DRAGOS

ANOMALI

WEBINAR

FORTIFYING INFRASTRUCTURE:

An Intelligence-First Approach to Industrial Threats

Scott Dowsett
Global Field CTO
Anomali

Magpie Graham
Technical Director (Intel)
Dragos

AGENDA

1. INTRODUCTIONS
2. USING CYBER THREAT INTEL
3. UNDERSTANDING OT THREATS
4. ANALYZING ***YOUR*** OT THREATS
5. ASK QUESTIONS

INTRODUCTIONS

DRAGOS

The Dragos Platform offers the most effective industrial cybersecurity technology, giving customers visibility into their ICS/OT assets, vulnerabilities, threats, and response actions.

Magpie Graham
Technical Director (Intelligence)

ANOMALI

Anomali provides a Security Operations Platform powered by AI to Protect and Drive your business

Scott Dowsett
Global Field CTO

CYBER THREAT INTEL: MYTHS & TRUTHS

A continuous stream of unfiltered data from a single source

Research applicable to every industry or organization

Used for reacting to incidents after they have occurred

Evidence-based analysis of data collected from multiple data sources

Made relevant to specific industries and ***your*** organization

Used to take preemptive action and mitigate potential threats

WHERE TO GET INFORMATION ON CYBER THREATS

Global Threat Landscape

Adversaries, their tools, targets, and infrastructure

Data Sources: Commercial Cyber Threat Intelligence Providers, ISACs, Government Advisories, OSINT, Peer-to-Peer Sharing Networks, Joint Cybersecurity Operations, Partner Agreements

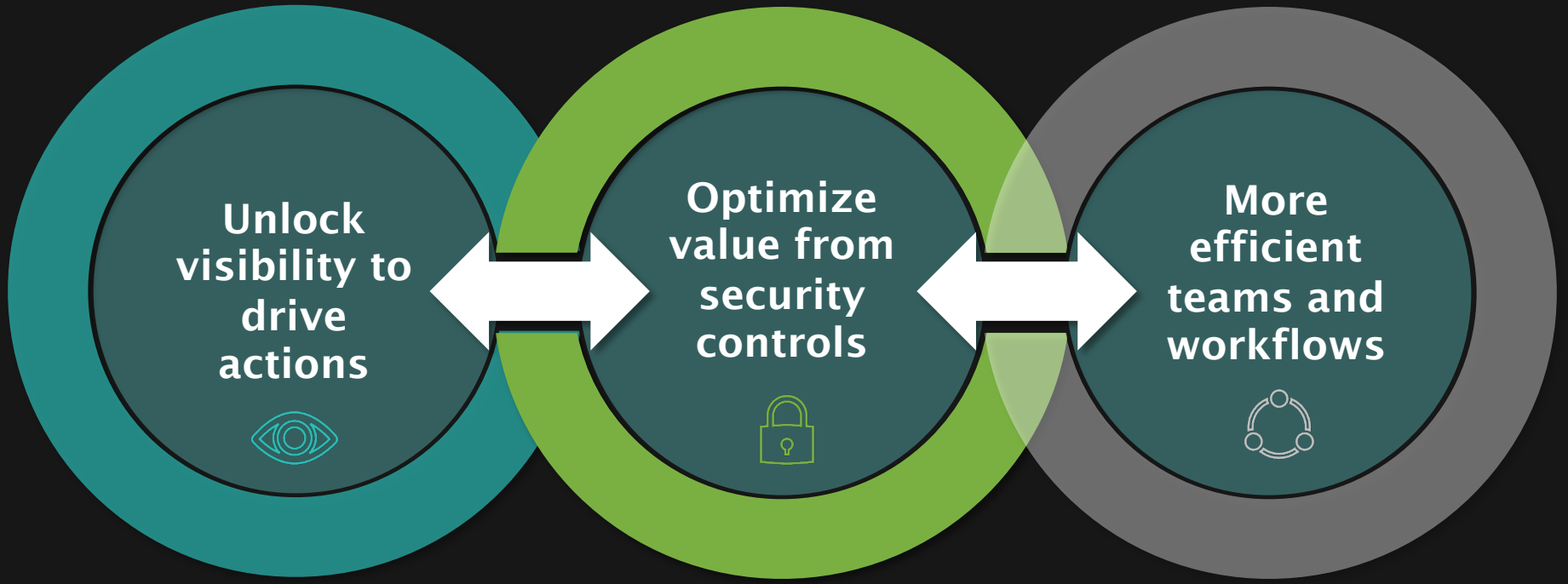
Local Threat Environment

Telemetry from all infrastructure and security functions

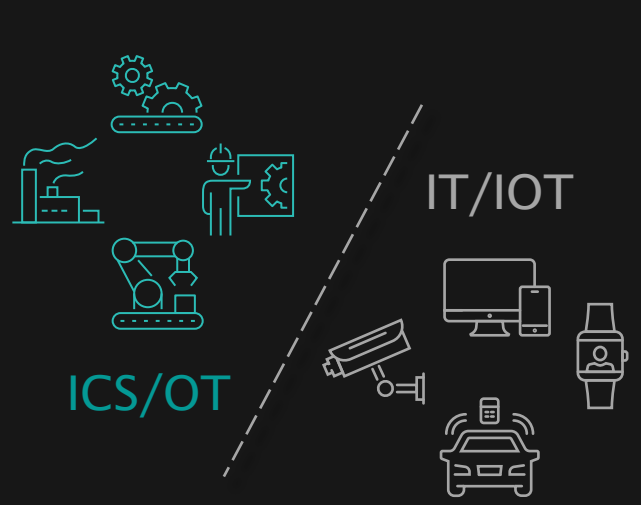
Data Sources: Network and Endpoint Traffic Data, Security Logs, Incident Reports, Any information that is generated internally

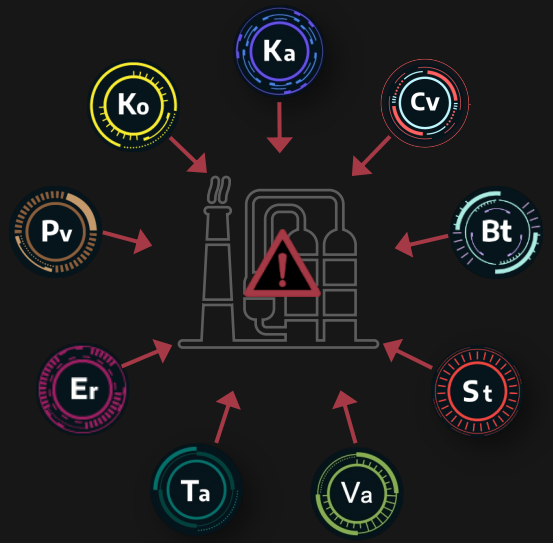
FINDING WHAT MATTERS TO YOU

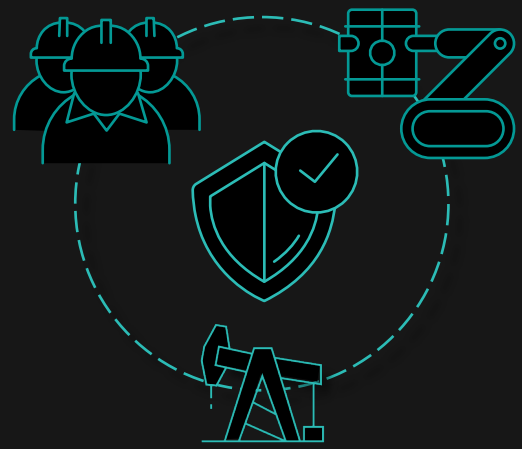
FINDING WHAT MATTERS TO YOU



OT THREATS ARE DIFFERENT THAN IT THREATS







ICS/OT Systems, Networks, & Vulnerabilities are Very Different from IT/IOT	Specialized Threat Groups Target ICS/OT Systems With TTPs Specific to the Environments	There Can Be Significant Impacts to Public Safety, Environment, & Revenue

UNDERSTANDING THE ICS CYBER KILL CHAIN

This is an example of a successful cyber attack on ICS.
These events occurred in Ukraine in 2016.

KAMACITE FACILITATED INITIAL ACCESS TO IT NETWORKS & PIVOT TO OT

Delivery	STAGE 1
Exploit	STAGE 1
Install/Modify	STAGE 1
C2	STAGE 1
Act	STAGE 1

ELECTRUM DEPLOYED CRASHOVERRIDE OT MALWARE DISRUPTING POWER TO ¼ MILLION HOMES

STAGE 2	Develop
STAGE 2	Test
STAGE 2	Deliver
STAGE 2	Install / Modify
STAGE 2	Execute ICS Attack

KAMACITE

CAPABLE OF STAGE 1: INITIAL ACCESS, PIVOT TO OT

February 2022

CYCLOPS BLINK targeting vulnerabilities in small/home office devices

April

WatchGuard firewall & router devices

ASUS firewall & router devices

May

Targets another set of routers & IP cameras for initial network access (outside of CYCLOPS BLINK operations)

June

Communication with the same oblenergo targeted in a 2015 Ukraine cyber attack

2023

KAMACITE was observed utilizing DarkCrystal malware to conduct reconnaissance

The compromise of IT networks can lead to future impacts on OT environments.

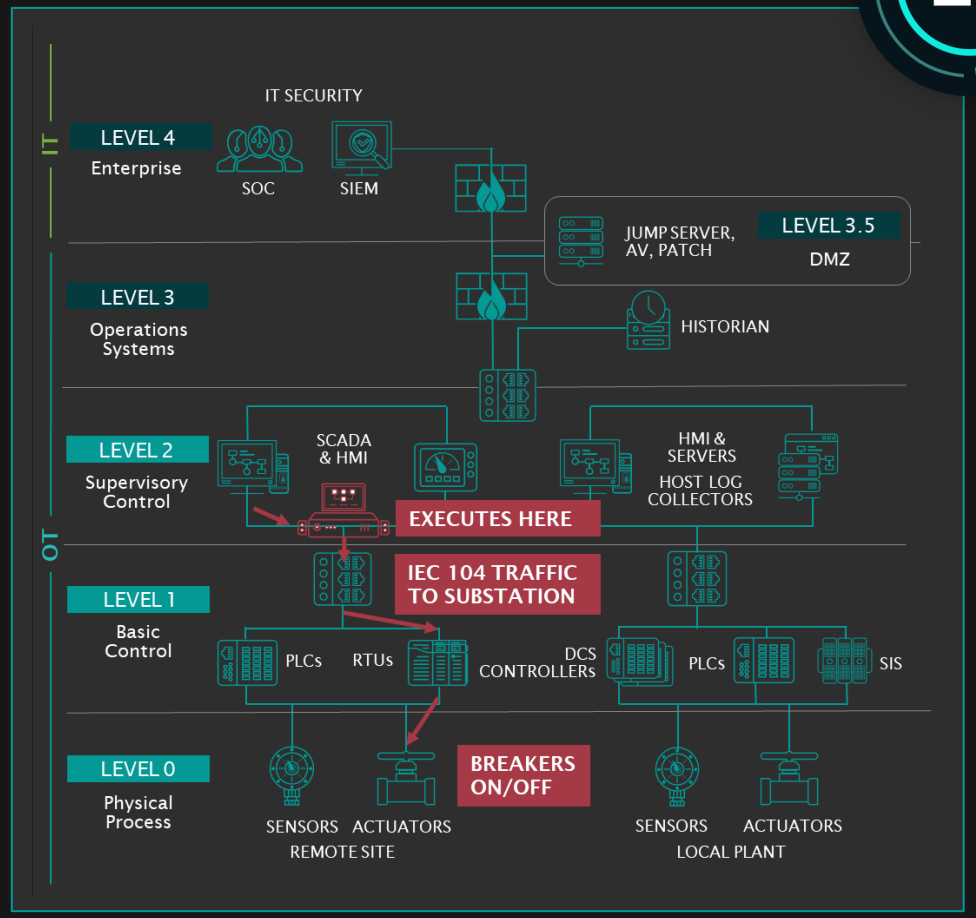
ELECTRUM

CAPABLE OF STAGE 2: EXECUTING ICS ATTACKS

In April 2022 malware is uncovered at a Ukrainian utility provider

The malware is a variant of CRASHOVERRIDE, used in the 2016 attack by ELECTRUM

Wiper malware is also deployed: CADDYWIPER, ORCSHRED, SOLOSHRED, & AWFULSHRED

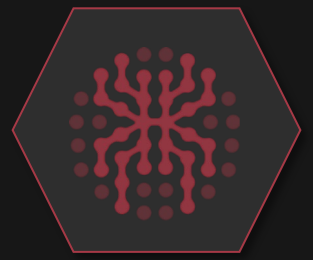


XENOTIME

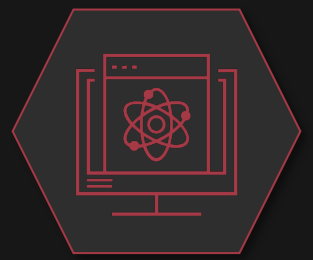
CONDUCTING STAGE 1 ACTIVITIES, CAPABLE OF STAGE 2 ATTACKS

Now ----------→ Then

Reconnaissance focused on oil & natural gas (ONG), liquified natural gas (LNG) industries



Heavy use of off-the-shelf tools & open-source information



Currently in the development phase, continues to target downstream & midstream ONG/LNG with a focus on pipeline, maritime, refining

TRISIS Malware, 2017

- Delivered to an industrial facility in the Middle East
- Targeted Safety Instrumented System (SIS) and failed causing a stop in operations
- First malware to specifically target human life

RANSOMWARE: #1 CYBER THREAT

CASCADING IMPACTS FOR INDUSTRIAL ORGANIZATIONS, PARTICULARLY MANUFACTURERS

- Ransomware chiefly not explicitly targeting OT
- In flat networks, ransomware can spread more easily to OT
- Precautionary shutdowns due to lack of preparation
- Supply chain impacts
- Potential unforeseen consequences
- Greater risk to loss of life

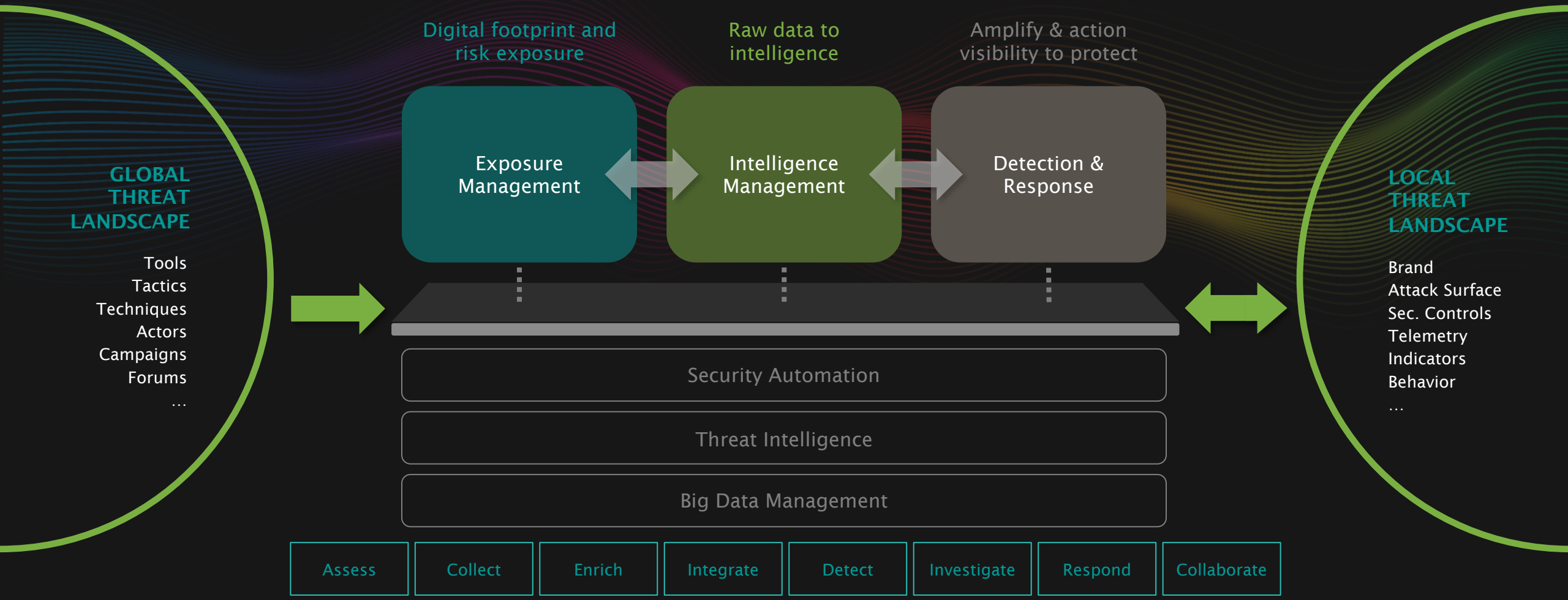
RANSOMWARE DEPLOYED TO LEGACY SERVERS & COMPUTERS

4 OT PRODUCTION FACILITIES TEMPORARILY SHUT DOWN

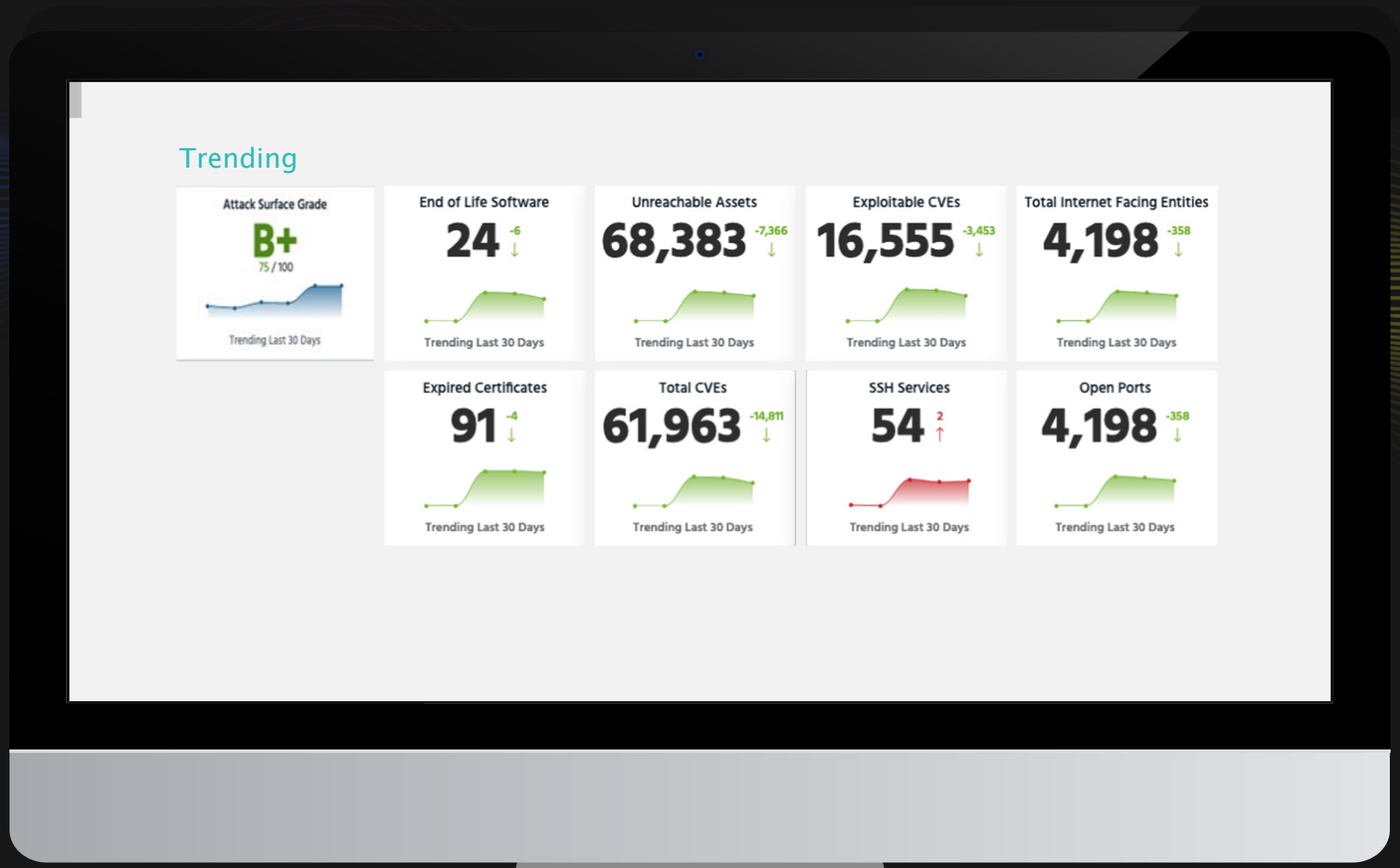
Delays and shortages of salad kits for more than a week

COSTS FROM THIS ATTACK EXCEEDED $10 MILLION

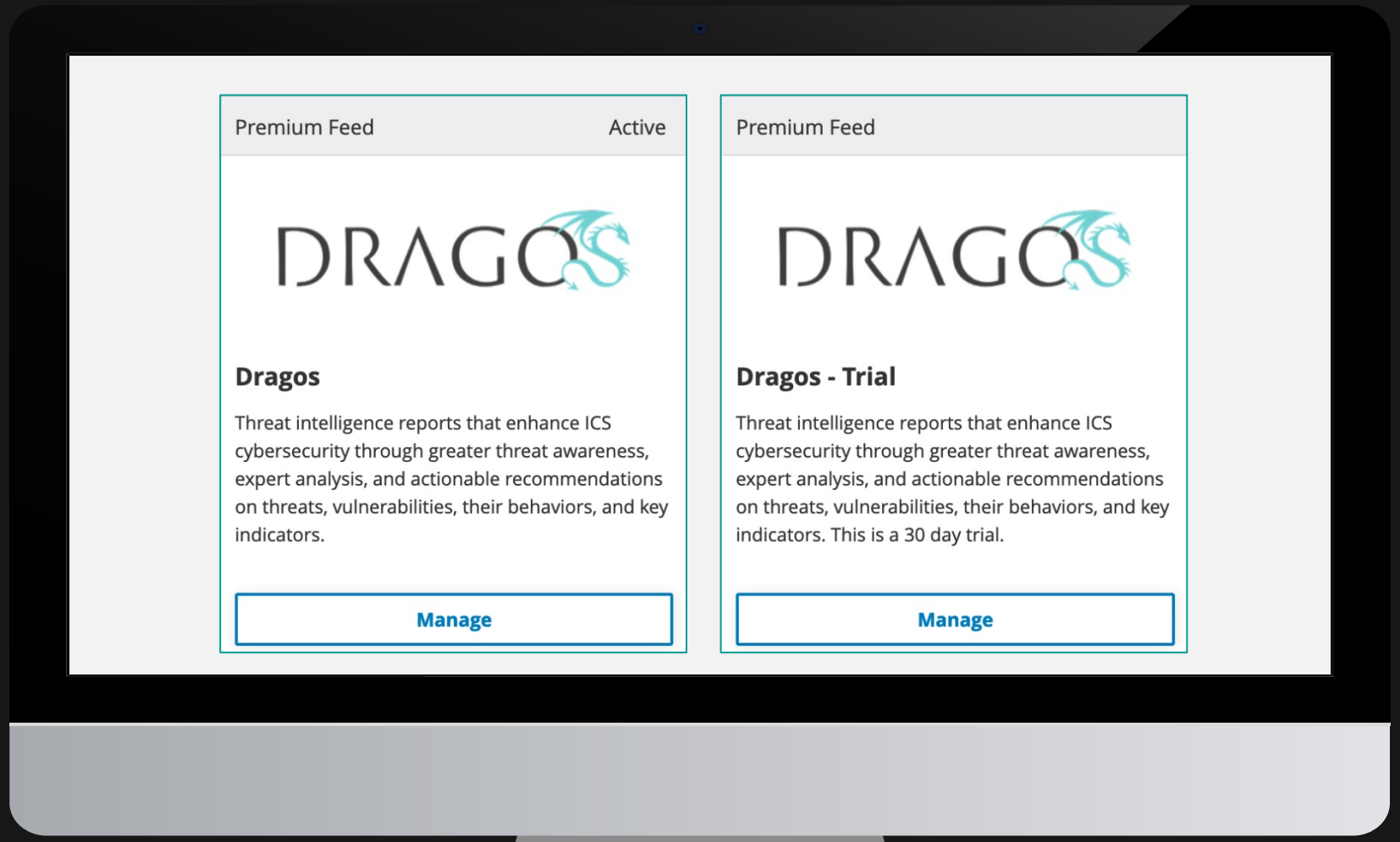
OPERATIONALIZING OT THREAT INTEL



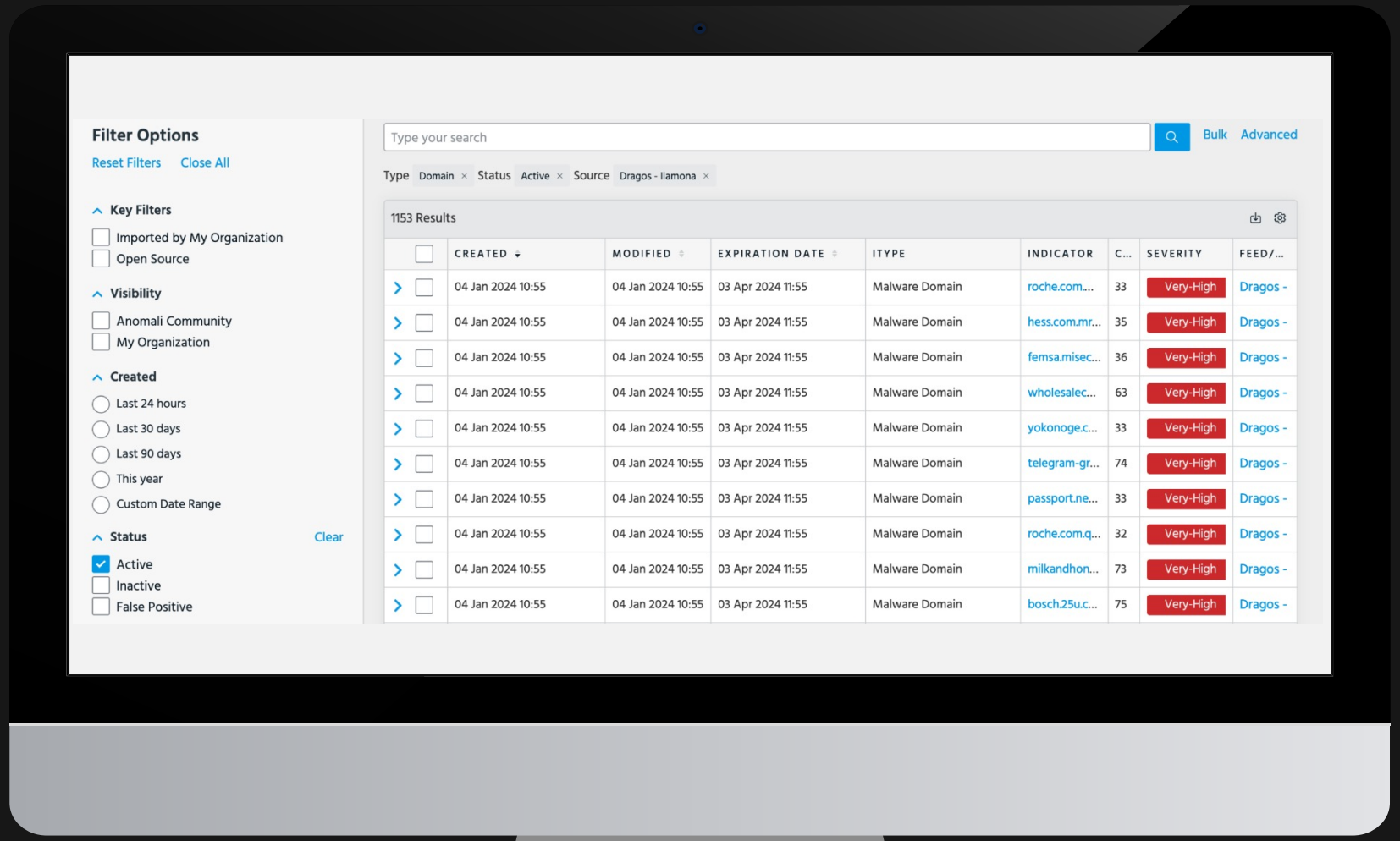
ANOMALI ATTACK SURFACE MANAGEMENT



ANOMALI APPSTORE — DRAGOS



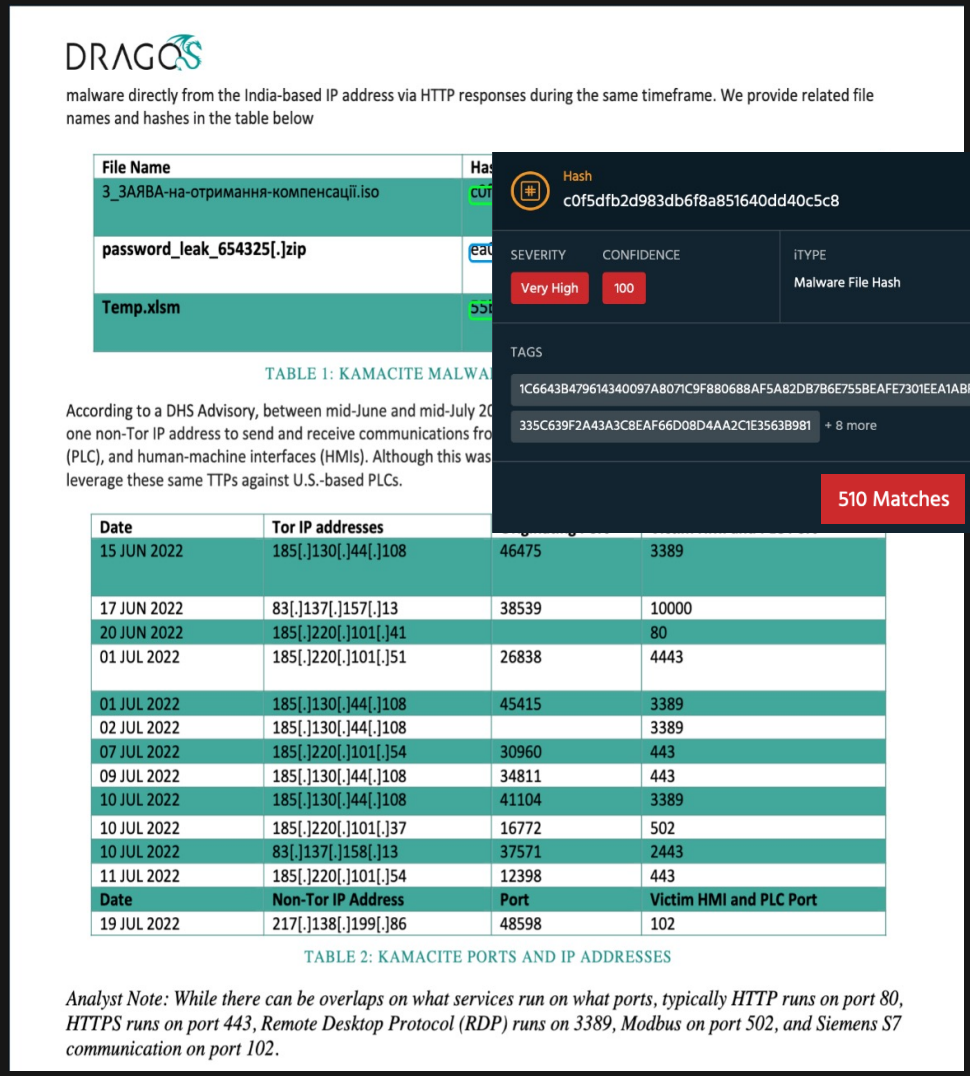
EXAMPLE DRAGOS INDICATORS IN ANOMALI



AN EXAMPLE WORKFLOW: “ARE WE AFFECTED?”

- You hear about a new threat – “Are we affected?”
- Skim the article and identify key terms, indicators, and TTPs
- Research threat actors, malware families, vulnerabilities, etc
- Extract and validate IOCs
- Search logs to validate presence for X weeks/months…
- Expand the search for other associated indicators and repeat
- Trigger response, remediation, and cleanup

ELAPSED TIME:
1 WEEK - 1+ MONTH



DRAGOS

malware directly from the India-based IP address via HTTP responses during the same timeframe. We provide related file names and hashes in the table below

File Name	Has
3_ЗАЯВА-на-отримання-компенсації.iso	cUf
password_leak_654325[.]zip	eaU
Temp.xlsm	55t

TABLE 1: KAMACITE MALWA

According to a DHS Advisory, between mid-June and mid-July 20
one non-Tor IP address to send and receive communications fro
(PLC), and human-machine interfaces (HMIs). Although this was
leverage these same TTPs against U.S.-based PLCs.

Date	Tor IP addresses		
15 JUN 2022	185[.]130[.]44[.]108	46475	3389
17 JUN 2022	83[.]137[.]157[.]13	38539	10000
20 JUN 2022	185[.]220[.]101[.]41		80
01 JUL 2022	185[.]220[.]101[.]51	26838	4443
01 JUL 2022	185[.]130[.]44[.]108	45415	3389
02 JUL 2022	185[.]130[.]44[.]108		3389
07 JUL 2022	185[.]220[.]101[.]54	30960	443
09 JUL 2022	185[.]130[.]44[.]108	34811	443
10 JUL 2022	185[.]130[.]44[.]108	41104	3389
10 JUL 2022	185[.]220[.]101[.]37	16772	502
10 JUL 2022	83[.]137[.]158[.]13	37571	2443
11 JUL 2022	185[.]220[.]101[.]54	12398	443
Date	**Non-Tor IP Address**	**Port**	**Victim HMI and PLC Port**
19 JUL 2022	217[.]138[.]199[.]86	48598	102

TABLE 2: KAMACITE PORTS AND IP ADDRESSES

Analyst Note: While there can be overlaps on what services run on what ports, typically HTTP runs on port 80, HTTPS runs on port 443, Remote Desktop Protocol (RDP) runs on 3389, Modbus on port 502, and Siemens S7 communication on port 102.

Hash
c0f5dfb2d983db6f8a851640dd40c5c8
Active

SEVERITY: Very High
CONFIDENCE: 100
iTYPE: Malware File Hash

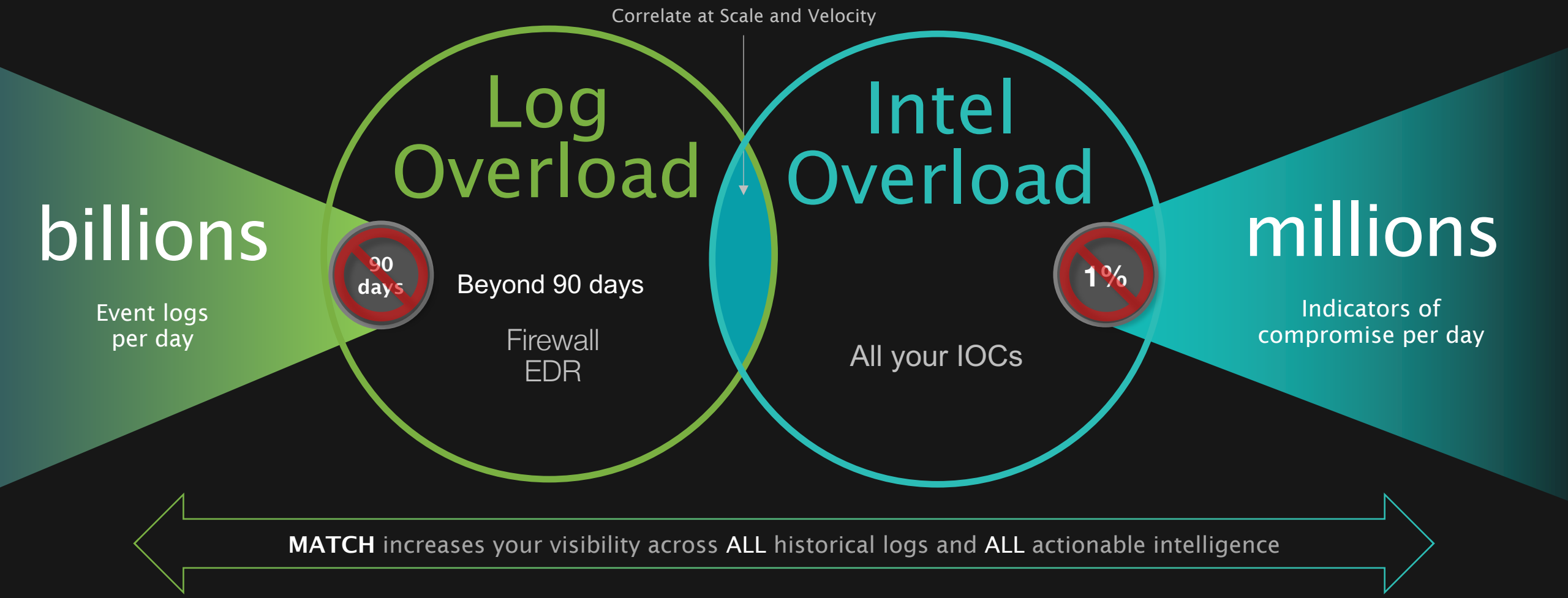
TAGS
1C6643B479614340097A8071C9F880688AF5A82DB7B6E755BEAFE7301EEA1ABF
335C639F2A43A3C8EAF66D08D4AA2C1E3563B981 + 8 more

510 Matches | Details

- You hear about a new threat – “Are we affected?”
- Use Lens+ to immediately scans the article, extract associated indicators, actors, TTPs
- Lens+ also correlates against logs in Match, going back several years
- Send indicators to security controls via Anomali Integrator, integrate with ticketing systems to trigger investigations and response

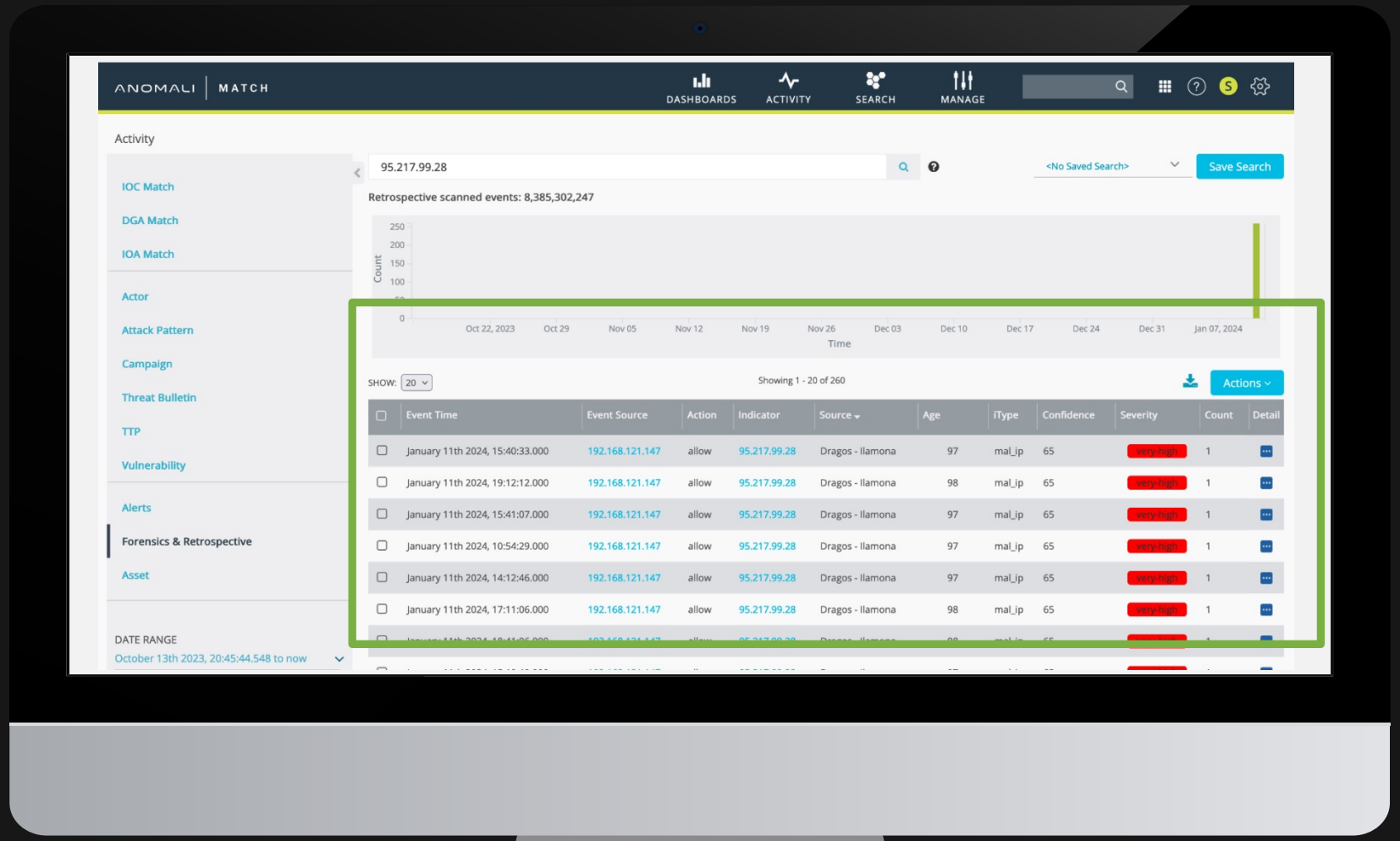
ELAPSED TIME:
15 SECONDS – 5 MINUTES

ANOMALI MATCH PROVIDING FULL VISIBILITY

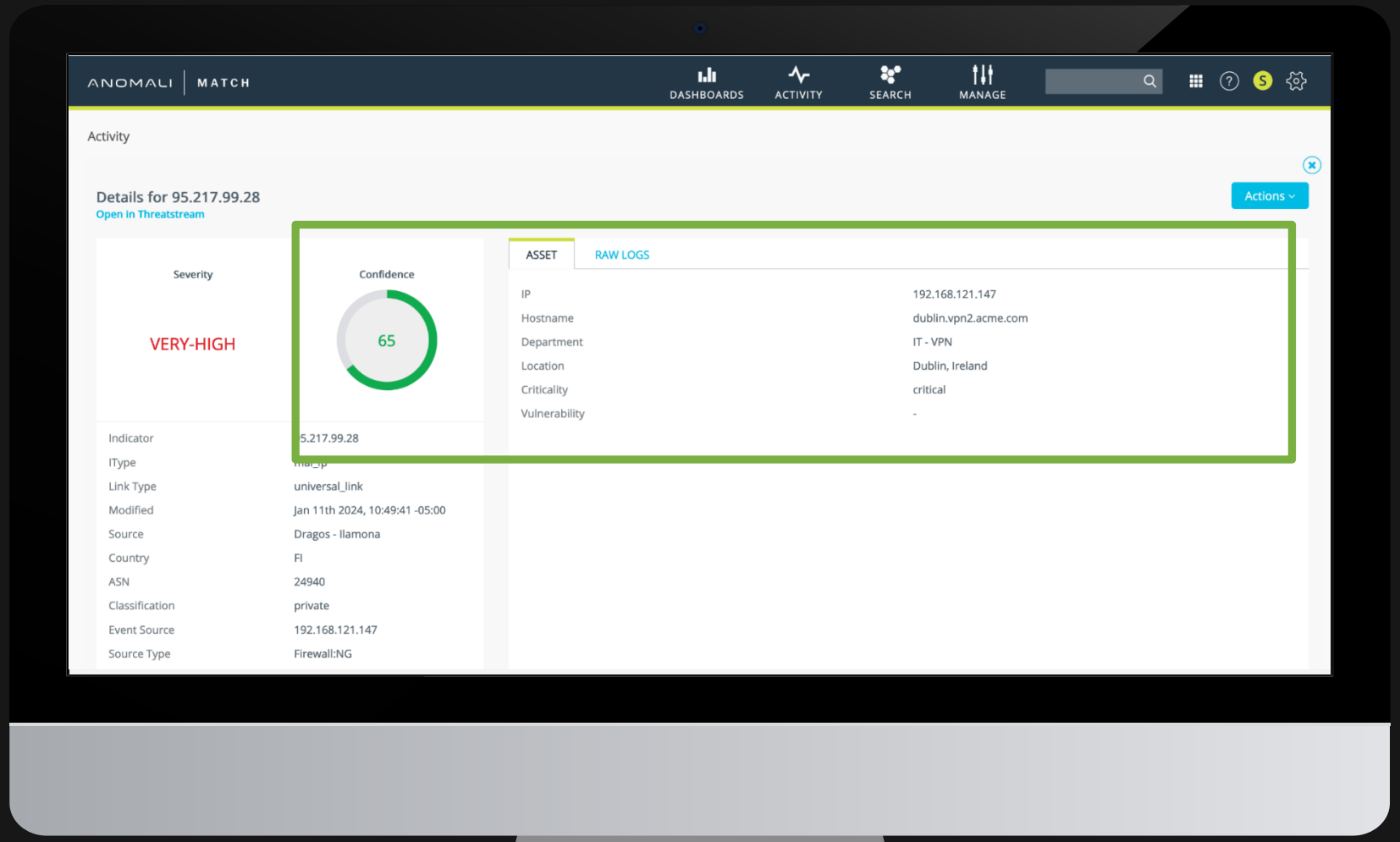


MATCH increases your visibility across **ALL** historical logs and **ALL** actionable intelligence

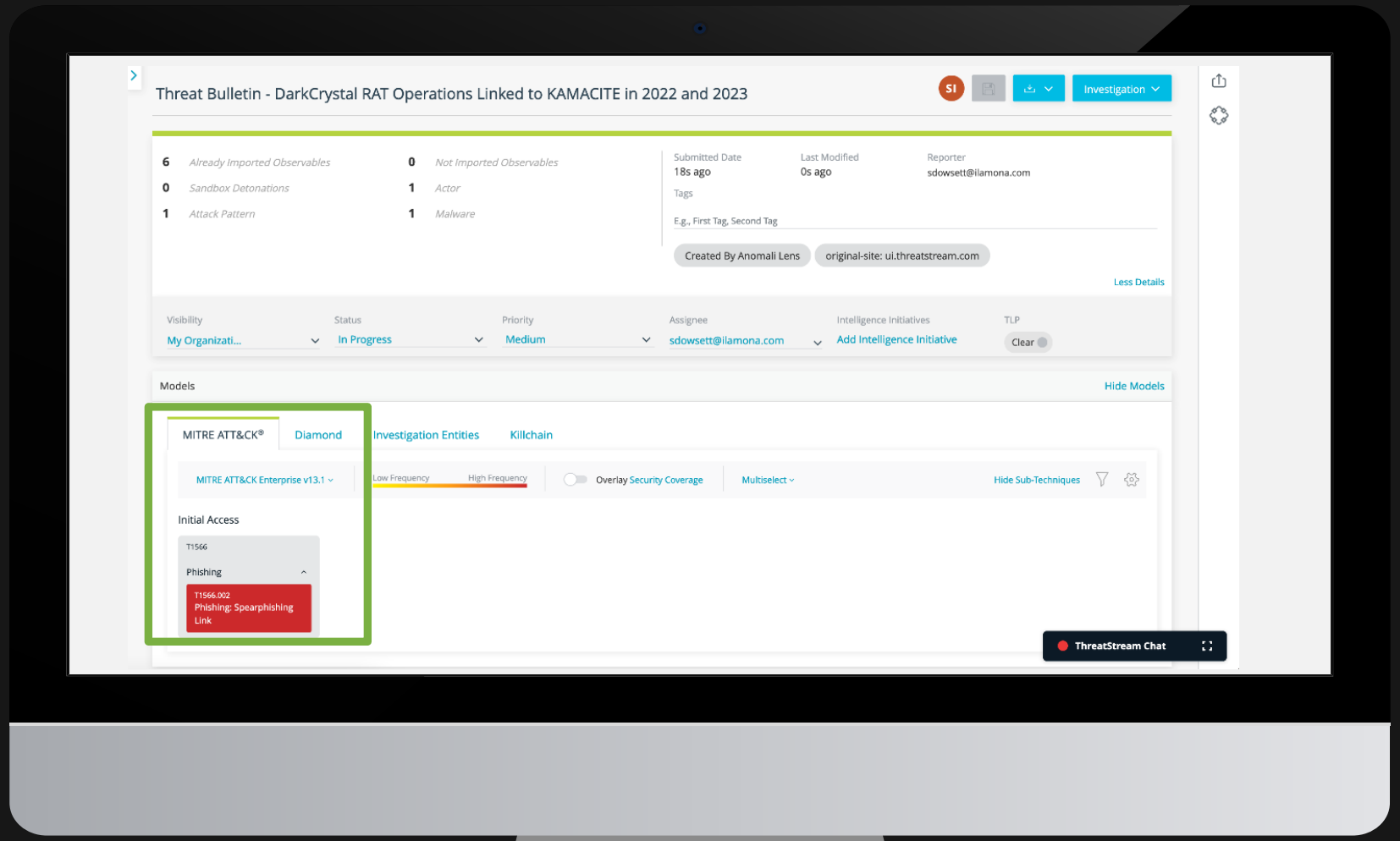
ANOMALI MATCH — CORRELATION DRAGOS



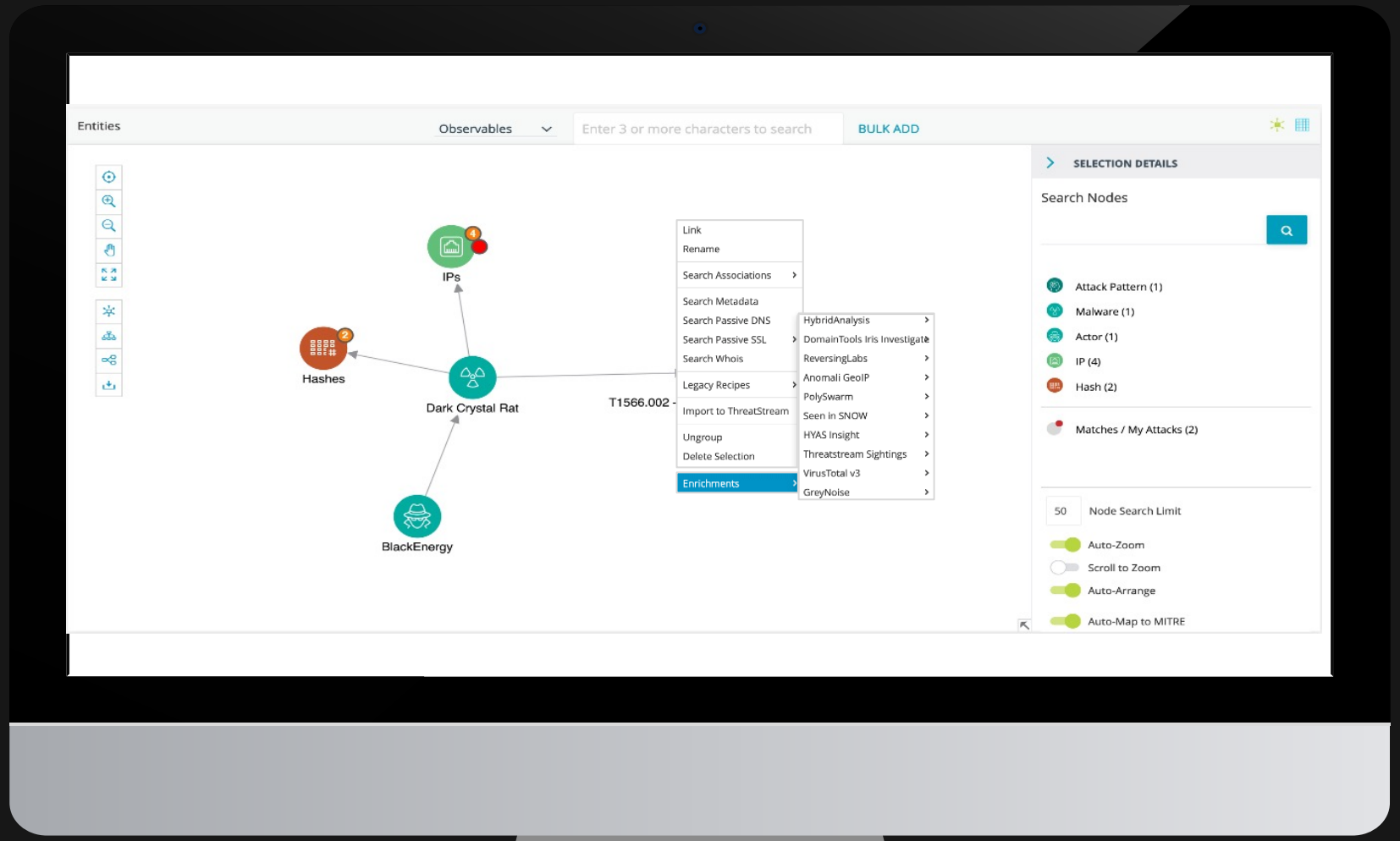
ANOMALI MATCH — ASSET DETAILS



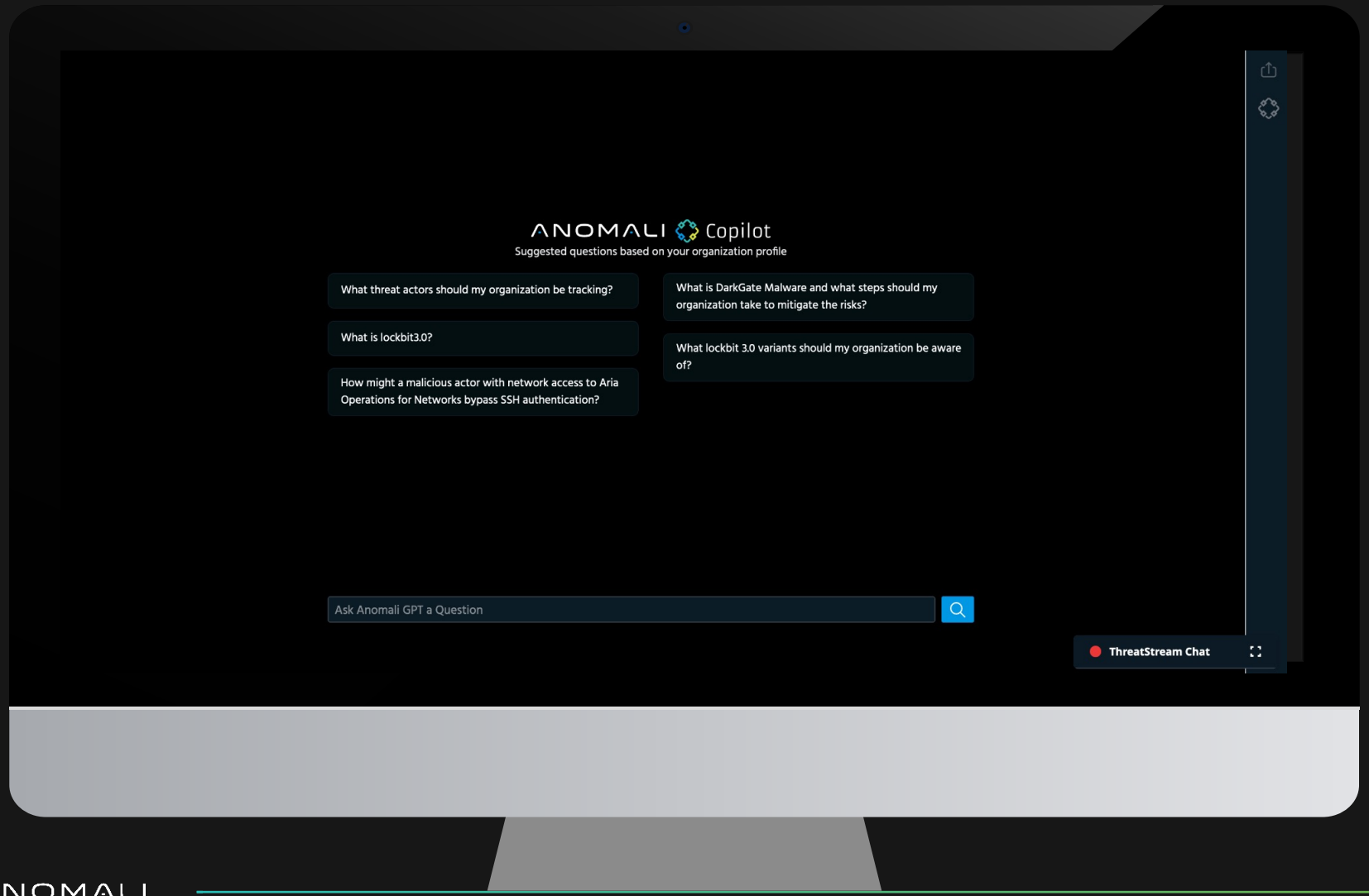
ANOMALI INVESTIGATE



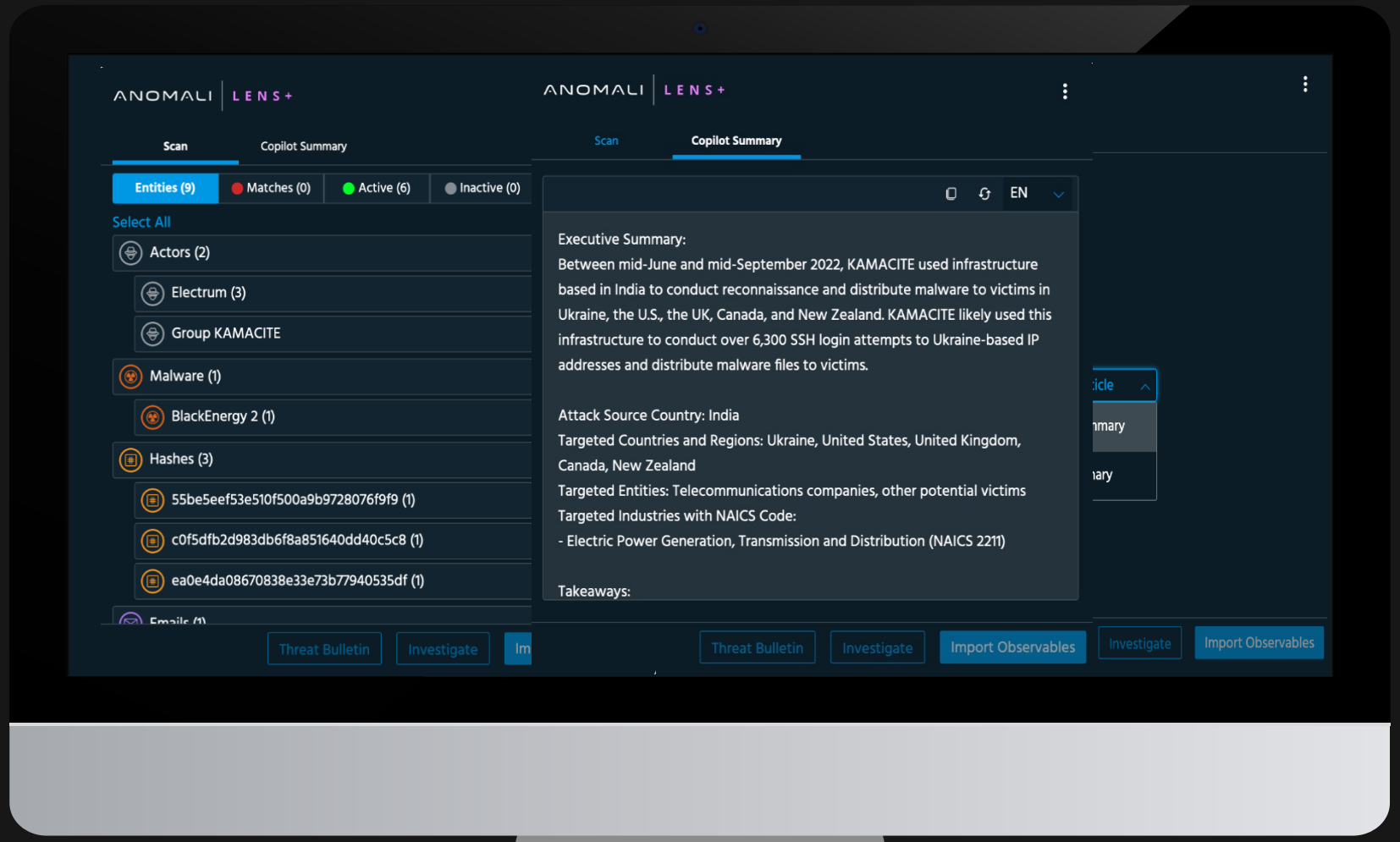
ANOMALI INVESTIGATE



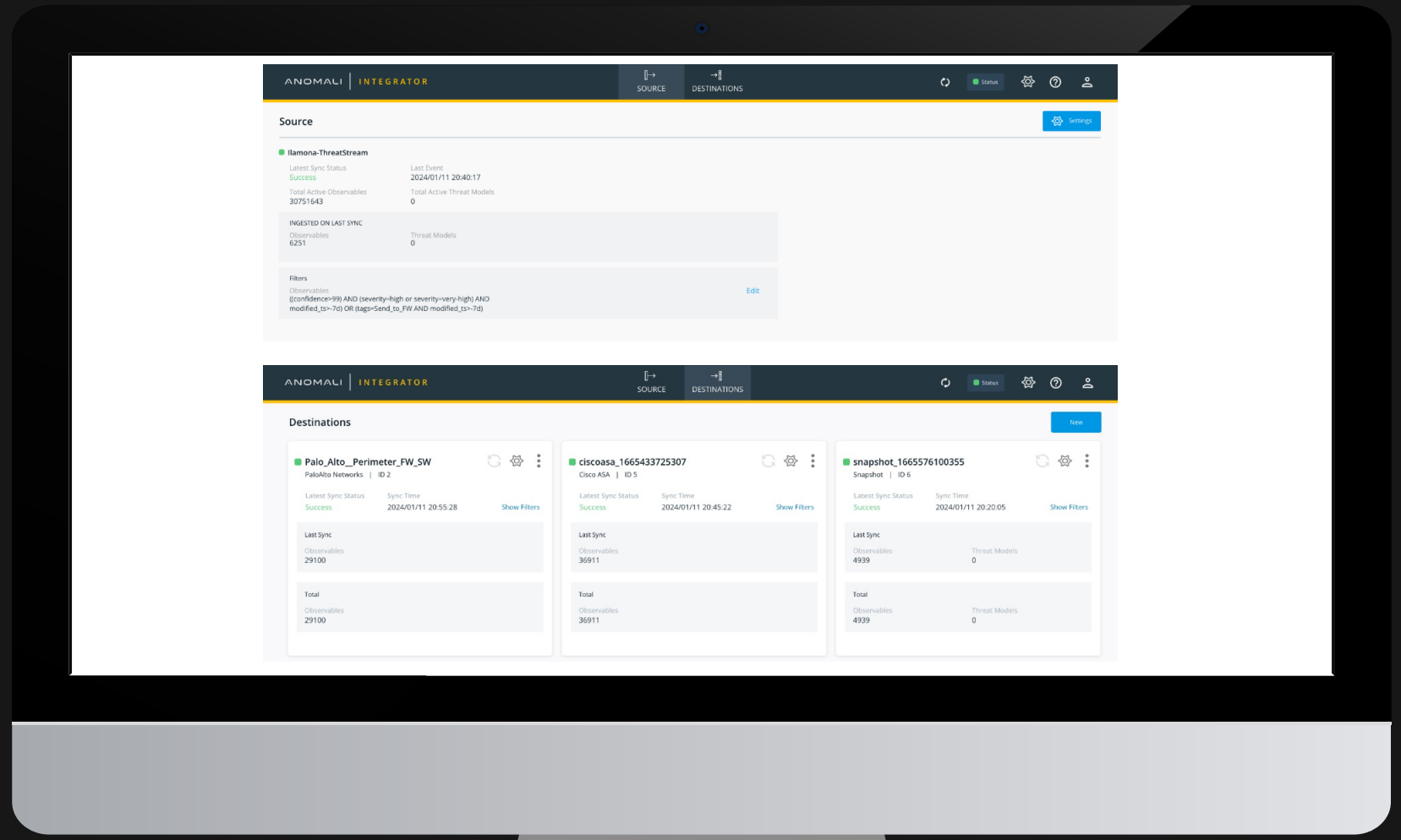
ANOMALI COPILOT



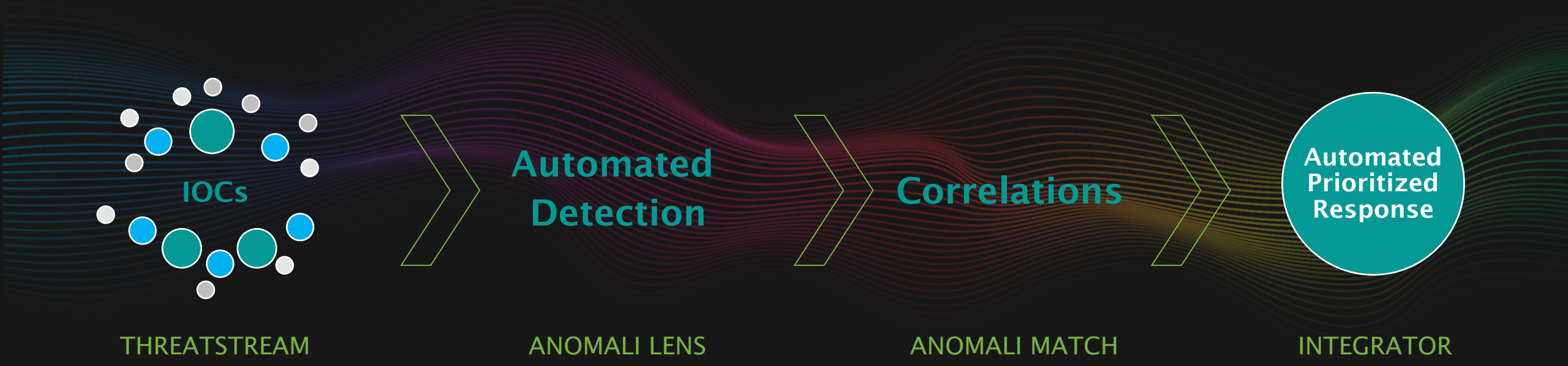
ANOMALI COPILOT IN LENS



ANOMALI INTEGRATOR — REMEDIATION



ANOMALI — AUTOMATION



Alerts Processed Per Analyst: 1000s+
Time to Process Alerts: Seconds

TAKEAWAY & RECOMMENDATIONS

OT threats are unique, as are the systems, vulnerabilities, and impacts in OT.

Dragos provides **OT specific threat intelligence**, but your threat intelligence will come from multiple sources

You need to **consolidate data from multiple sources** including OT threat intel and then **find what matters to you** in Anomali.

QUESTIONS AND ANSWERS

DRAGOS | ANOMALI

THANK YOU!