Trellix

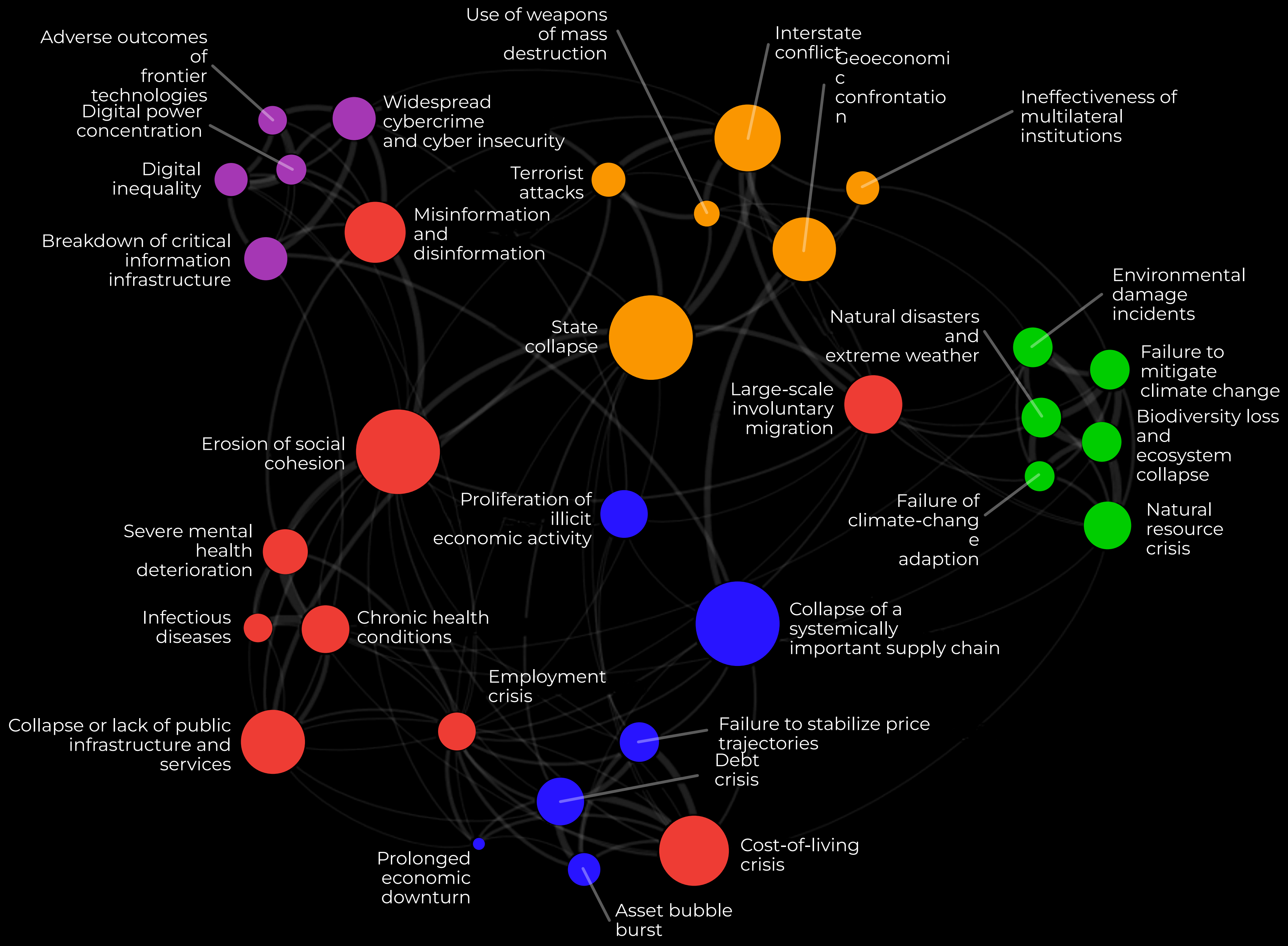
Unveiling the Shadows in a Polycrisis

Chaos to Clarity

Polycrisis

“A cluster of related global risks with compounding effects, such that the overall impact exceeds the sum of each part ”.

The World Economic Forum’s
Global Risks Report 2023


Adverse outcomes of frontier technologies
Digital power concentration
Digital inequality
Breakdown of critical information infrastructure
Widespread cybercrime and cyber insecurity
Misinformation and disinformation
Use of weapons of mass destruction
Terrorist attacks
Interstate conflict
Geoeconomic confrontation
Ineffectiveness of multilateral institutions
State collapse
Natural disasters and extreme weather
Environmental damage incidents
Failure to mitigate climate change
Large-scale involuntary migration
Biodiversity loss and ecosystem collapse
Failure of climate-change adaption
Natural resource crisis
Erosion of social cohesion
Proliferation of illicit economic activity
Severe mental health deterioration
Infectious diseases
Chronic health conditions
Collapse of a systemically important supply chain
Employment crisis
Collapse or lack of public infrastructure and services
Failure to stabilize price trajectories
Debt crisis
Cost-of-living crisis
Prolonged economic downturn
Asset bubble burst

Cyber crime thrives during an era of “Polycrisis”

The World Economic Forum defines a ”polycrisis” as follows:

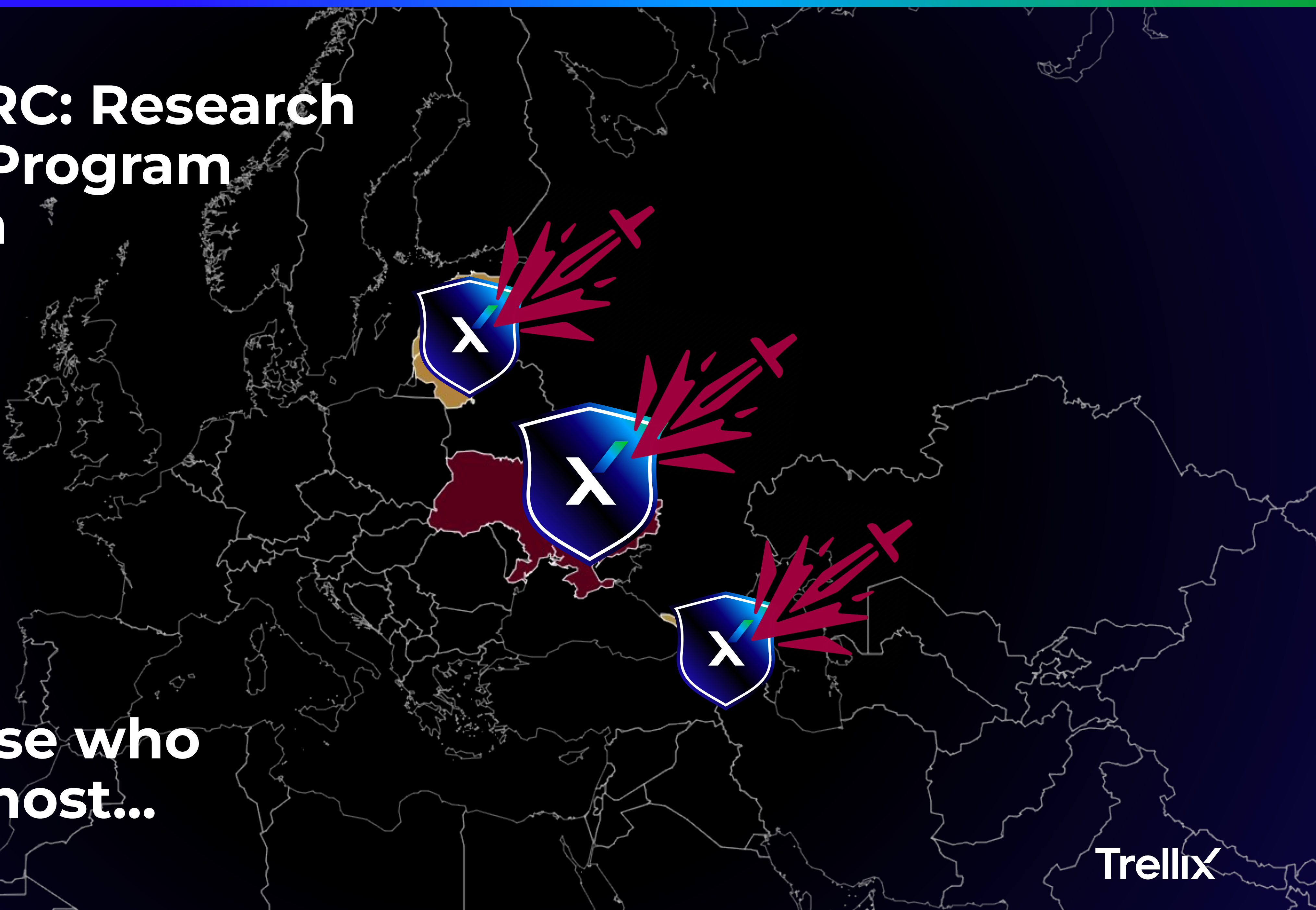
“A cluster of related global risks with compounding effects, such that the overall impact exceeds the sum of each part”

Reuters:

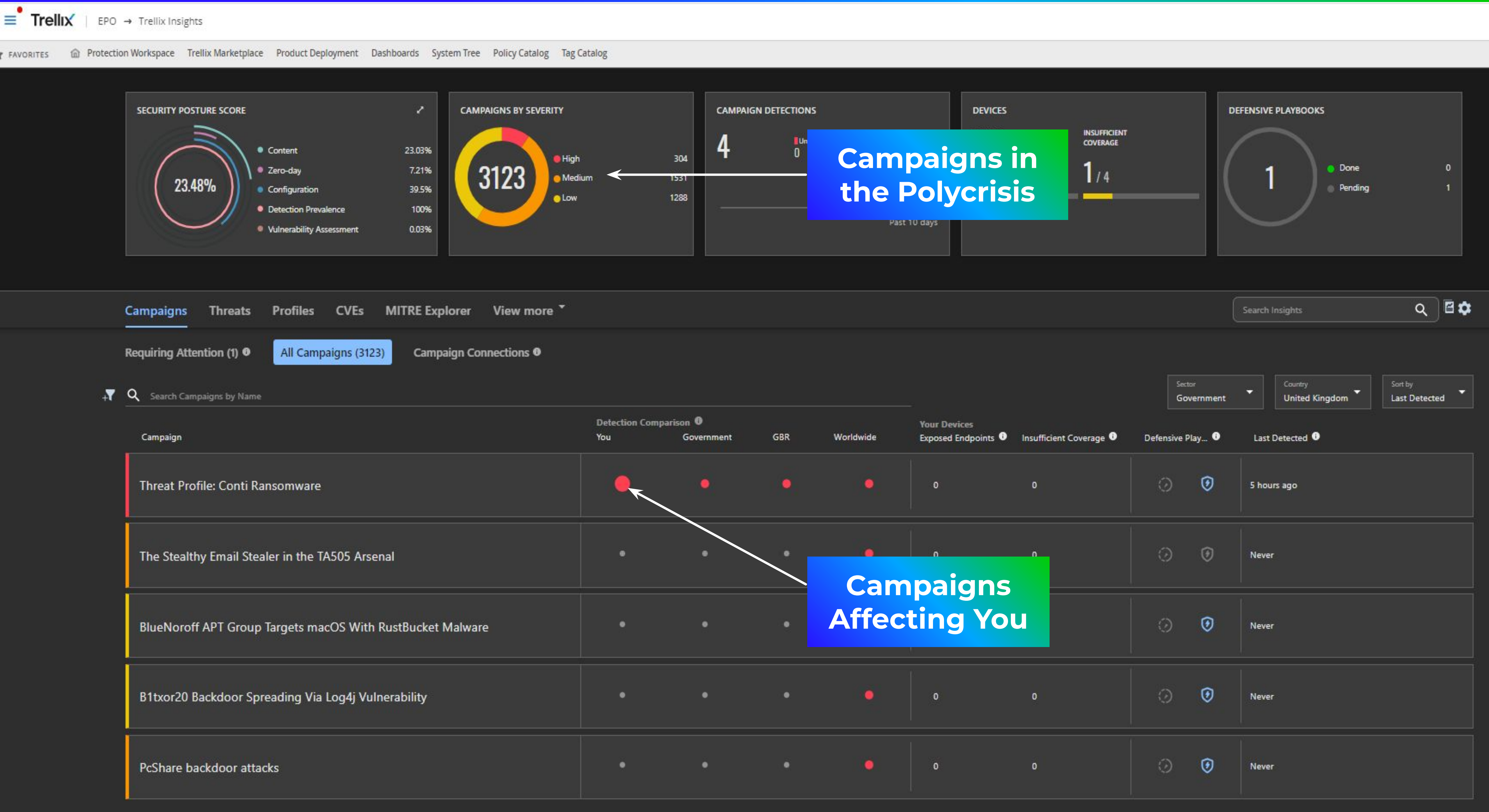
“Often the transportation sector finds itself at the heart of this upheaval, both as victim and protagonist.”

Trellix

Trellix ARC: Research Partner Program In Action



Help those who need it most...



Trellix | EPO → Trellix Insights

FAVORITES | Protection Workspace | Trellix Marketplace | Product Deployment | Dashboards | System Tree | Policy Catalog | Tag Catalog

SECURITY POSTURE SCORE

23.48%

Content	23.03%
Zero-day	7.21%
Configuration	39.5%
Detection Prevalence	100%
Vulnerability Assessment	0.03%

CAMPAIGNS BY SEVERITY

3123

High	304
Medium	1531
Low	1288

CAMPAIGN DETECTIONS

4

Un
0

Past 10 days

DEVICES

INSUFFICIENT COVERAGE

1 / 4

DEFENSIVE PLAYBOOKS

1

Done	0
Pending	1

Campaigns | Threats | Profiles | CVEs | MITRE Explorer | View more

Search Insights

Requiring Attention (1) | All Campaigns (3123) | Campaign Connections

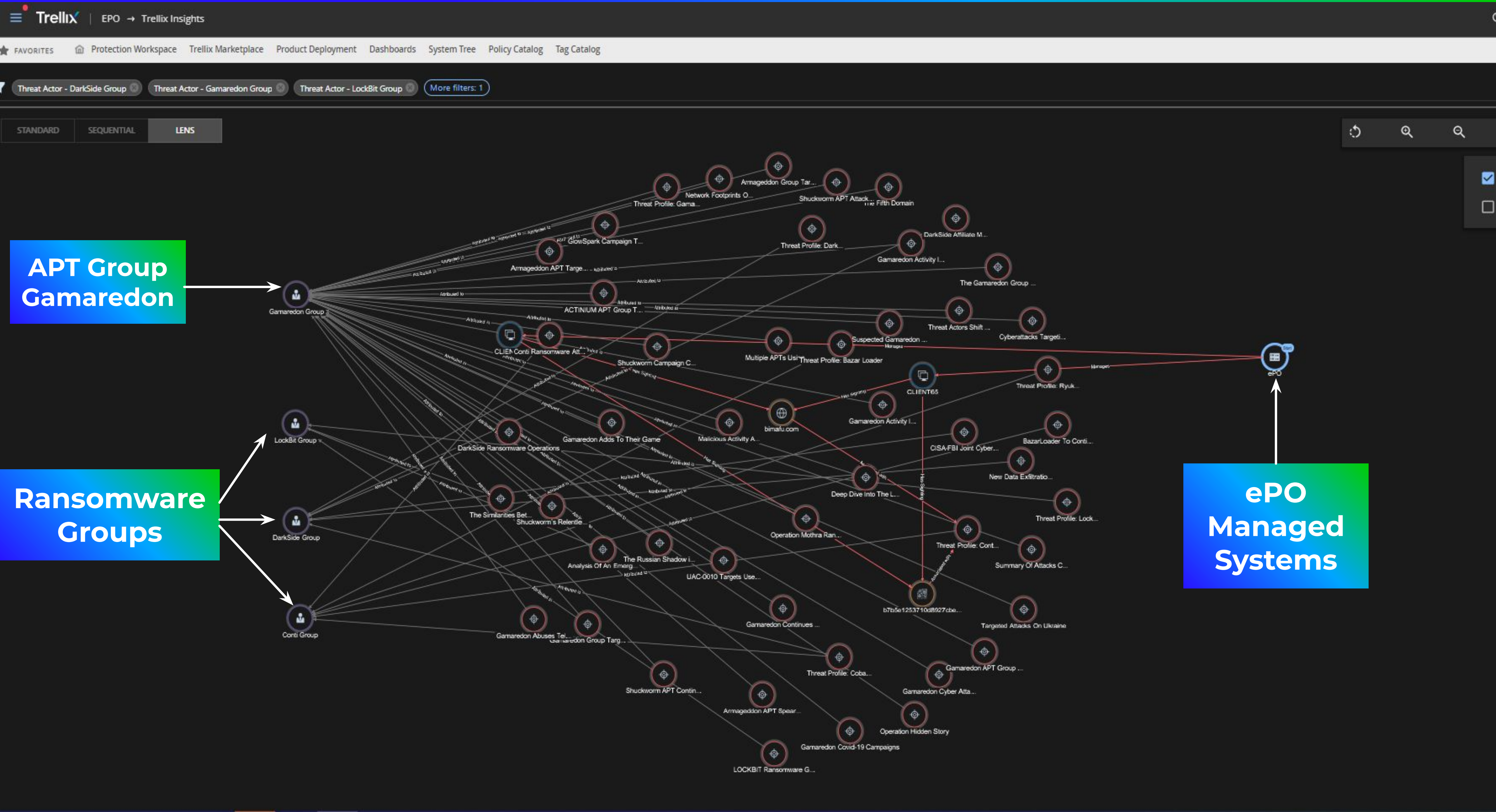
Search Campaigns by Name

Sector: Government
Country: United Kingdom
Sort by: Last Detected

	Detection Comparison				Your Devices			
Campaign	You	Government	GBR	Worldwide	Exposed Endpoints	Insufficient Coverage	Defensive Play...	Last Detected
Threat Profile: Conti Ransomware	●	●	●	●	0	0		5 hours ago
The Stealthy Email Stealer in the TA505 Arsenal	·	·	·	●	0	0		Never
BlueNoroff APT Group Targets macOS With RustBucket Malware	·	·	·					Never
B1txor20 Backdoor Spreading Via Log4j Vulnerability	·	·	·	●	0	0		Never
PcShare backdoor attacks	·	·	·	●	0	0		Never

Campaigns in the Polycrisis

Campaigns Affecting You



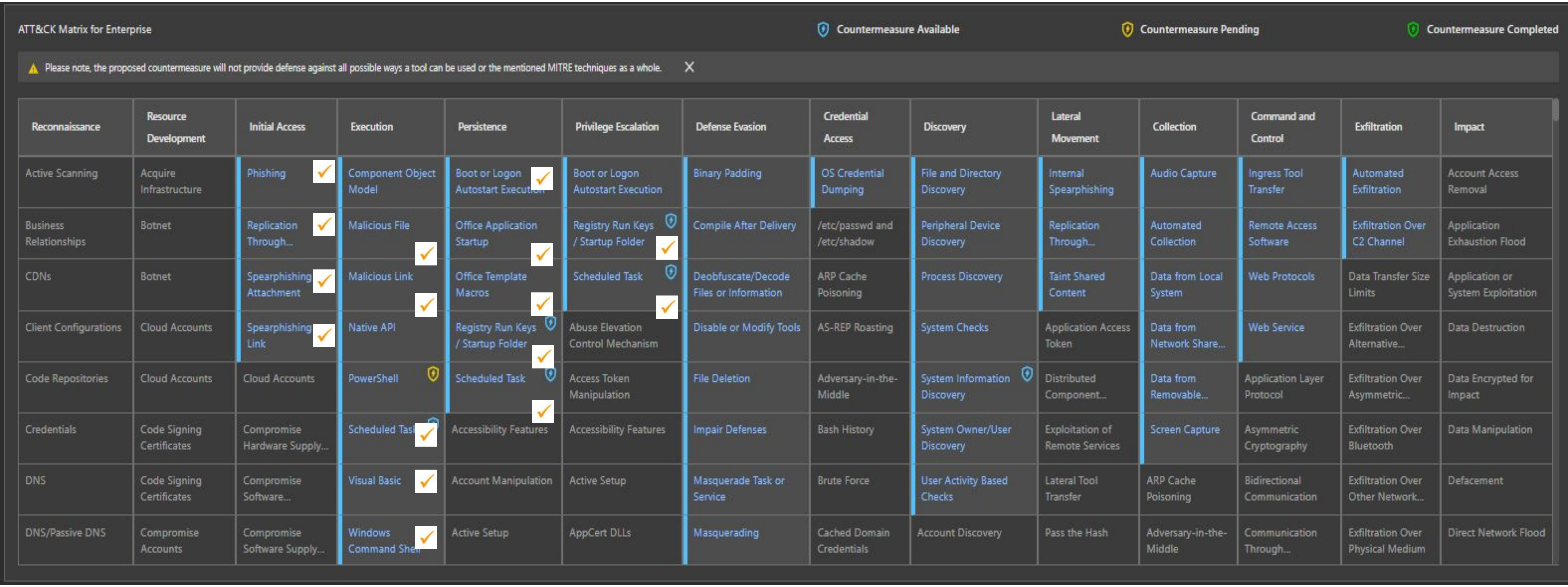
Threat Actor - DarkSide Group
Threat Actor - Gamaredon Group
Threat Actor - LockBit Group
More filters: 1

APT Group Gamaredon

Ransomware Groups

ePO Managed Systems

Identify APT Attacks Early

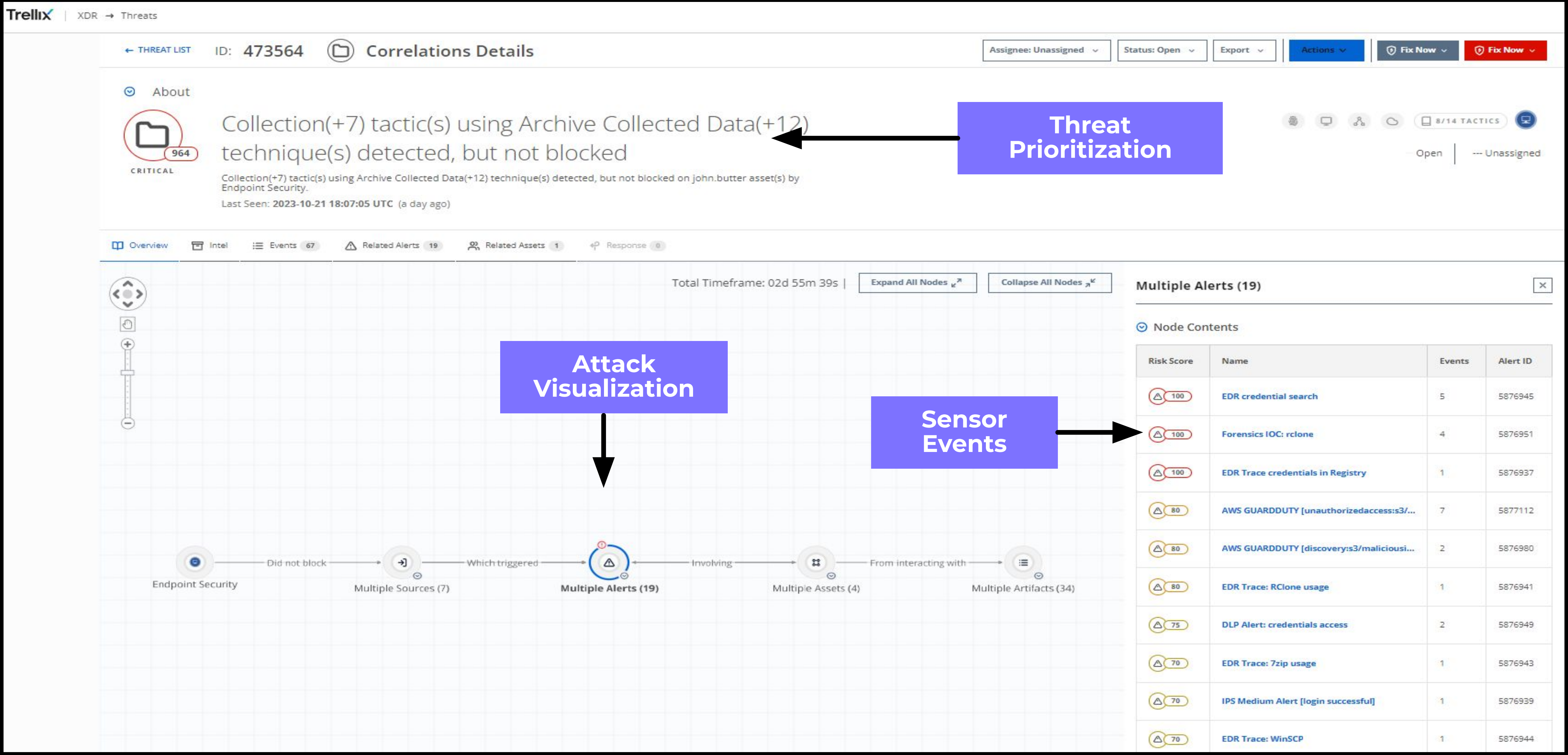


ATT&CK Matrix for Enterprise — 🛡 Countermeasure Available — 🛡 Countermeasure Pending — 🛡 Countermeasure Completed

⚠ Please note, the proposed countermeasure will not provide defense against all possible ways a tool can be used or the mentioned MITRE techniques as a whole. ✕

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Phishing ✓	Component Object Model	Boot or Logon Autostart Execution ✓	Boot or Logon Autostart Execution	Binary Padding	OS Credential Dumping	File and Directory Discovery	Internal Spearphishing	Audio Capture	Ingress Tool Transfer	Automated Exfiltration	Account Access Removal
Business Relationships	Botnet	Replication Through... ✓	Malicious File ✓	Office Application Startup ✓	Registry Run Keys / Startup Folder 🛡 ✓	Compile After Delivery	/etc/passwd and /etc/shadow	Peripheral Device Discovery	Replication Through...	Automated Collection	Remote Access Software	Exfiltration Over C2 Channel	Application Exhaustion Flood
CDNs	Botnet	Spearphishing Attachment ✓	Malicious Link ✓	Office Template Macros ✓	Scheduled Task 🛡 ✓	Deobfuscate/Decode Files or Information	ARP Cache Poisoning	Process Discovery	Taint Shared Content	Data from Local System	Web Protocols	Data Transfer Size Limits	Application or System Exploitation
Client Configurations	Cloud Accounts	Spearphishing Link ✓	Native API	Registry Run Keys / Startup Folder 🛡 ✓	Abuse Elevation Control Mechanism	Disable or Modify Tools	AS-REP Roasting	System Checks	Application Access Token	Data from Network Share...	Web Service	Exfiltration Over Alternative...	Data Destruction
Code Repositories	Cloud Accounts	Cloud Accounts	PowerShell 🛡	Scheduled Task 🛡 ✓	Access Token Manipulation	File Deletion	Adversary-in-the-Middle	System Information Discovery 🛡	Distributed Component...	Data from Removable...	Application Layer Protocol	Exfiltration Over Asymmetric...	Data Encrypted for Impact
Credentials	Code Signing Certificates	Compromise Hardware Supply...	Scheduled Task 🛡 ✓	Accessibility Features	Accessibility Features	Impair Defenses	Bash History	System Owner/User Discovery	Exploitation of Remote Services	Screen Capture	Asymmetric Cryptography	Exfiltration Over Bluetooth	Data Manipulation
DNS	Code Signing Certificates	Compromise Software...	Visual Basic ✓	Account Manipulation	Active Setup	Masquerade Task or Service	Brute Force	User Activity Based Checks	Lateral Tool Transfer	ARP Cache Poisoning	Bidirectional Communication	Exfiltration Over Other Network...	Defacement
DNS/Passive DNS	Compromise Accounts	Compromise Software Supply...	Windows Command Shell ✓	Active Setup	AppCert DLLs	Masquerading	Cached Domain Credentials	Account Discovery	Pass the Hash	Adversary-in-the-Middle	Communication Through...	Exfiltration Over Physical Medium	Direct Network Flood

XDR = Visibility Across the Kill Chain



ID: 473564 Correlations Details

About

964 CRITICAL

Collection(+7) tactic(s) using Archive Collected Data(+12) technique(s) detected, but not blocked

Collection(+7) tactic(s) using Archive Collected Data(+12) technique(s) detected, but not blocked on john.butter asset(s) by Endpoint Security.

Last Seen: **2023-10-21 18:07:05 UTC** (a day ago)

Total Timeframe: 02d 55m 39s |

Multiple Alerts (19)

Node Contents

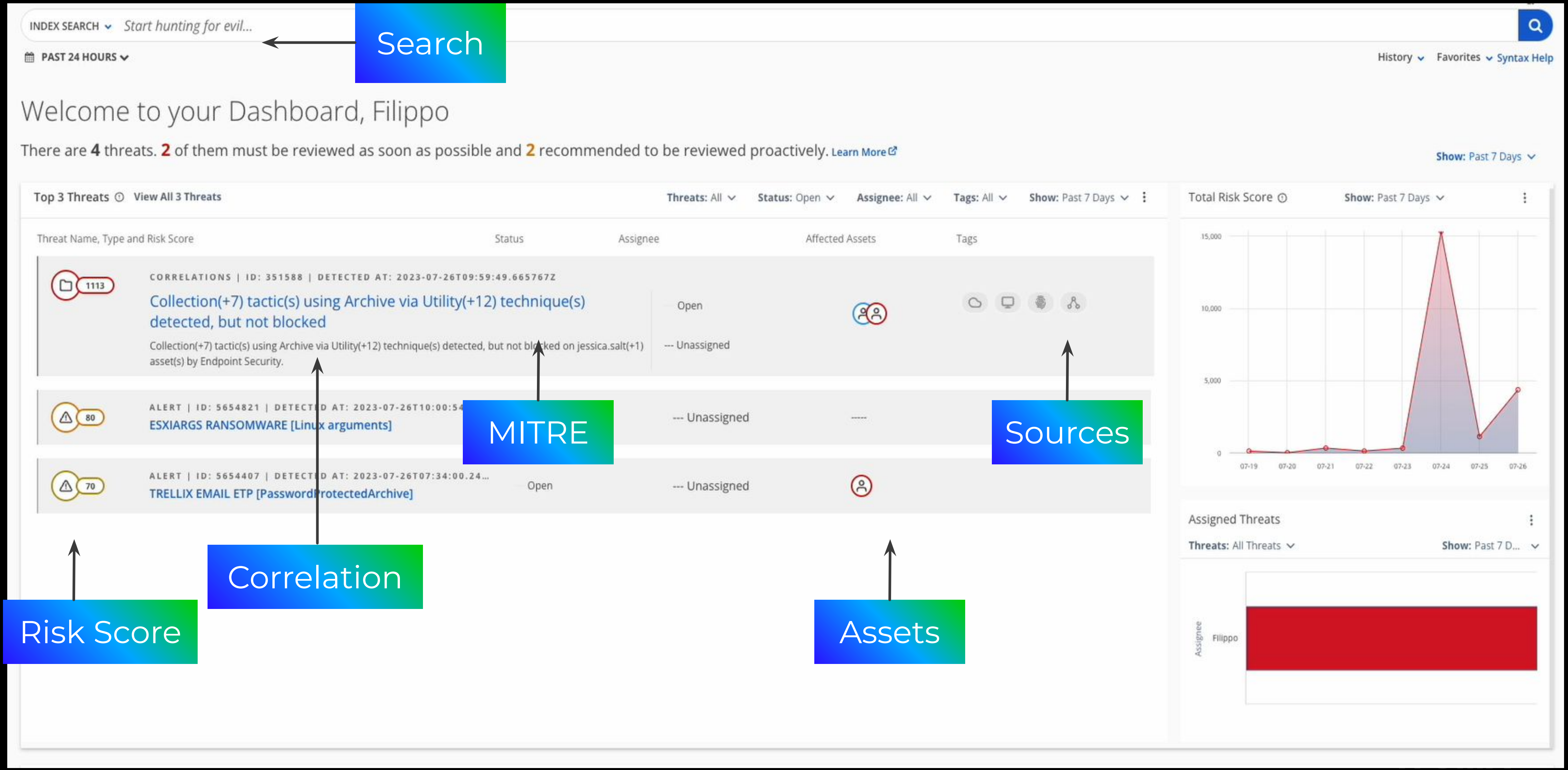
Risk Score	Name	Events	Alert ID
100	EDR credential search	5	5876945
100	Forensics IOC: rclone	4	5876951
100	EDR Trace credentials in Registry	1	5876937
80	AWS GUARDDUTY [unauthorizedaccess:s3/...	7	5877112
80	AWS GUARDDUTY [discovery:s3/maliciousi...	2	5876980
80	EDR Trace: RClone usage	1	5876941
75	DLP Alert: credentials access	2	5876949
70	EDR Trace: 7zip usage	1	5876943
70	IPS Medium Alert [login successful]	1	5876939
70	EDR Trace: WinSCP	1	5876944

Threat Prioritization

Attack Visualization

Sensor Events

XDR Simplifies Detection



INDEX SEARCH ⌄ Start hunting for evil...

PAST 24 HOURS ⌄

History ⌄ Favorites ⌄ Syntax Help

Welcome to your Dashboard, Filippo

There are 4 threats. 2 of them must be reviewed as soon as possible and 2 recommended to be reviewed proactively. Learn More

Show: Past 7 Days ⌄

Top 3 Threats View All 3 Threats

Threats: All ⌄ Status: Open ⌄ Assignee: All ⌄ Tags: All ⌄ Show: Past 7 Days ⌄

Threat Name, Type and Risk Score		Status	Assignee	Affected Assets	Tags
1113	CORRELATIONS | ID: 351588 | DETECTED AT: 2023-07-26T09:59:49.665767Z Collection(+7) tactic(s) using Archive via Utility(+12) technique(s) detected, but not blocked Collection(+7) tactic(s) using Archive via Utility(+12) technique(s) detected, but not blocked on jessica.salt(+1) asset(s) by Endpoint Security.	Open	--- Unassigned		
80	ALERT | ID: 5654821 | DETECTED AT: 2023-07-26T10:00:54 ESXIARGS RANSOMWARE [Linux arguments]		--- Unassigned	-----	
70	ALERT | ID: 5654407 | DETECTED AT: 2023-07-26T07:34:00.24... TRELLIX EMAIL ETP [PasswordProtectedArchive]	Open	--- Unassigned		

Total Risk Score

Show: Past 7 Days ⌄

Assigned Threats

Threats: All Threats ⌄ Show: Past 7 D... ⌄

Search

MITRE

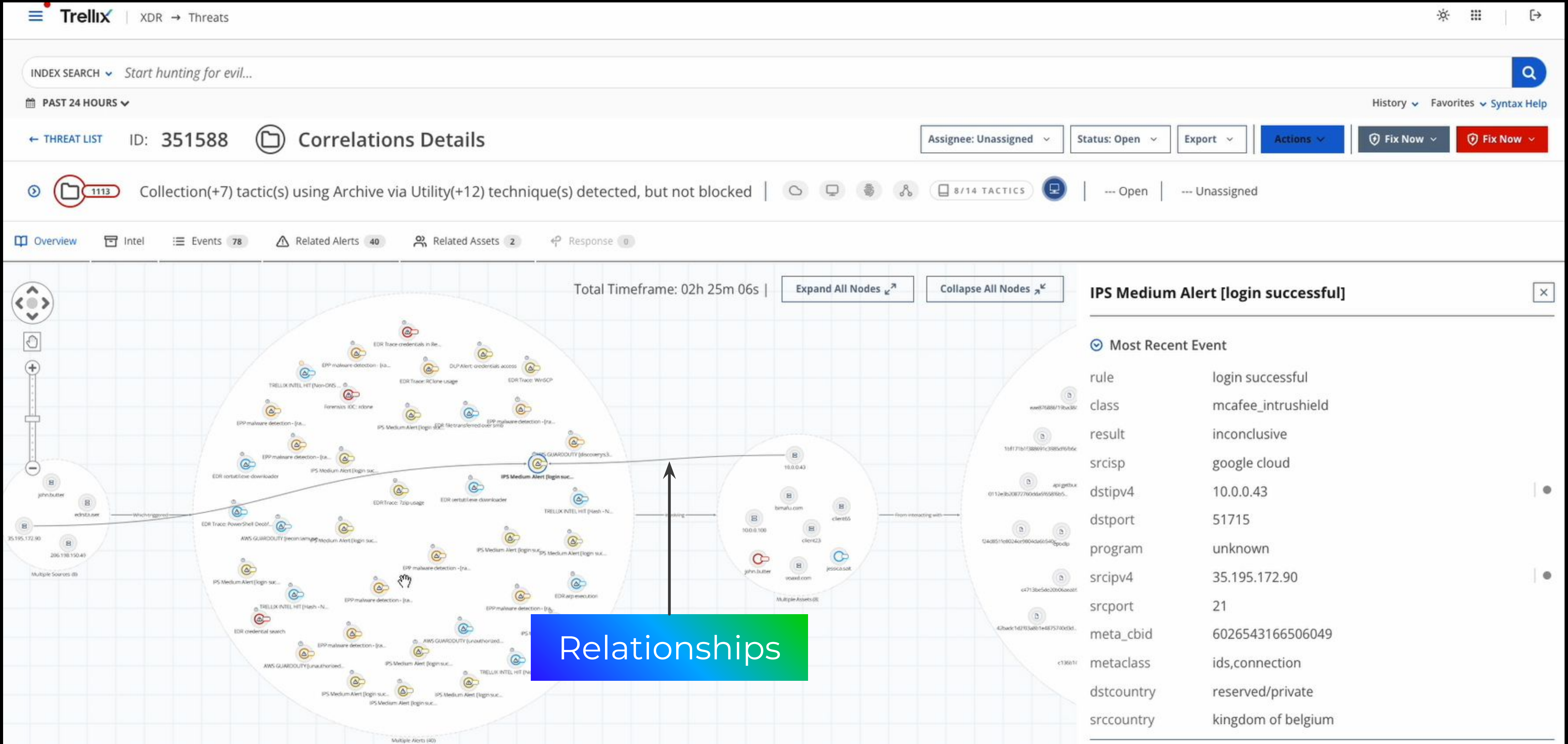
Sources

Correlation

Risk Score

Assets

XDR Simplifies Investigation



ID: 351588 Correlations Details

Collection(+7) tactic(s) using Archive via Utility(+12) technique(s) detected, but not blocked

IPS Medium Alert [login successful]

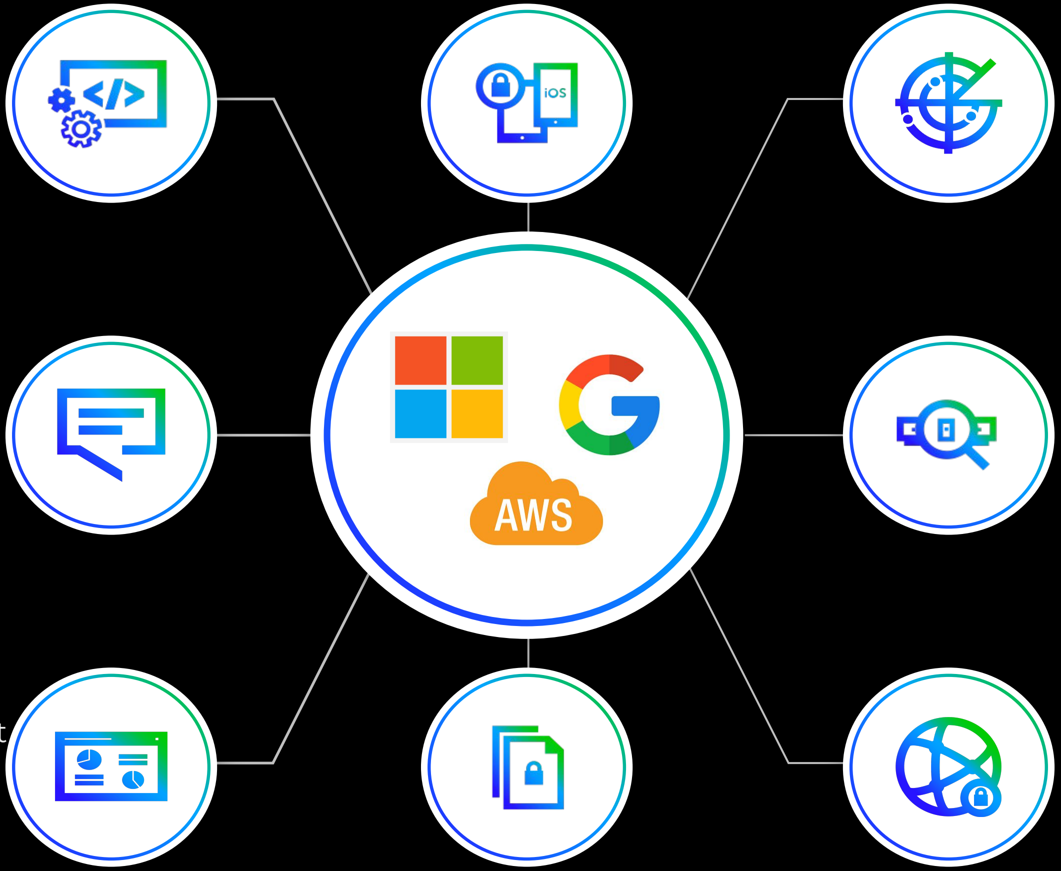
Most Recent Event

rule	login successful
class	mcafee_intrushield
result	inconclusive
srcisp	google cloud
dstipv4	10.0.0.43
dstport	51715
program	unknown
srcipv4	35.195.172.90
srcport	21
meta_cbid	6026543166506049
metaclass	ids,connection
dstcountry	reserved/private
srccountry	kingdom of belgium

Relationships

Augment Built in Defences

Make Your Organization more Resilient with Trellix



Mobile Threat Protection

Trellix Mobile extends protection to
Mobile Devices managed by Intune

Legacy Systems Protection

Trellix Application Control protects
legacy Operating Systems

Email Security

Trellix Email Security protects against
advance threats and business email
compromise

Benchmark Assessments

Trellix Policy Auditor provides continuous
monitoring to verify configuration against
customer security benchmarks

XDR

Trellix XDR provides Open XDR capability
that detects threats using logs from
Defender and O365 applications as well
as Trellix security controls.

Forensics and OnPrem EDR

Trellix HX supplements Defender with
additional visibility and investigative
capability

Threat Intelligence

Trellix Insights provides contextual threat
indicators which can be imported into
Defender or other SOC tools

Data Security

Trellix Data Security covers
endpoint, network and databases