Softcat

Secure by design – Data resilience and recovery

Softcat Summit 2026

Speakers

Ryan Birch

Cyber Tower Sales Lead,
Softcat

James Smare

Proposition Owner
Softcat

Kev Johnson

Staff Technical Marketing Manager
Rubrik

John Spencer

Sales Engineering Director, Northern Europe
CrowdStrike

Key pillars of resilience & continuity

AI impact on operational resilience

Operational resilience concept		AI context
Important business services	→	AI-enabled services (decision making, analytics, automation)
Impact tolerances	→	Maximum acceptable model downtime, accuracy loss, or decision delay
Mapping	→	Data pipelines, feature stores, models, APIs, cloud platforms, identities
Severe but plausible scenarios	→	Data poisoning, ransomware, cloud region loss, identity compromise
Response & recovery	→	Restore clean data, models, pipelines and access within tolerance

Identity


Identity
User
Access management
Intrusion detection
Data

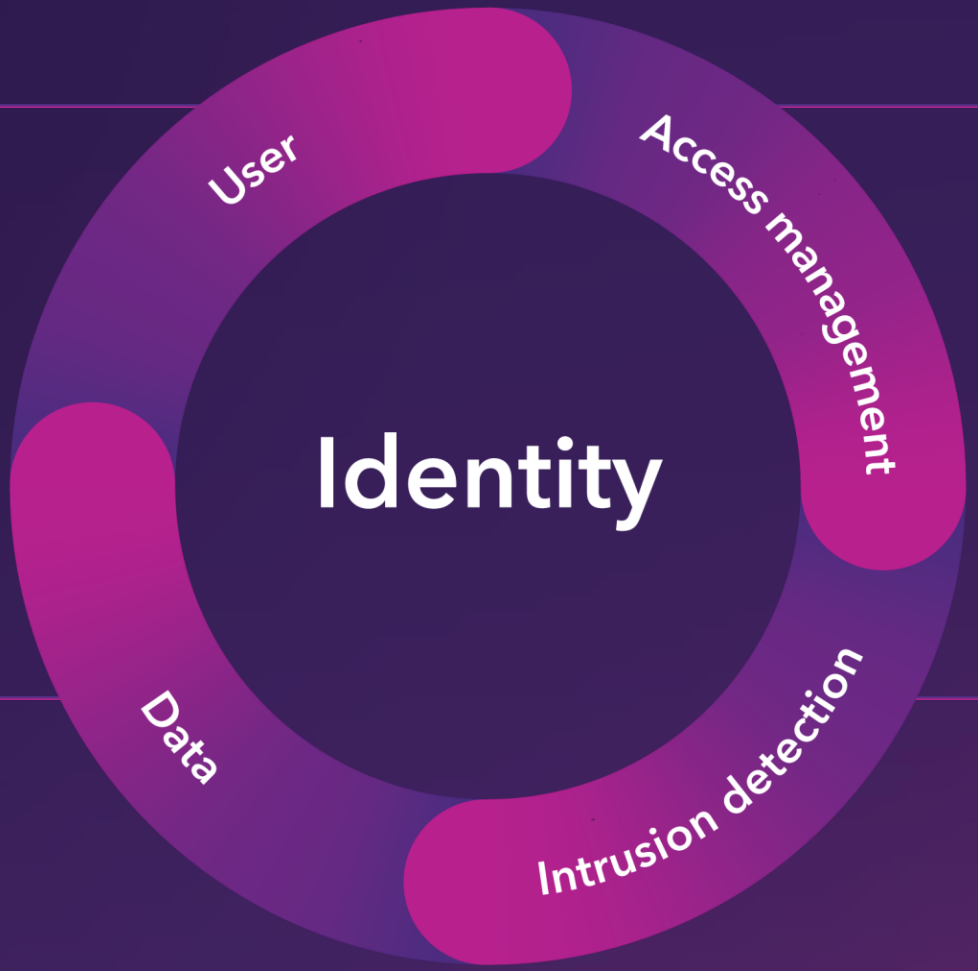
Identity

- Non Human Identities set to be between 50 and 100:1 ratio by end of 2030
- 68% of cyber incidents in UK in 2025 involved a machine identity

Pain points

"How am I able to get an understanding of the risk to my identities?"

"How am I able to manage what my identities are able to access?"



"How am I able to get visibility of data movement and who has access?"

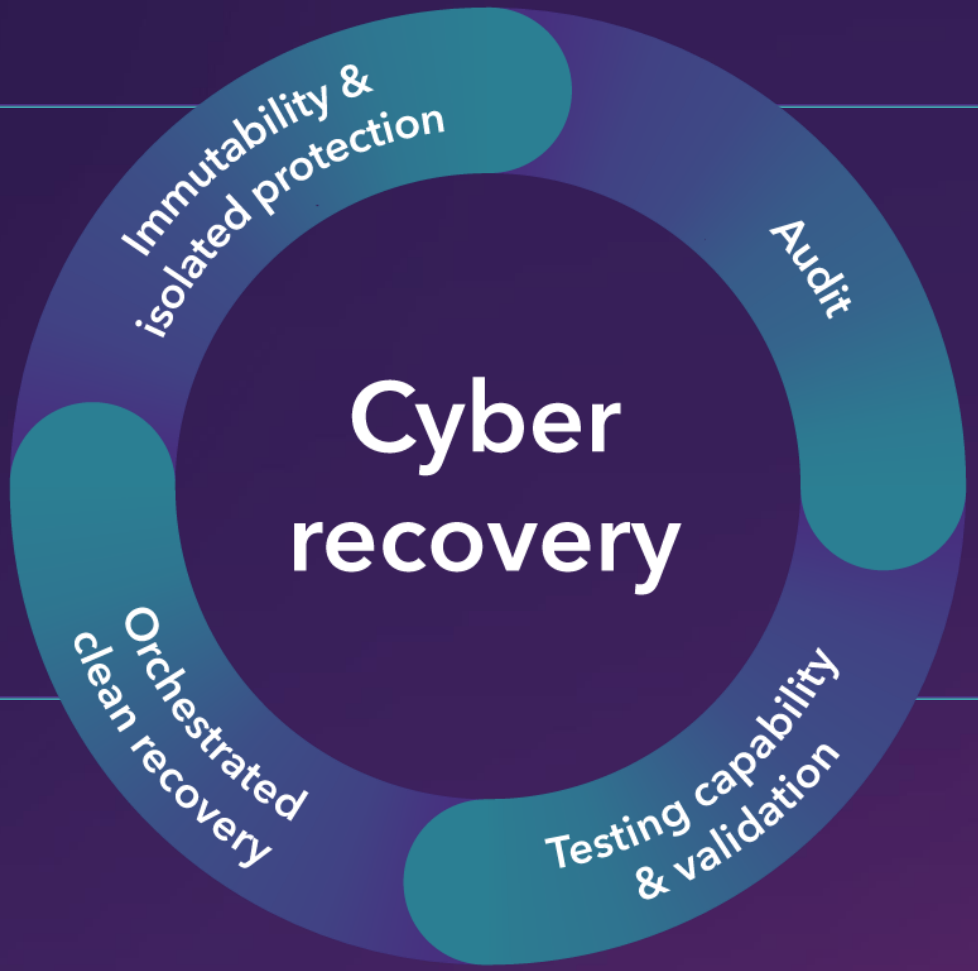
"How am I able to detect if an identity has been compromised?"

Cyber recovery

Pain points

"If attackers can alter or delete my backups, I have nothing to recover from."

"I don't know what's been hit or how far the attack spread."



"Even if I can recover, how do I do it quickly and without reintroducing malware?"

"We think we can recover, but we've never proven it under fire."

softcat

CrowdStrike: John Spencer

Sales Engineering Director, Northern Europe

CROWDSTRIKE

ADVERSARY DETECTION & RESPONSE

SCATTERED SPIDER

The problem

Ransomware detection/prevention by CrowdStrike

Compromised employee credentials

Persistence via new user account creation with elevated privileges

Detection & Response

[1] Investigation of detection, AI triage
Process table and tree

[2] Identity Investigation – who was the source?
New account creation?

[3] Real-Time Response
Host Containment
Credential / MFA Reset

DETECTION ALERT

Activity dashboard | Endpoint

falcon.crowdstrike.com/dashboards-v2/dashboard/9D5413A9-50CB-4242-8DE4-F32C23534A3B

Endpoint security | Activity dashboard | Search | Charlotte AI

Current CrowdScore

Today

0 / 100

Last refreshed: 15:52:20

New detections

1,715

Last refreshed: 15:53:17

SHA-based detections

ff79d3c4a0b7eb191783c323ab8363ebd1fd10be58d8bcc96b07067743ca81d5	532
4b8d3d6e379d70ccdc7afefb5da7eee7583f6f1405c98c8a452fb17490f4ba7c	402
9f914d42706fe215501044acd85a32d58aaef1419d404fddfa5d3b48f66ccd9f	306
761815301a00d0b3a7bb4959a5004b623c55009ce701c6e867c96f468dc1323a	150
Total	1,747

Last refreshed: 15:53:16

Prevented malware by host

Last 7 days

DIAL-BEE-USR1	42
DIAL-BEE-USR2	14
Total	56

Last refreshed: 15:53:16

CrowdScore over time

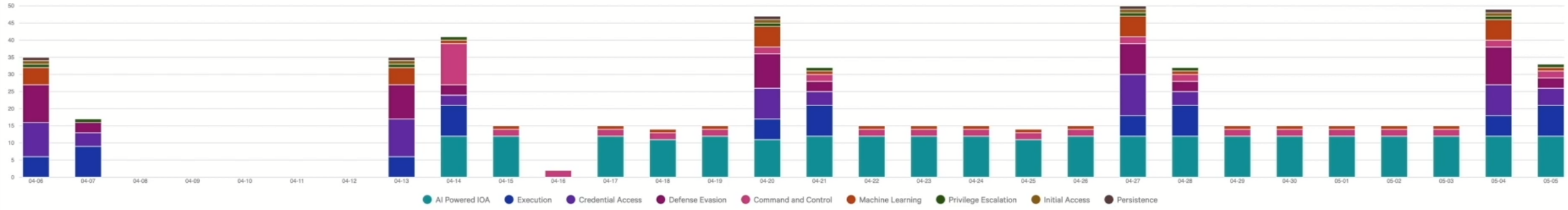
Last refreshed: 15:52:21

Most recent detections

Severity	Tactic & Technique	Time	Host ID	Link
High	AI Powered IOA via Malicious File	May 6, 2026 00:39:24	DIAL-BEE-USR1	See detection
High	AI Powered IOA via User Execution	May 6, 2026 00:39:17	DIAL-BEE-USR1	See detection
High	AI Powered IOA via Malicious File	May 6, 2026 00:38:54	DIAL-BEE-USR1	See detection
High	AI Powered IOA via User Execution	May 6, 2026 00:38:47	DIAL-BEE-USR1	See detection
High	AI Powered IOA via Malicious File	May 6, 2026 00:38:34	DIAL-BEE-USR1	See detection
High	AI Powered IOA via User Execution	May 6, 2026 00:38:27	DIAL-BEE-USR1	See detection

Last refreshed: 15:53:15

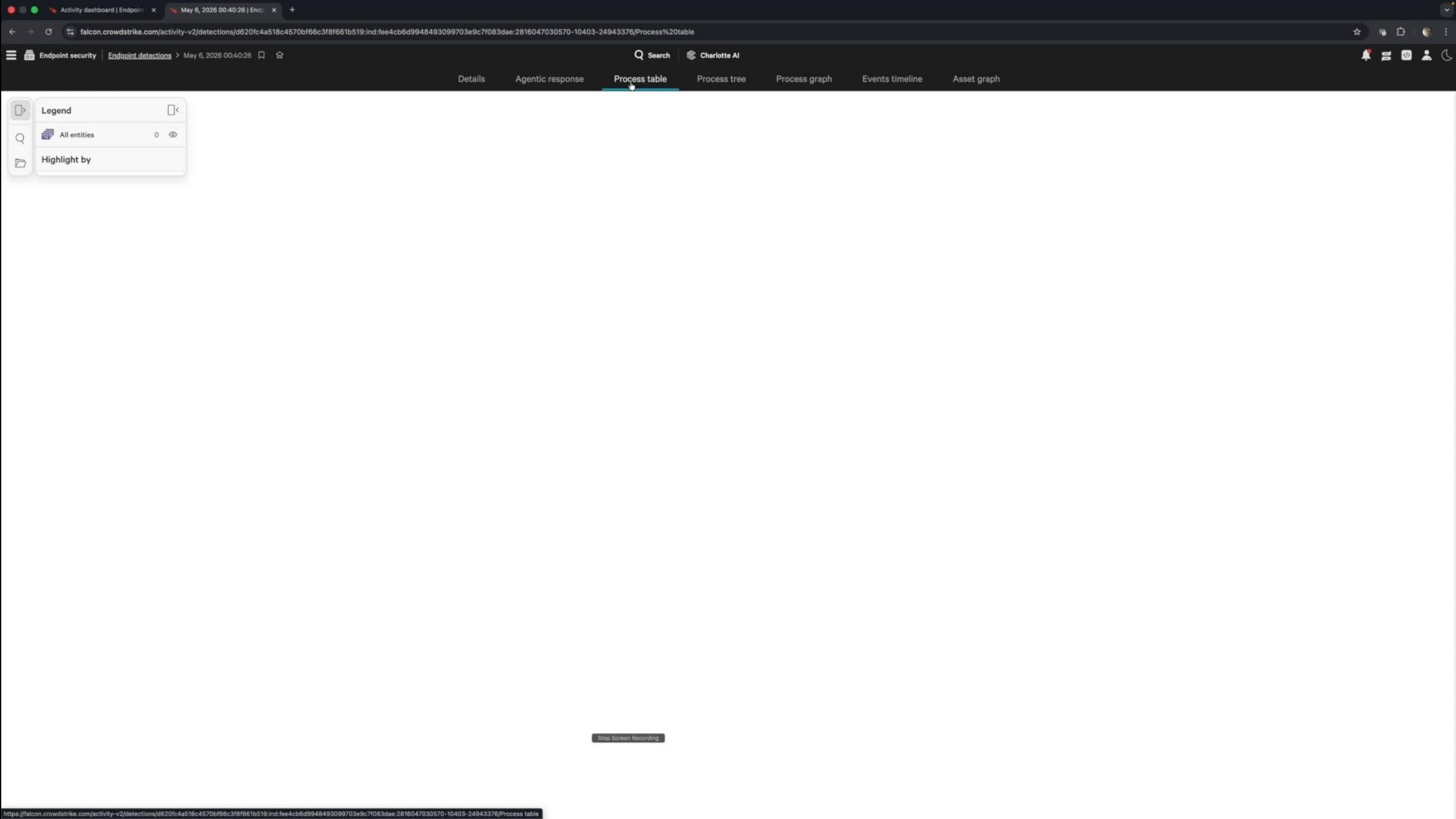
Detections by tactics



Last refreshed: 15:53:15

Stop Screen Recording

INVESTIGATION


Activity dashboard | Endpoint
May 6, 2026 00:40:26 | Endp
falcon.crowdstrike.com/activity-v2/detections/d620fc4a518c4570bf66c3f8f661b519:ind:fee4cb6d9948493099703e9c7f083dae:2816047030570-10403-24943376/Process%20table
Endpoint security
Endpoint detections
May 6, 2026 00:40:26
Search
Charlotte AI
Details
Agentic response
Process table
Process tree
Process graph
Events timeline
Asset graph
Legend
All entities
0
Highlight by
Stop Screen Recording
https://falcon.crowdstrike.com/activity-v2/detections/d620fc4a518c4570bf66c3f8f661b519:ind:fee4cb6d9948493099703e9c7f083dae:2816047030570-10403-24943376/Process table

IDENTITY

Activity dashboard | Endpoint | Hosts | Investigate | Falcon | hi.exe | Sandbox | Counter Ac | SCATTERED SPIDER | Adver

falcon.crowdstrike.com/investigate/host?searchType=aid&searchValue=fee4cb6d9948493099703e9c7f083dae&timeRange=lastWeek

Investigate | Hosts

Search | Charlotte AI

Bookmarks

Recently visited

Charlotte AI

Next-Gen SIEM

Endpoint security

Cloud security

SaaS security

Identity protection

Exposure management

Counter Adversary Operations

Investigate

Fusion SOAR

Foundry

Asset inventory

Dashboards and reports

Host setup and management

CrowdStrike Store

Audit logs

Support and resources

Connectors

Investigate

Search

- Advanced event search
- Event search
- Scheduled search
- Hosts Updated
- Users Updated
- Hash search Updated
- IP addresses Updated
- Bulk domains Updated
- Search by agent ID New
- Search by IP address New
- Search by process context New
- Data settings New

Hunt

- Linux sensors
- Mac sensors
- Detection activity
- Detection resolutions
- Detections details New
- Detections event summary New
- MITRE ATT&CK evaluation New
- Indicator activity
- Command line and ASEP activity
- Executables running from Recycle Bin
- Executables running from temp directories
- Files written to removable media - windows
- Files written to removable media - mac
- Windows account discovery New
- Windows user logon activity New
- Firewall set rules
- Powershell hunt
- Scheduled tasks registered

Timelines

- Hosts Updated
- Processes Updated

BIOS

Host: fee4cb6d9948493099703e9c7f083dae

1 host(s) found.

Company: All

Time range: Last week

Apply

	and admin tools (Windows)	Suspicious file activity	Registry, tasks and firewall	Networking				
	8EE-USR1	DIAL-BEE-UN1	2026-04-29T16:09:26+01:00	2026-05-06T15:39:13+01:00	--	172.17.0.50/24	06-BC-D4-B1-F5-F5	

Page 1 of 1

View in Advanced event search | Export

	Log on type	Log on time	Log off time	Duration
	Network	2026-05-05T23:38:16Z	2026-05-05T23:38:37Z	21s
	Interactive	2026-05-05T23:38:16Z	--	--
	Network	2026-05-04T23:38:14Z	2026-05-04T23:38:35Z	22s
	Interactive	2026-05-04T23:38:14Z	--	--
	Network	2026-05-03T23:43:32Z	2026-05-03T23:43:54Z	22s
	Interactive	2026-05-03T23:43:32Z	--	--
	Network	2026-05-02T23:43:32Z	2026-05-02T23:43:53Z	22s
	Interactive	2026-05-02T23:43:32Z	--	--
	Network	2026-05-01T23:42:44Z	2026-05-01T23:43:06Z	21s
	Interactive	2026-05-01T23:42:45Z	--	--
	Network	2026-04-30T23:43:09Z	2026-04-30T23:43:31Z	22s
	Interactive	2026-04-30T23:43:10Z	--	--
	Network	2026-04-29T23:39:45Z	2026-04-29T23:40:07Z	21s
	Interactive	2026-04-29T23:39:46Z	--	--

Page 1 of 1

Unique ASEP values updated

17

Stop Screen Recording

Unique browser injected threads

0

Unique DLL injections

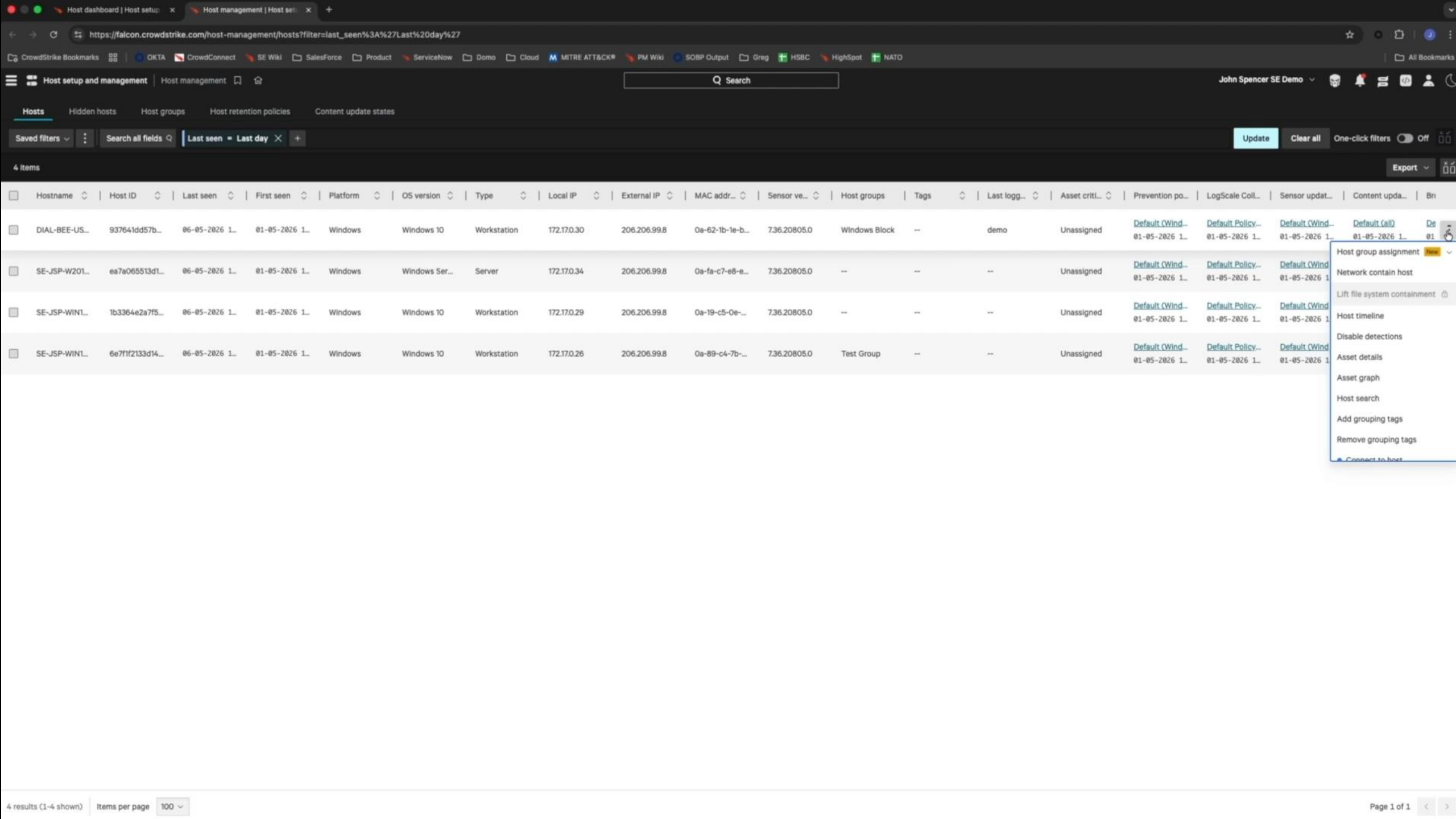
0

Java injected threads

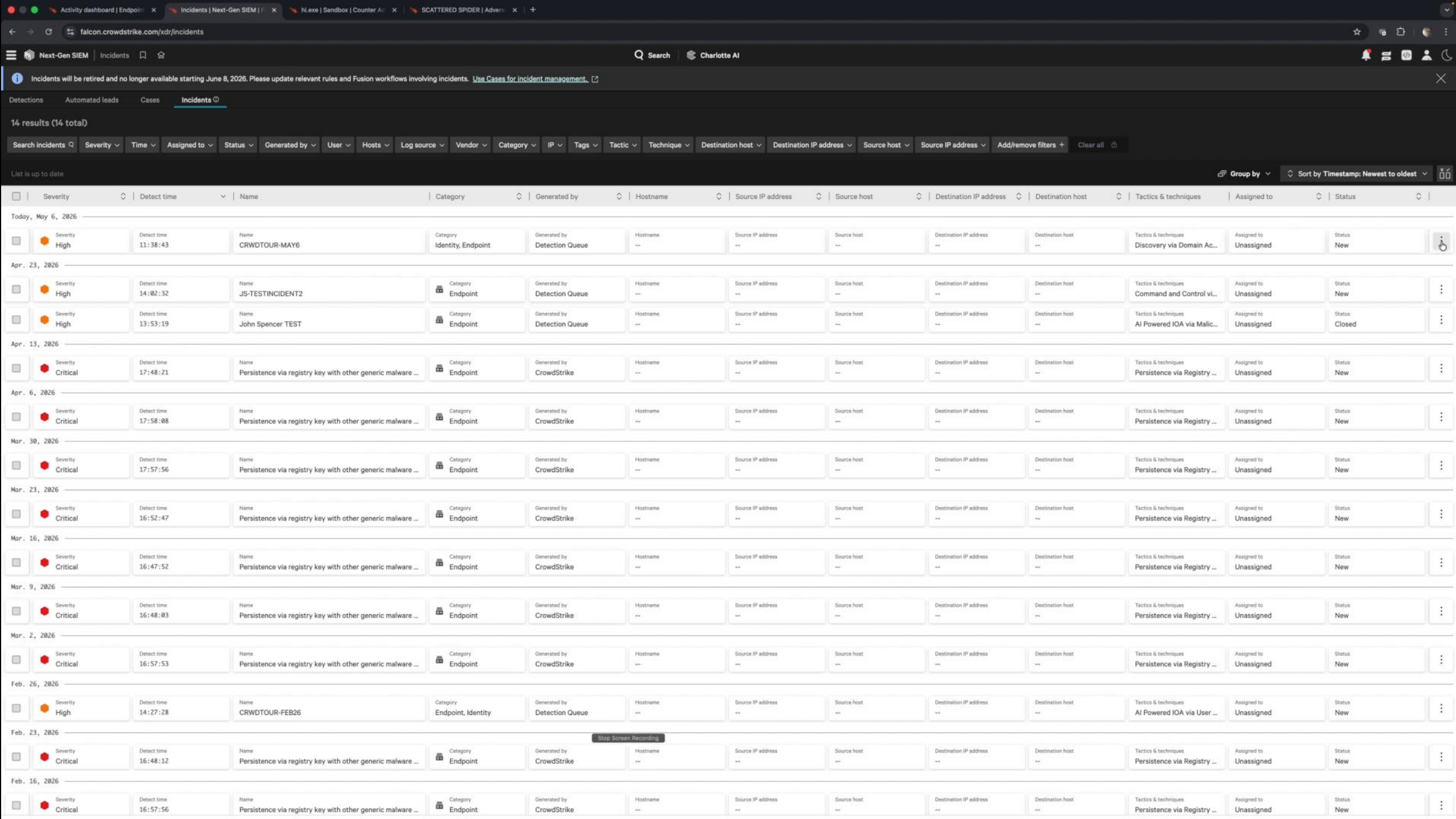
Unique executables written

Injected thread from unsigned modules

REAL TIME RESPONSE


Host dashboard | Host setup
Host management | Host set
https://falcon.crowdstrike.com/host-management/hosts?filter=last_seen%3A%27Last%20day%27
CrowdStrike Bookmarks
OKTA
CrowdConnect
SE Wiki
SalesForce
Product
ServiceNow
Domo
Cloud
MITRE ATT&CK®
PM Wiki
SOBP Output
Greg
HSBC
HighSpot
NATO
All Bookmarks
Host setup and management
Host management
Search
John Spencer SE Demo
Hosts
Hidden hosts
Host groups
Host retention policies
Content update states
Saved filters
Search all fields
Last seen = Last day
Update
Clear all
One-click filters
Off
4 items
Export
Hostname
Host ID
Last seen
First seen
Platform
OS version
Type
Local IP
External IP
MAC addr...
Sensor ve...
Host groups
Tags
Last logg...
Asset criti...
Prevention po...
LogScale Coll...
Sensor updat...
Content upda...
DIAL-BEE-US...
937641dd57b...
06-05-2026 1...
01-05-2026 1...
Windows
Windows 10
Workstation
172.17.0.30
206.206.99.8
0a-62-1b-1e-b...
7.36.20805.0
Windows Block
--
demo
Unassigned
Default (Wind...
01-05-2026 1...
Default Policy...
01-05-2026 1...
Default (Wind...
01-05-2026 1...
Default (all)
01-05-2026 1...
SE-JSP-W201...
ea7a065513d1...
06-05-2026 1...
01-05-2026 1...
Windows
Windows Ser...
Server
172.17.0.34
206.206.99.8
0a-fa-c7-e8-e...
7.36.20805.0
--
--
--
Unassigned
Default (Wind...
01-05-2026 1...
Default Policy...
01-05-2026 1...
Default (Wind
01-05-2026 1
SE-JSP-WIN1...
1b3364e2a7f5...
06-05-2026 1...
01-05-2026 1...
Windows
Windows 10
Workstation
172.17.0.29
206.206.99.8
0a-19-c5-0e-...
7.36.20805.0
--
--
--
Unassigned
Default (Wind...
01-05-2026 1...
Default Policy...
01-05-2026 1...
Default (Wind
01-05-2026 1
SE-JSP-WIN1...
6e7f1f2133d14...
06-05-2026 1...
01-05-2026 1...
Windows
Windows 10
Workstation
172.17.0.26
206.206.99.8
0a-89-c4-7b-...
7.36.20805.0
Test Group
--
--
Unassigned
Default (Wind...
01-05-2026 1...
Default Policy...
01-05-2026 1...
Default (Wind
01-05-2026 1
Host group assignment
New
Network contain host
Lift file system containment
Host timeline
Disable detections
Asset details
Asset graph
Host search
Add grouping tags
Remove grouping tags
4 results (1-4 shown)
Items per page
100
Page 1 of 1

INVESTIGATION WORKBENCH


Activity dashboard | Endpoint
Incidents | Next-Gen SIEM
hi.exe | Sandbox | Counter Ac
SCATTERED SPIDER | Adver
falcon.crowdstrike.com/xdr/incidents
Next-Gen SIEM
Incidents
Search
Charlotte AI
Incidents will be retired and no longer available starting June 8, 2026. Please update relevant rules and Fusion workflows involving incidents. Use Cases for incident management.
Detections
Automated leads
Cases
Incidents
14 results (14 total)
Search incidents
Severity
Time
Assigned to
Status
Generated by
User
Hosts
Log source
Vendor
Category
IP
Tags
Tactic
Technique
Destination host
Destination IP address
Source host
Source IP address
Add/remove filters
Clear all
List is up to date
Group by
Sort by Timestamp: Newest to oldest
Severity
Detect time
Name
Category
Generated by
Hostname
Source IP address
Source host
Destination IP address
Destination host
Tactics & techniques
Assigned to
Status
Today, May 6, 2026
High
11:38:43
CRWDTOUR-MAY6
Identity, Endpoint
Detection Queue
Discovery via Domain Ac...
Unassigned
New
Apr. 23, 2026
High
14:02:32
JS-TESTINCIDENT2
Endpoint
Detection Queue
Command and Control vi...
Unassigned
New
High
13:53:19
John Spencer TEST
Endpoint
Detection Queue
AI Powered IOA via Malic...
Unassigned
Closed
Apr. 13, 2026
Critical
17:48:21
Persistence via registry key with other generic malware ...
Endpoint
CrowdStrike
Persistence via Registry ...
Unassigned
New
Apr. 6, 2026
Critical
17:58:08
Persistence via registry key with other generic malware ...
Endpoint
CrowdStrike
Persistence via Registry ...
Unassigned
New
Mar. 30, 2026
Critical
17:57:56
Persistence via registry key with other generic malware ...
Endpoint
CrowdStrike
Persistence via Registry ...
Unassigned
New
Mar. 23, 2026
Critical
16:52:47
Persistence via registry key with other generic malware ...
Endpoint
CrowdStrike
Persistence via Registry ...
Unassigned
New
Mar. 16, 2026
Critical
16:47:52
Persistence via registry key with other generic malware ...
Endpoint
CrowdStrike
Persistence via Registry ...
Unassigned
New
Mar. 9, 2026
Critical
16:48:03
Persistence via registry key with other generic malware ...
Endpoint
CrowdStrike
Persistence via Registry ...
Unassigned
New
Mar. 2, 2026
Critical
16:57:53
Persistence via registry key with other generic malware ...
Endpoint
CrowdStrike
Persistence via Registry ...
Unassigned
New
Feb. 26, 2026
High
14:27:28
CRWDTOUR-FEB26
Endpoint, Identity
Detection Queue
AI Powered IOA via User ...
Unassigned
New
Feb. 23, 2026
Stop Screen Recording
Critical
16:48:12
Persistence via registry key with other generic malware ...
Endpoint
CrowdStrike
Persistence via Registry ...
Unassigned
New
Feb. 16, 2026
Critical
16:57:56
Persistence via registry key with other generic malware ...
Endpoint
CrowdStrike
Persistence via Registry ...
Unassigned
New

RECOVERY?

softcat

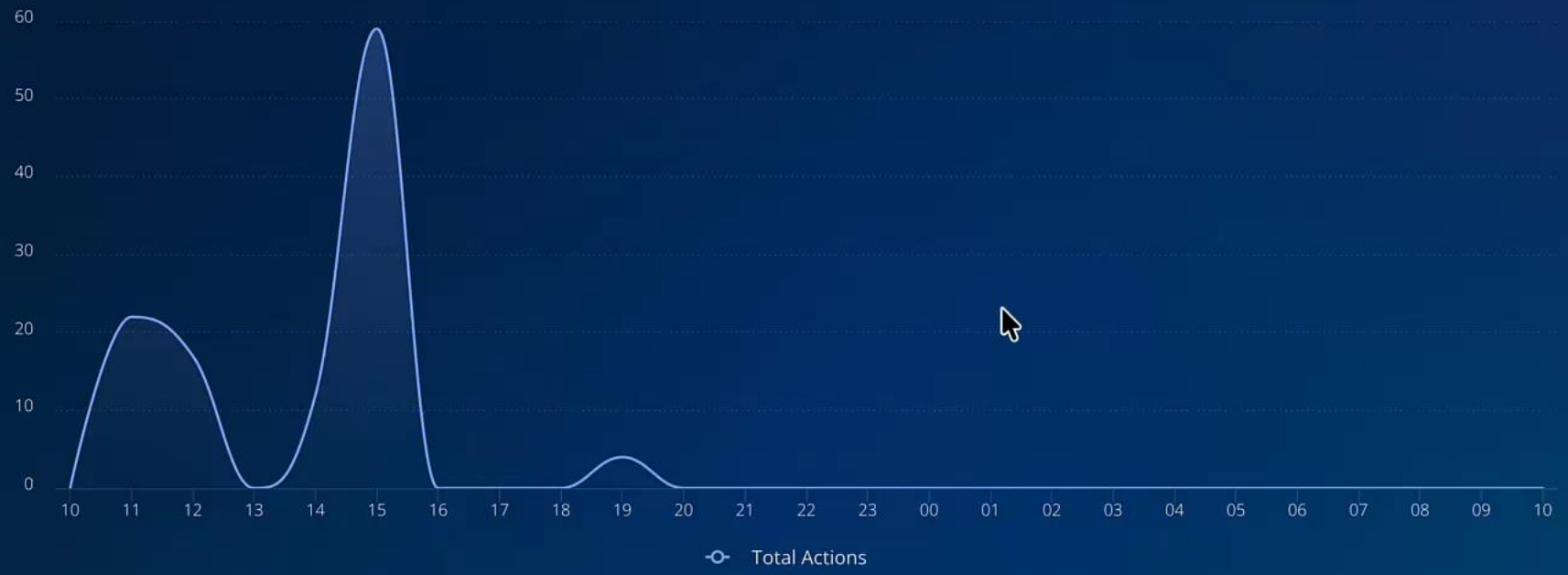
Rubrik:
Kev Johnson

Staff Technical Marketing Manager

Activity and Top Actors Pulse

All IdPs | Past 24 hours

114 -657	19 -378	84 -70	8 -169	3 -5	0 -35	0 — 0
Total Actions	Creation	Deletion	Membership Change	Permission Change	Policy Configuration Change	Tenant Settings Change



Top Actors for Selected Type

Identity Display Name	Actions	
da.waltz@rubrikdemo....	37	↑ 37
rubrikgaia Entra A...	28	↓ 9
Thomas Waltz DA	19	↓ 102
Microsoft Online Servi...	11	
Microsoft Online Servi...	4	↑ 4

User Lifecycle Actions

All IdPs | Past 24 hours

18 -360	4 -110	0 — 0	6 -88	0 — 0	0 — 0	8 -162
Total Actions	Users Created	Password Changed	Users Deleted	Users Locked	Users Disabled	Group Changes

HOW LONG WILL IT TAKE TO RECOVER?

CYBER RECOVERY TIMELINE

WHAT IS CLEAN?

01

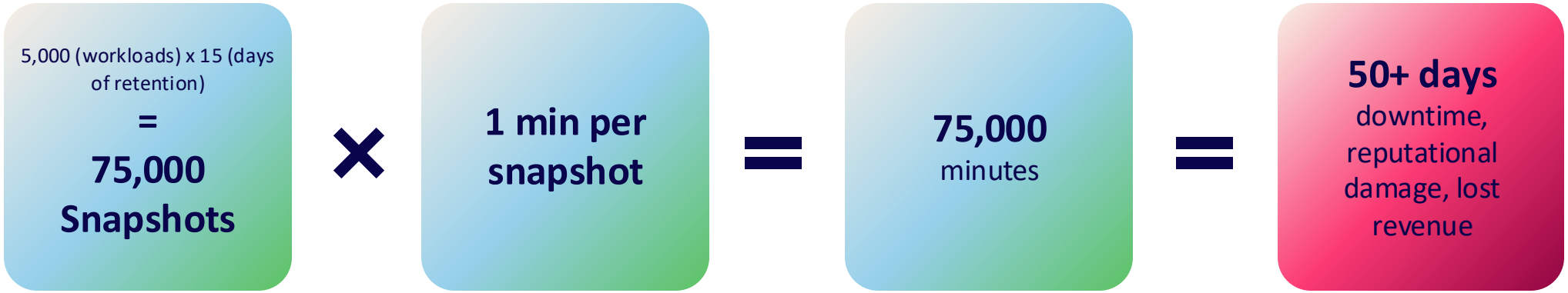
Data Pre-Encryption or Deletion

02

Free From Attacker Ransomware

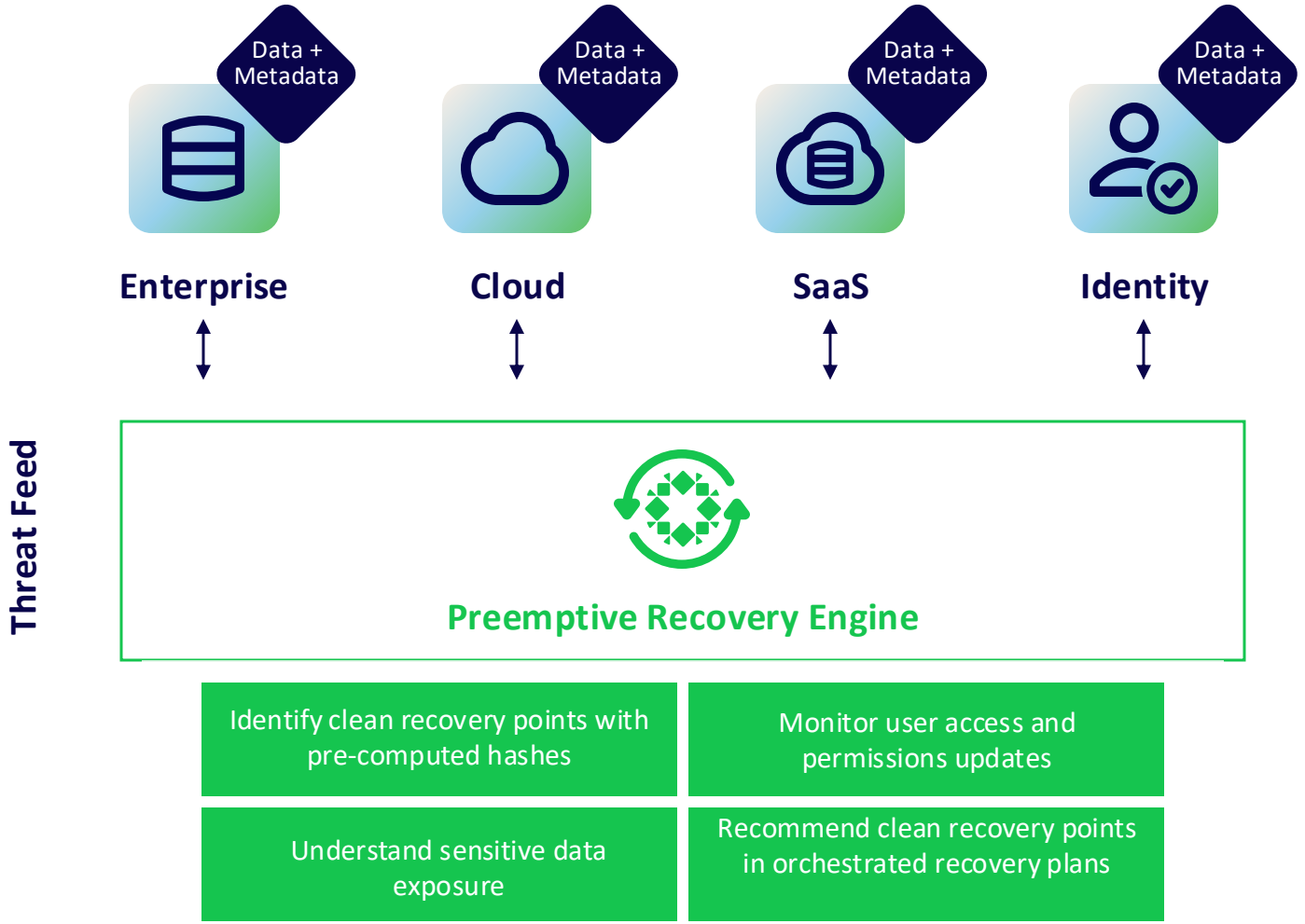
03

Free From Attacker Tools

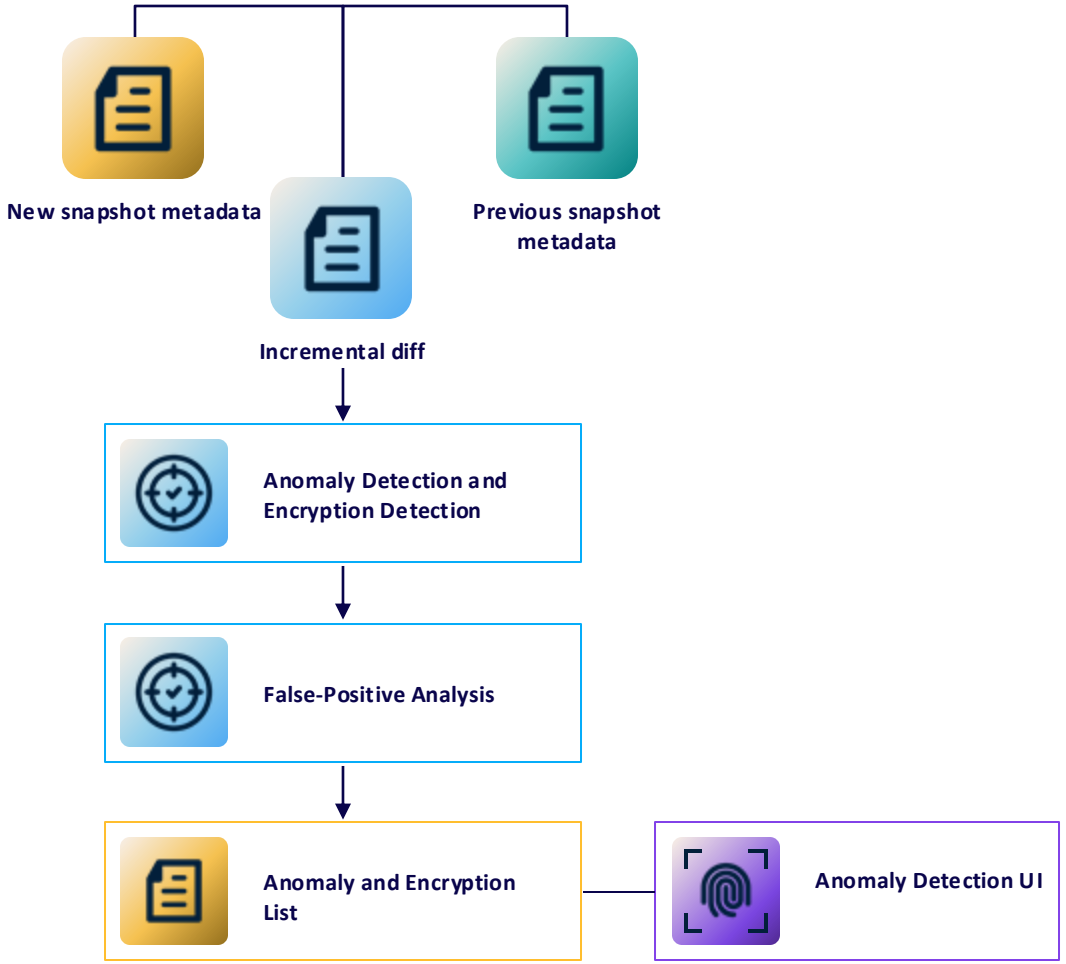


HOW FAST CAN YOU SCAN YOUR BACKUPS?

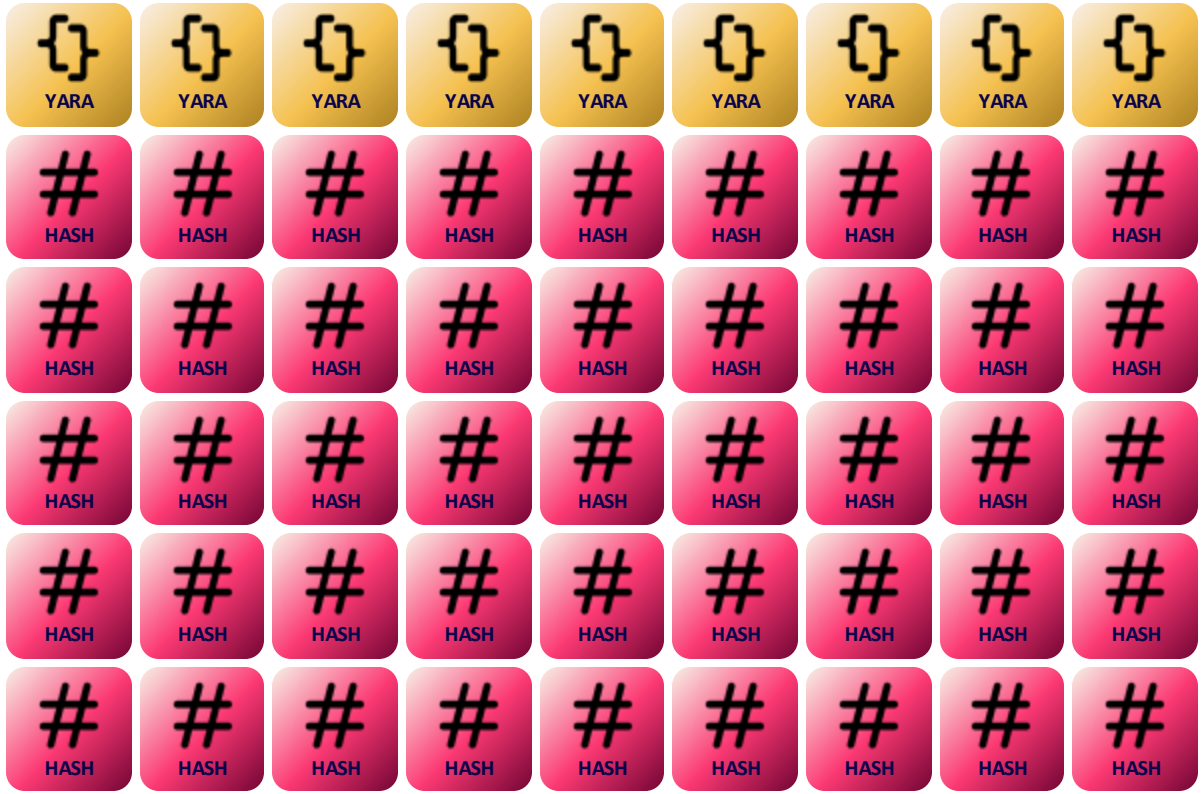
INTRODUCING
THE RUBRIK PREEMPTIVE RECOVERY ENGINE


Data + Metadata
Data + Metadata
Data + Metadata
Data + Metadata
Enterprise
Cloud
SaaS
Identity
Threat Feed
Preemptive Recovery Engine
Identify clean recovery points with pre-computed hashes
Monitor user access and permissions updates
Understand sensitive data exposure
Recommend clean recovery points in orchestrated recovery plans

ANOMALY DETECTION

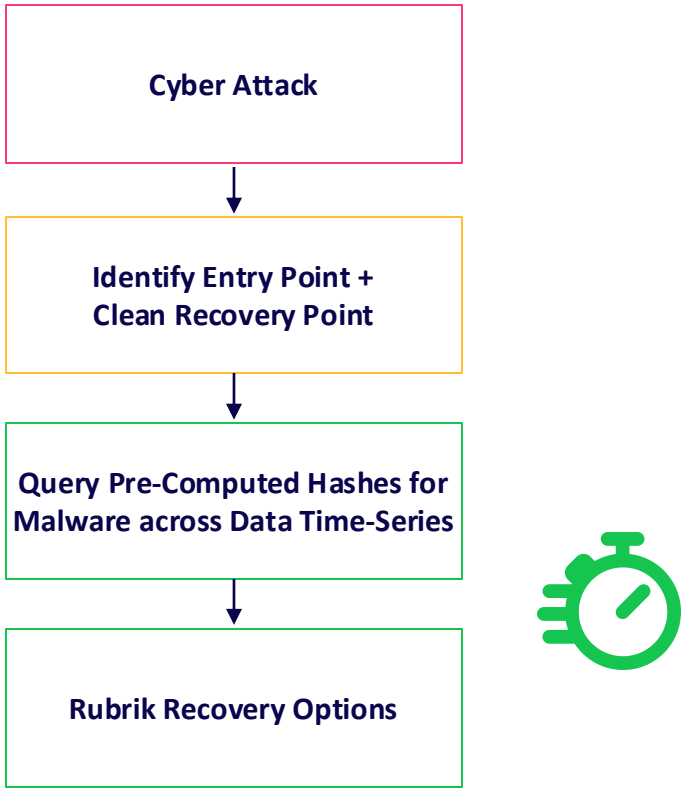


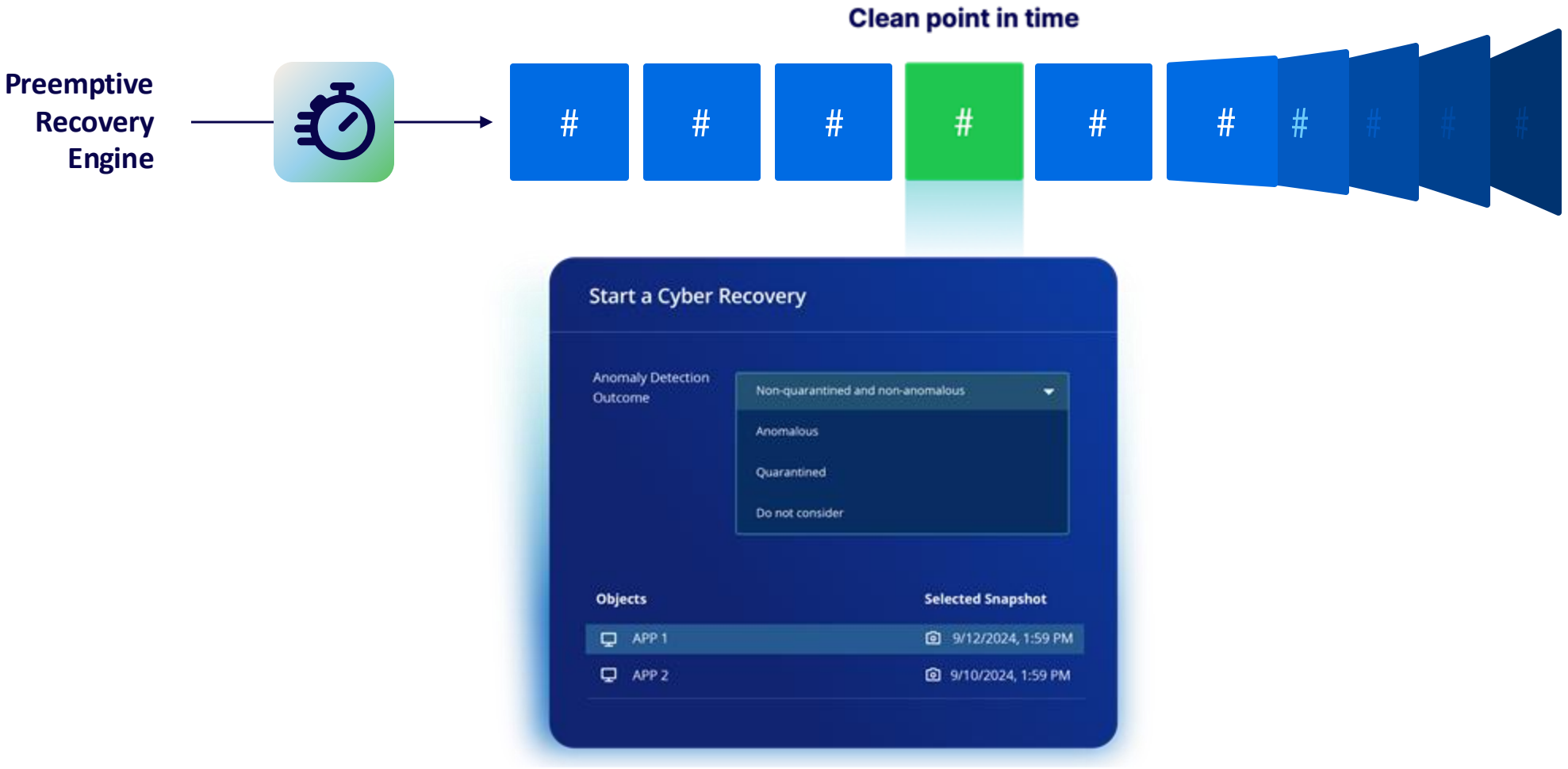
THREAT MONITORING AND HUNTING



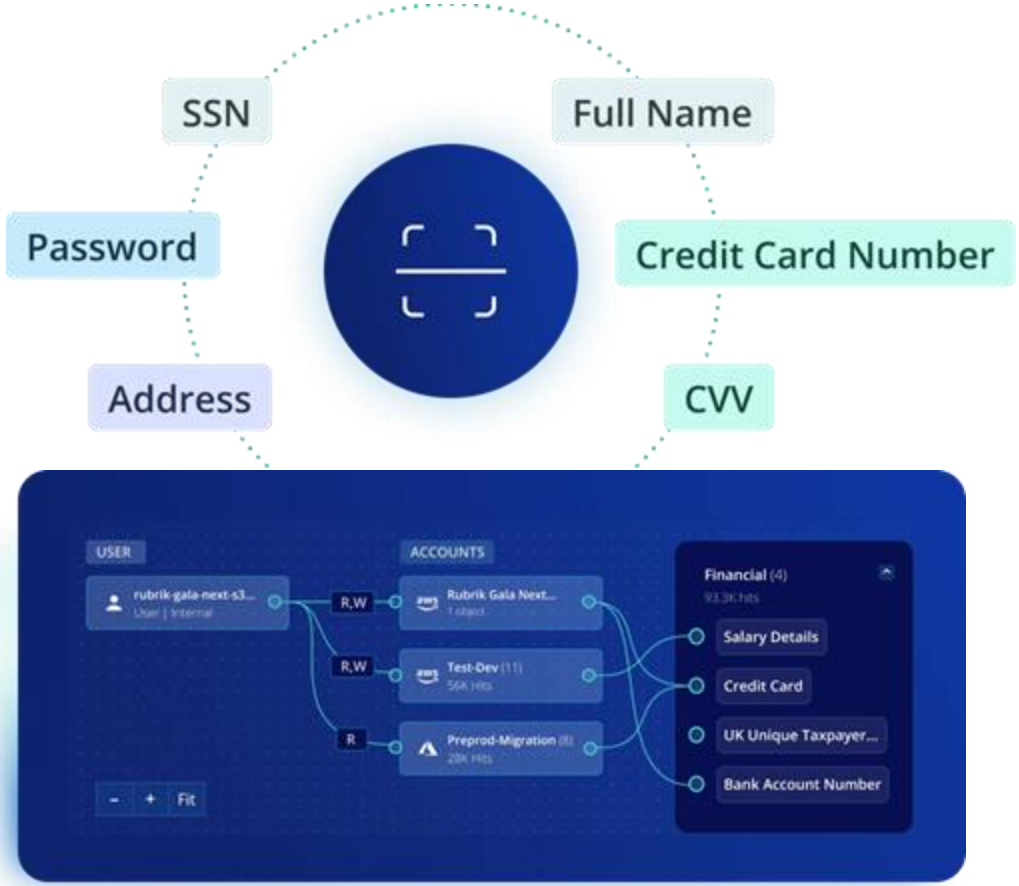
TURBO THREAT HUNTING

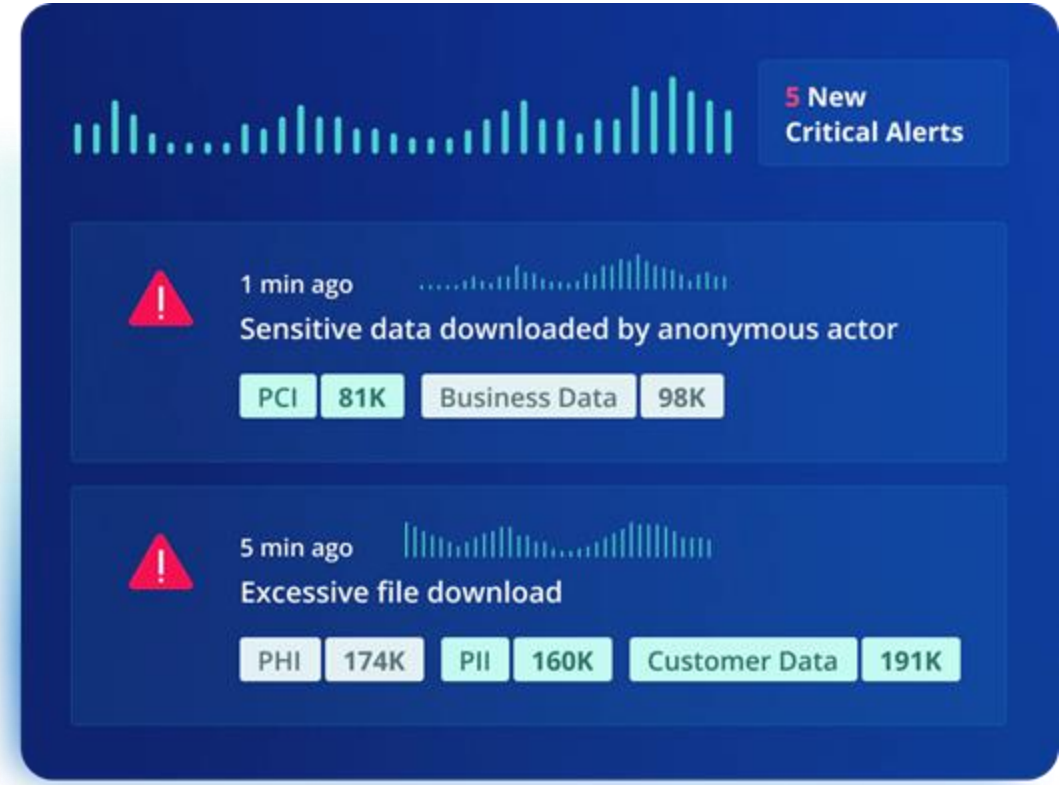
75,000 snapshots scanned in up to 60 seconds!



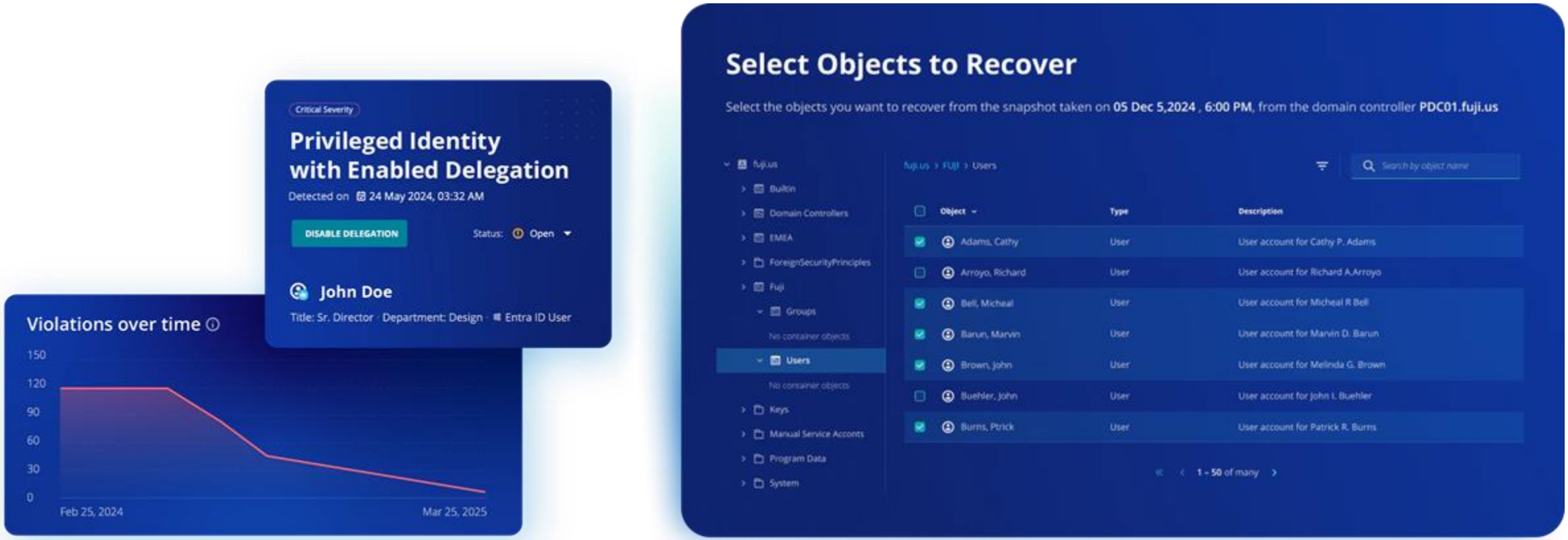

Clean point in time
Preemptive Recovery Engine
Start a Cyber Recovery
Anomaly Detection Outcome
Non-quarantined and non-anomalous
Anomalous
Quarantined
Do not consider
Objects
Selected Snapshot
APP 1
9/12/2024, 1:59 PM
APP 2
9/10/2024, 1:59 PM

SENSITIVE DATA EXPOSURE





IDENTITY RESILIENCE



MINIMIZING IMPACT OF CYBERATTACKS

MINIMIZING IMPACT OF CYBERATTACKS


WHAT THE
CHUNGAR!?

MONITOR

Full visibility into your agents and their actions with granular app & identity understanding.

VALIDATE & GOVERN

Enforce policies, quantify risk and detect agent errors in real time

REMEDIATE

Undo destructive actions to data, apply guardrails, and optimise agent performance.

CONTEXT ENRICHMENT CARDS

Current CrowdScore

Today

0 / 100

Last refreshed: 11:41:38

New detections

1,822

Last refreshed: 11:41:38

SHA-based detections

27d849efb6c5d9d031a356743de848a70fc827623...	720
d7f10571f58adbe122f615b869eb42b05286770148...	668
Total	1,822

Last refreshed: 11:41:38

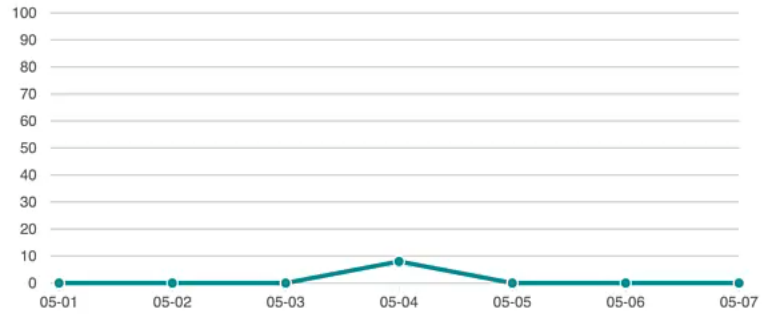
Prevented malware by host

Last 7 days

No data found

Last refreshed: 11:41:38

CrowdScore over time



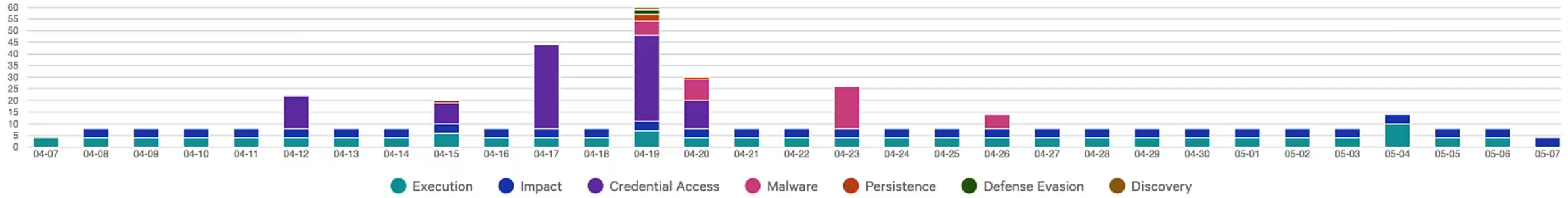
Last refreshed: 11:41:38

Most recent detections

Severity	Tactic & Technique	Time	Host ID	Link
High	Impact via Data Encrypte...	May 7, 2026 02:00:03	SX1-CRWD-W1	See detection
High	Impact via Data Encrypte...	May 7, 2026 02:00:03	SH1-CRWD-W1	See detection
High	Impact via Data Encrypte...	May 7, 2026 02:00:03	SX2-CRWD-W1	See detection

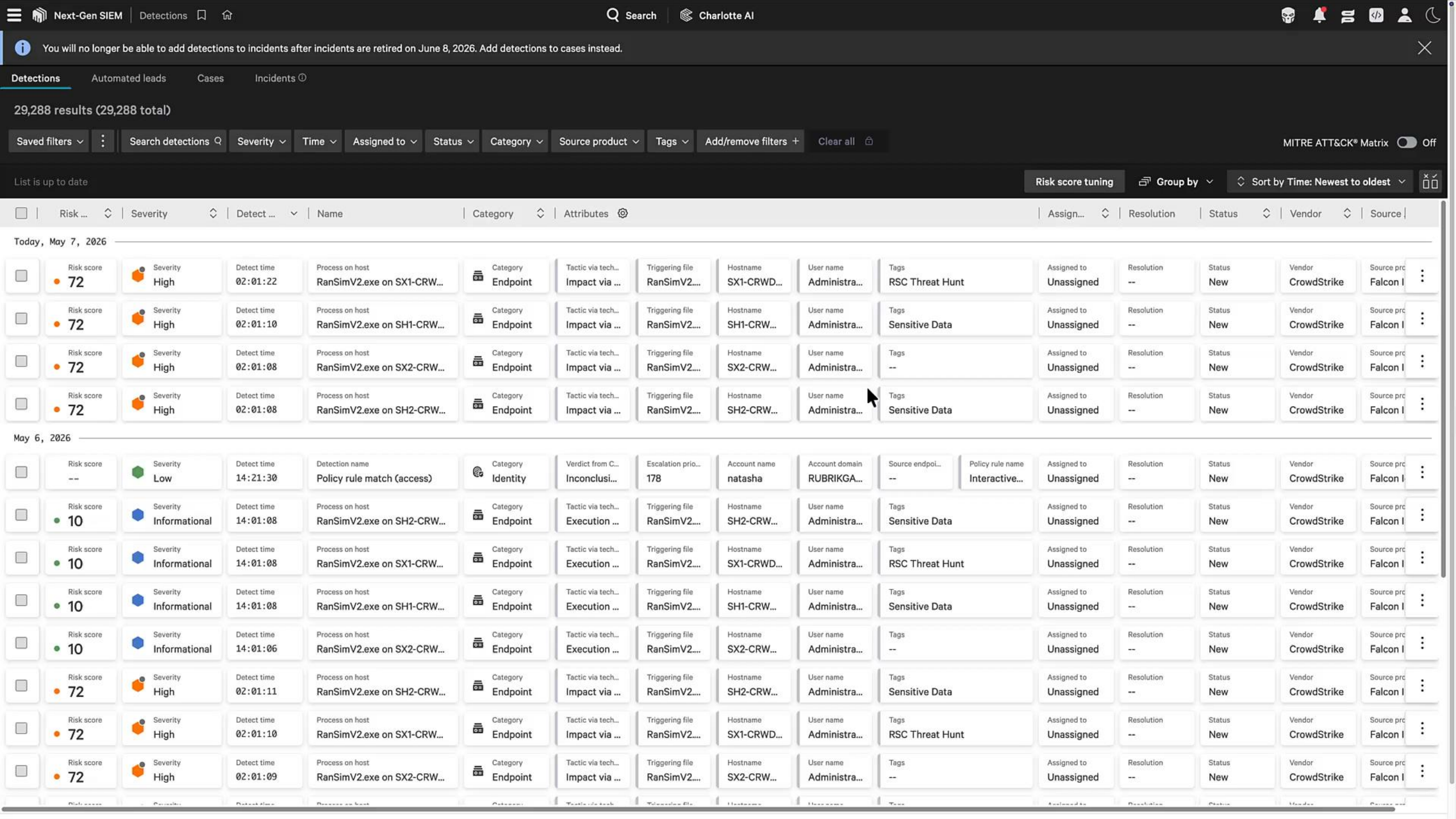
Last refreshed: 11:41:38

Detections by tactics



Last refreshed: 11:41:38

NG-SIEM & FUSION SOAR


Next-Gen SIEM
Detections
Search
Charlotte AI
You will no longer be able to add detections to incidents after incidents are retired on June 8, 2026. Add detections to cases instead.
Detections
Automated leads
Cases
Incidents
29,288 results (29,288 total)
Saved filters
Search detections
Severity
Time
Assigned to
Status
Category
Source product
Tags
Add/remove filters
Clear all
MITRE ATT&CK® Matrix
Off
List is up to date
Risk score tuning
Group by
Sort by Time: Newest to oldest
Risk ...
Severity
Detect ...
Name
Category
Attributes
Assign...
Resolution
Status
Vendor
Source
Today, May 7, 2026
Risk score 72 | Severity High | Detect time 02:01:22 | Process on host RanSimV2.exe on SX1-CRW... | Category Endpoint | Tactic via tech... Impact via ... | Triggering file RanSimV2.... | Hostname SX1-CRWD... | User name Administra... | Tags RSC Threat Hunt | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 72 | Severity High | Detect time 02:01:10 | Process on host RanSimV2.exe on SH1-CRW... | Category Endpoint | Tactic via tech... Impact via ... | Triggering file RanSimV2.... | Hostname SH1-CRW... | User name Administra... | Tags Sensitive Data | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 72 | Severity High | Detect time 02:01:08 | Process on host RanSimV2.exe on SX2-CRW... | Category Endpoint | Tactic via tech... Impact via ... | Triggering file RanSimV2.... | Hostname SX2-CRW... | User name Administra... | Tags -- | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 72 | Severity High | Detect time 02:01:08 | Process on host RanSimV2.exe on SH2-CRW... | Category Endpoint | Tactic via tech... Impact via ... | Triggering file RanSimV2.... | Hostname SH2-CRW... | User name Administra... | Tags Sensitive Data | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
May 6, 2026
Risk score -- | Severity Low | Detect time 14:21:30 | Detection name Policy rule match (access) | Category Identity | Verdict from C... Inconclusi... | Escalation prio... 178 | Account name natasha | Account domain RUBRIKGA... | Source endpoi... -- | Policy rule name Interactive... | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 10 | Severity Informational | Detect time 14:01:08 | Process on host RanSimV2.exe on SH2-CRW... | Category Endpoint | Tactic via tech... Execution ... | Triggering file RanSimV2.... | Hostname SH2-CRW... | User name Administra... | Tags Sensitive Data | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 10 | Severity Informational | Detect time 14:01:08 | Process on host RanSimV2.exe on SX1-CRW... | Category Endpoint | Tactic via tech... Execution ... | Triggering file RanSimV2.... | Hostname SX1-CRWD... | User name Administra... | Tags RSC Threat Hunt | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 10 | Severity Informational | Detect time 14:01:08 | Process on host RanSimV2.exe on SH1-CRW... | Category Endpoint | Tactic via tech... Execution ... | Triggering file RanSimV2.... | Hostname SH1-CRW... | User name Administra... | Tags Sensitive Data | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 10 | Severity Informational | Detect time 14:01:06 | Process on host RanSimV2.exe on SX2-CRW... | Category Endpoint | Tactic via tech... Execution ... | Triggering file RanSimV2.... | Hostname SX2-CRW... | User name Administra... | Tags -- | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 72 | Severity High | Detect time 02:01:11 | Process on host RanSimV2.exe on SH2-CRW... | Category Endpoint | Tactic via tech... Impact via ... | Triggering file RanSimV2.... | Hostname SH2-CRW... | User name Administra... | Tags Sensitive Data | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 72 | Severity High | Detect time 02:01:10 | Process on host RanSimV2.exe on SX1-CRW... | Category Endpoint | Tactic via tech... Impact via ... | Triggering file RanSimV2.... | Hostname SX1-CRWD... | User name Administra... | Tags RSC Threat Hunt | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I
Risk score 72 | Severity High | Detect time 02:01:09 | Process on host RanSimV2.exe on SX2-CRW... | Category Endpoint | Tactic via tech... Impact via ... | Triggering file RanSimV2.... | Hostname SX2-CRW... | User name Administra... | Tags -- | Assigned to Unassigned | Resolution -- | Status New | Vendor CrowdStrike | Source pro Falcon I

HOW DO I GET THIS?

Current CrowdScore

Today

0 / 100

Last refreshed: 10:22:01

New detections

1,822

Last refreshed: 10:22:01

SHA-based detections

27d849efb6c5d9d031a356743de848a70fc827623...	720
d7f10571f58adbe122f615b869eb42b05286770148...	668
Total	1,822

Last refreshed: 10:22:01

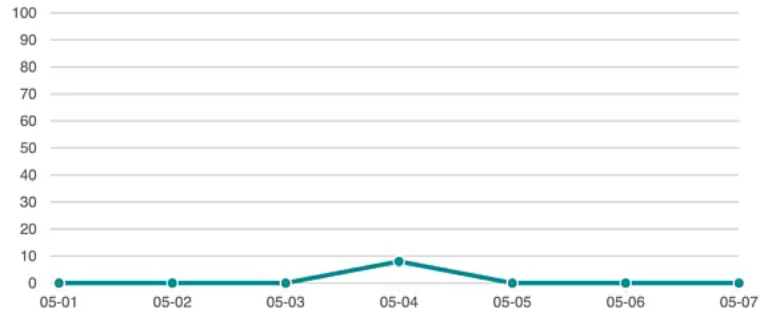
Prevented malware by host

Last 7 days

No data found

Last refreshed: 10:22:02

CrowdScore over time



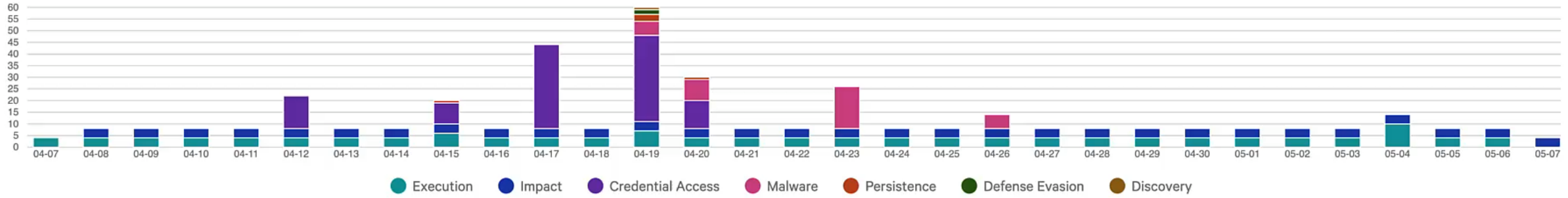
Last refreshed: 10:22:01

Most recent detections

Severity	Tactic & Technique	Time	Host ID	Link
High	Impact via Data Encrypte...	May 7, 2026 02:00:03	SX1-CRWD-W1	See detection
High	Impact via Data Encrypte...	May 7, 2026 02:00:03	SH1-CRWD-W1	See detection
High	Impact via Data Encrypte...	May 7, 2026 02:00:03	SX2-CRWD-W1	See detection

Last refreshed: 10:22:01

Detections by tactics



Last refreshed: 10:22:01

Security + IT = resilience

CROWDSTRIKE

rubrik

Security ⟷ Unified response & recovery ⟷ **IT operations**

- Threat detection & response
- Identity threat protection
- AI model monitoring

- Data protection & backup
- Clean recovery points
- Secure data restoration

Detect & notify →

Cyber threats

- AI-powered attacks
- Data breaches
- Ransomware

← **Validate & recover**

Recovery options

- Verify clean data
- Restore AI models
- Rollback identity changes

How Softcat can help

1. **Bespoke security workshop:** Framing and mitigation of risk and how to ensure clean and fast recovery.

2. **Rubrik & CrowdStrike discovery sessions:** Displaying the already existing and pre-built integrations available from the CrowdStrike marketplace with your teams.

softcat

Thank you