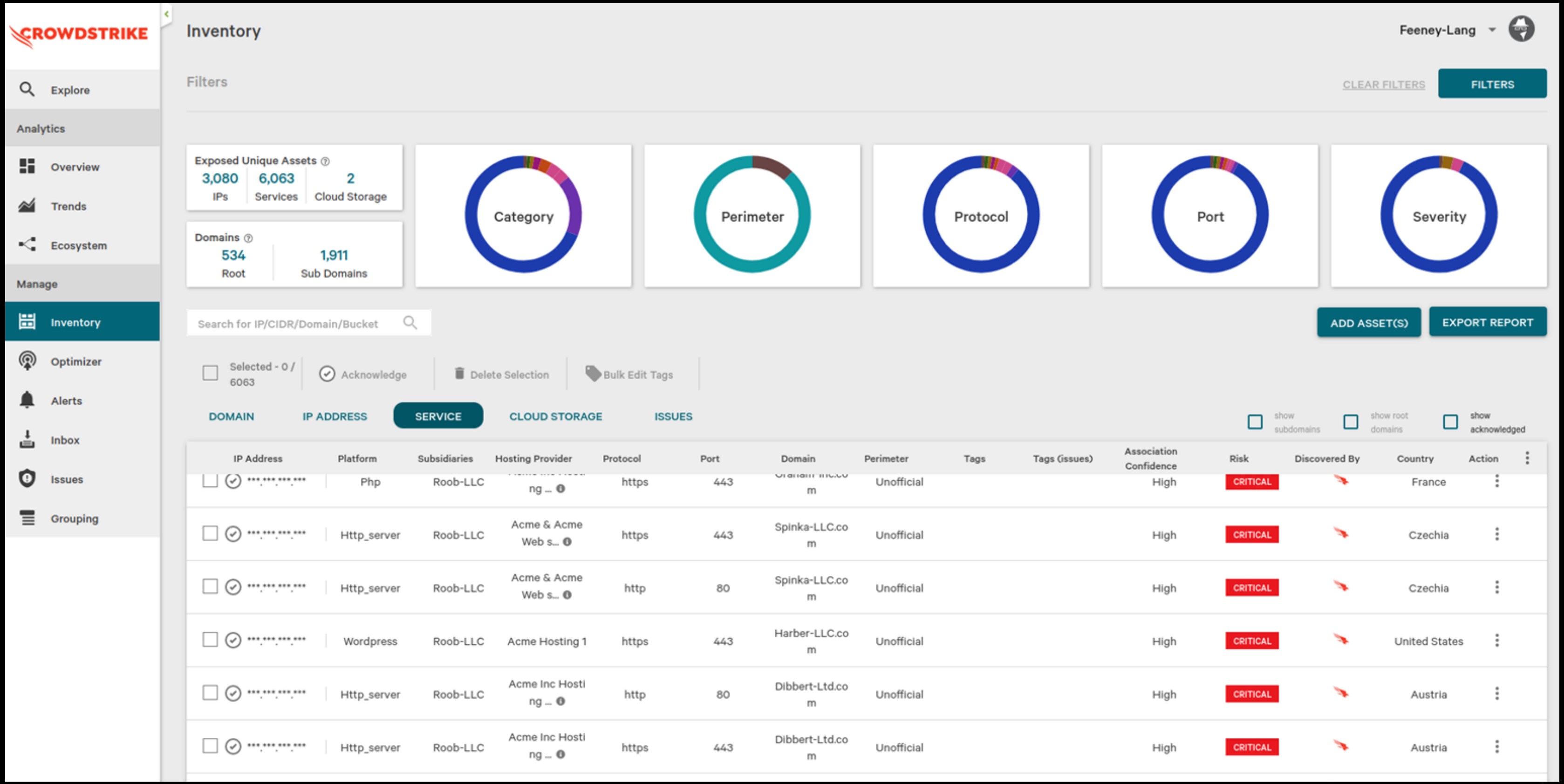


- Automate ecosystem mapping, no user input is needed
- Reveal your subsidiaries' unknown risks, see exactly how they affect your overall security posture.
- Resolve risks before they are exploited

CROWDSTRIKE USE CASE

CONTROL ASSET INVENTORY SOLUTION

FIND YOUR UNKNOWN EXPOSED ASSETS ACROSS THE ENTIRE INTERNET.



CROWDSTRIKE

- Explore
- Analytics
- Overview
- Trends
- Ecosystem
- Manage
- Inventory
- Optimizer
- Alerts
- Inbox
- Issues
- Grouping

Inventory

Feeney-Lang

Filters

CLEAR FILTERS FILTERS

Exposed Unique Assets: 3,080 IPs | 6,063 Services | 2 Cloud Storage

Domains: 534 Root | 1,911 Sub Domains

Search for IP/CIDR/Domain/Bucket

ADD ASSET(S) EXPORT REPORT

□ Selected - 0 / 6063 | Acknowledge | Delete Selection | Bulk Edit Tags

DOMAIN | IP ADDRESS | SERVICE | CLOUD STORAGE | ISSUES

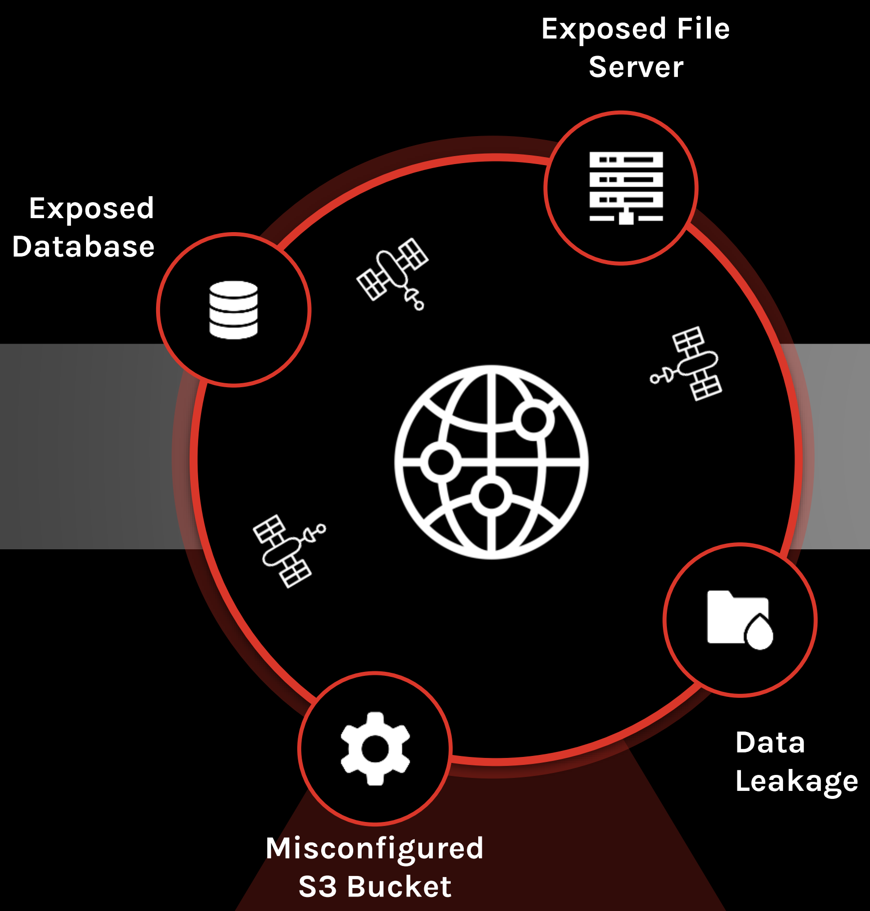
□ show subdomains □ show root domains □ show acknowledged

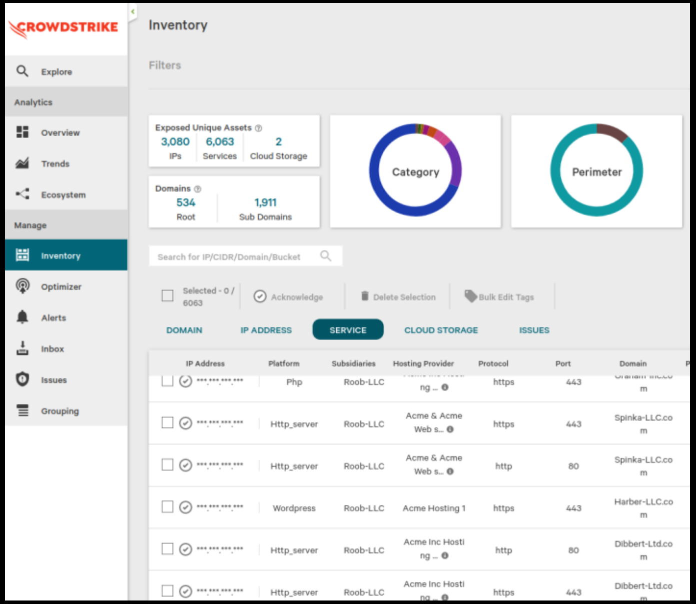
IP Address	Platform	Subsidiaries	Hosting Provider	Protocol	Port	Domain	Perimeter	Tags	Tags (issues)	Association Confidence	Risk	Discovered By	Country	Action
□ ✓ ***.***.***.***	Php	Roob-LLC	Acme Inc Hosting ...	https	443	Graham-Inc.com	Unofficial			High	CRITICAL		France	⋮
□ ✓ ***.***.***.***	Http_server	Roob-LLC	Acme & Acme Web s...	https	443	Spinka-LLC.com	Unofficial			High	CRITICAL		Czechia	⋮
□ ✓ ***.***.***.***	Http_server	Roob-LLC	Acme & Acme Web s...	http	80	Spinka-LLC.com	Unofficial			High	CRITICAL		Czechia	⋮
□ ✓ ***.***.***.***	Wordpress	Roob-LLC	Acme Hosting 1	https	443	Harber-LLC.com	Unofficial			High	CRITICAL		United States	⋮
□ ✓ ***.***.***.***	Http_server	Roob-LLC	Acme Inc Hosting ...	http	80	Dibbert-Ltd.com	Unofficial			High	CRITICAL		Austria	⋮
□ ✓ ***.***.***.***	Http_server	Roob-LLC	Acme Inc Hosting ...	https	443	Dibbert-Ltd.com	Unofficial			High	CRITICAL		Austria	⋮

- Maintain an overarching view of your entire attack surface
- Stay on top of asset inventory changes in real-time
- Utilize our multi-location & adaptive indexing techniques for fresh & accurate data

CROWDSTRIKE

FALCON SURFACE MAPS THE WORLD'S INTERNET EXPOSURES IN REAL-TIME





Inventory

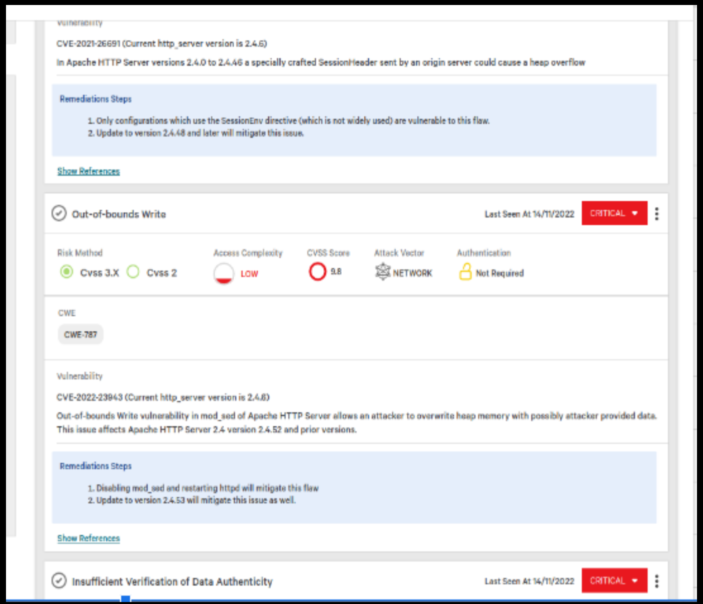
Filters

Exposed Unique Assets: 3,080 IPs | 6,063 Services | 2 Cloud Storage

Domains: 534 Root | 1,911 Sub Domains

☐ Selected - 0 / 6063

	IP Address	Platform	Subsidiaries	Hosting Provider	Protocol	Port	Domain
☐	***.***.***.***	Php	Roob-LLC	Acme Inc Hosting ...	https	443	Graham-Inc.com
☐	***.***.***.***	Http_server	Roob-LLC	Acme & Acme Web s...	https	443	Spinka-LLC.com
☐	***.***.***.***	Http_server	Roob-LLC	Acme & Acme Web s...	http	80	Spinka-LLC.com
☐	***.***.***.***	Wordpress	Roob-LLC	Acme Hosting 1	https	443	Harber-LLC.com
☐	***.***.***.***	Http_server	Roob-LLC	Acme Inc Hosting ...	http	80	Dibbert-Ltd.com
☐	***.***.***.***	Http_server	Roob-LLC	Acme Inc Hosting ...	https	443	Dibbert-Ltd.com



Vulnerability

CVE-2021-26691 (Current http_server version is 2.4.6)

In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

Remediations Steps

1. Only configurations which use the SessionEnv directive (which is not widely used) are vulnerable to this flaw.
2. Update to version 2.4.48 and later will mitigate this issue.

Out-of-bounds Write — Last Seen At 14/11/2022 — CRITICAL

Risk Method: ● Cvss 3.X ○ Cvss 2

Access Complexity: LOW

CVSS Score: 9.8

Attack Vector: NETWORK

Authentication: Not Required

CWE: CWE-787

Vulnerability

CVE-2022-23943 (Current http_server version is 2.4.8)

Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

Remediations Steps

1. Disabling mod_sed and restarting httpd will mitigate this flaw
2. Update to version 2.4.53 will mitigate this issue as well.

Insufficient Verification of Data Authenticity — Last Seen At 14/11/2022 — CRITICAL

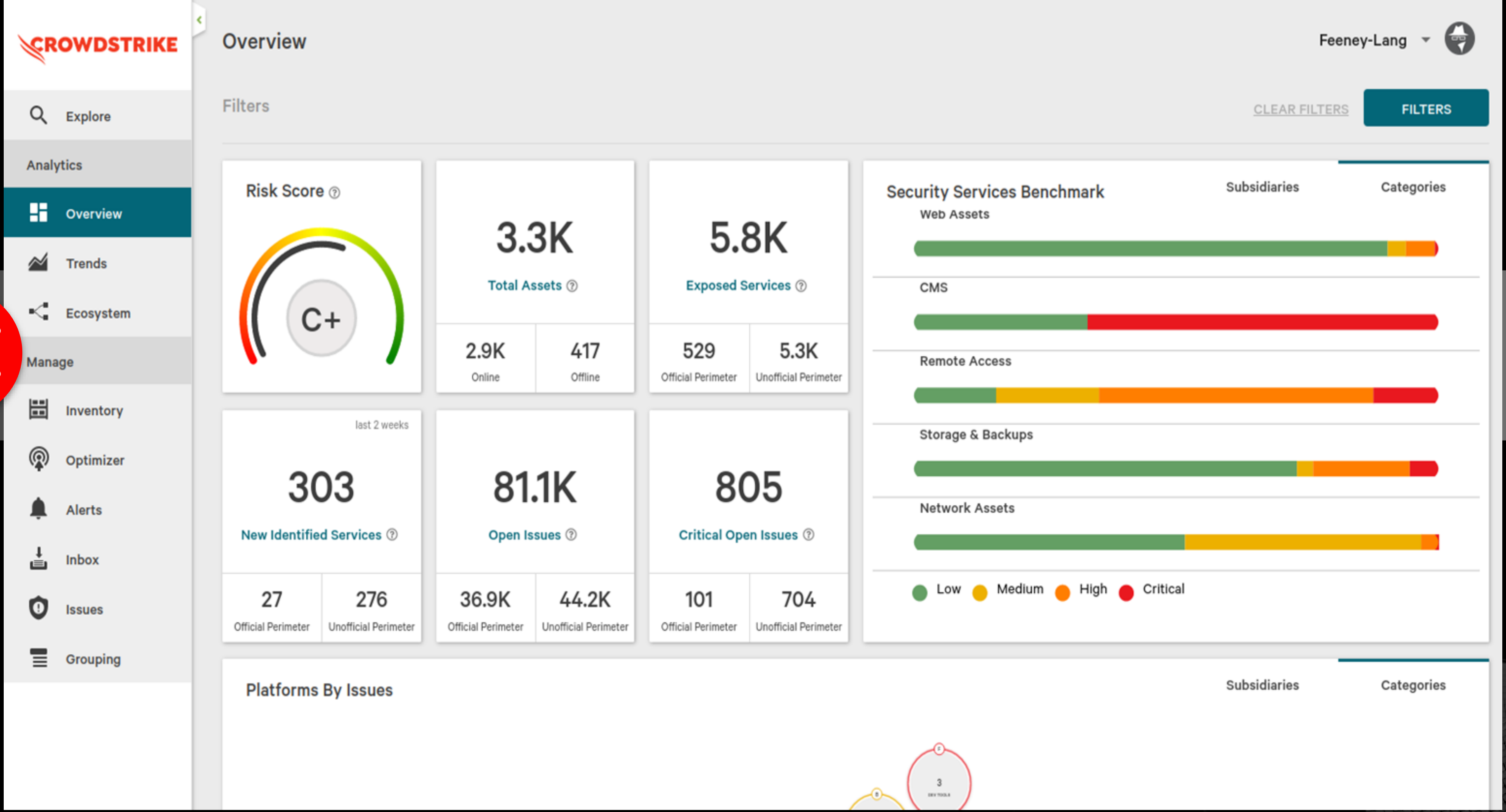
1 Scan the entire internet for exposed assets

2 Create exposed asset inventory and analyze security posture

3 Prioritize risk and generate guided remediation steps

CROWDSTRIKE

Do you know your external attack surface?



FALCON SURFACE

BOOK YOUR DEMO TODAY

MANAGED DETECTION & RESPONSE (MDR)

CROWDSTRIKE FALCON COMPLETE XDR

EXPERTS IN FALCON PLATFORM

Certified analysts, 100% focused on stopping breaches

EXPERTS IN INCIDENT RESPONSE

Years of DFIR experience, PIONEERED remote remediation as a core competency

ALWAYS IMPROVING

Every day building countermeasures to respond to the latest threats the moment they emerge

MISSION:

Manage, monitor, and remediate threats 24/7/365

CROWDSTRIKE

A PROVEN SECURITY LEADER

Leader In

Gartner • FORRESTER • IDC

Validated

MITRE • AV comparatives • SE Labs

Compliance & Certifications

Privacy Shield Framework · FedRAMP · PCI · aws competency · MEMBER amtso · FIEC · CYBER ESSENTIALS CERTIFIED · CCN · STAR LEVEL TWO · CREST

THANK YOU