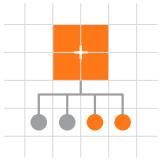
Argos™ Forensic Canvas

Visualizing Cyber Investigations

Cyberint

Data is everywhere today; on the surface, it might seem like all this data would make reaching optimal resolutions to investigations much simpler and faster. But in truth, the fractured and siloed nature of data means that it can be almost impossible to correlate events and extract meaningful insights. While organizations go to great lengths to gather data to help them get deeper understanding into events and indicators, much of this data will never be put to real use.



FORENSIC CANVAS
UNCOVER WHAT LIES BENEATH

Data that goes unmined is as good as useless.

Analysts need the right tools to help them uncover relationships between disparate data points and contextualize threats. Forensic Canvas, part of the Argos™ Platform, gives analysts all the tools and enriched data needed to triage and research IOCs (indicators of compromise) in an automated, visual, and intuitive manner.

By leveraging multiple sources of information via Cyberint's open-source Threat Intelligence capabilities, with comprehensive coverage of Darknet, Deep web, and open-net marketplaces, as well as hacking forums, pastebins, chat rooms, closed forums and additional sources, Forensic Canvas discovers and visually displays previously unknown connections, attack vectors, and related threat actors, enabling analysts to unmask the true identities and sources behind IOCs.

With the click of a button, analysts can leverage the canvas to expand IOCs to other known connections using sources such as:

- **NEWLY REGISTERED DOMAIN DISCOVERY**
- **EXTENDED WHOIS DATABASE SEARCHES**
- **PASSIVE DNS REPOSITORIES**
- **MALICIOUS FILE HASH REPOSITORIES**
- **AUTOMATIC DISCOVERY OF SOCIAL NETWORKS**

With the Forensic Canvas, analysts can identify and respond to emerging threats before they hit the network, to proactively detect breaches and attacks. It's the key to reducing the time to respond and stopping threats before they become harmful incidents.

Cyberint

WITH FORENSIC CANVAS, ANALYSTS CAN:

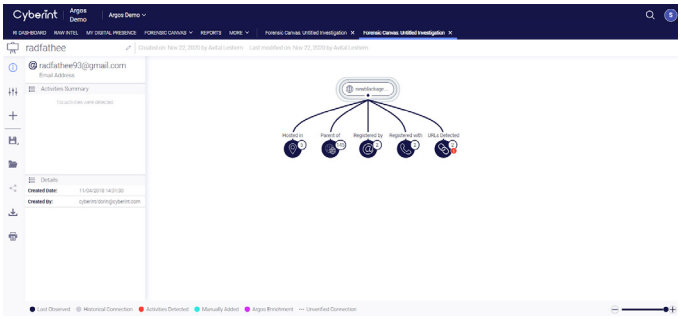
- FOCUS ON NEWLY FOUND IOCS DURING INVESTIGATIONS
- EXPLORE METADATA ON ALL CONNECTED ASSETS TO IMMEDIATELY UNDERSTAND RELEVANCE TO THE CURRENT INVESTIGATION
- MANUALLY ADD ADDITIONAL INFORMATION TO FIND POTENTIAL CONNECTIONS BETWEEN SEEMINGLY UNRELATED ENTITIES
- UNDERSTAND RELATIONSHIPS TO THE CURRENT INVESTIGATION IN AN ACTIONABLE AND INTUITIVE WAY
- BUILD A THREAT ACTOR PROFILE THAT INCLUDES A TIMELINE OF MALICIOUS ACTIVITIES

HOW DOES IT WORK?

The Forensic Canvas dashboard seamlessly correlates and displays rich visual insights that can be put to use instantly to enhance and support analyst efforts. Here is how it works:

1

START WITH AN IOC ANDAUTOMATICALLY DISCOVER IMMEDIATE CONNECTIONS

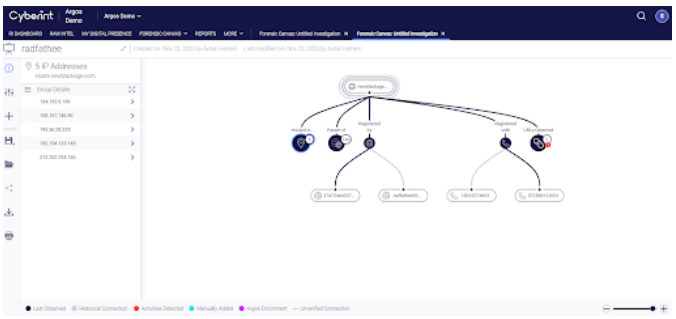


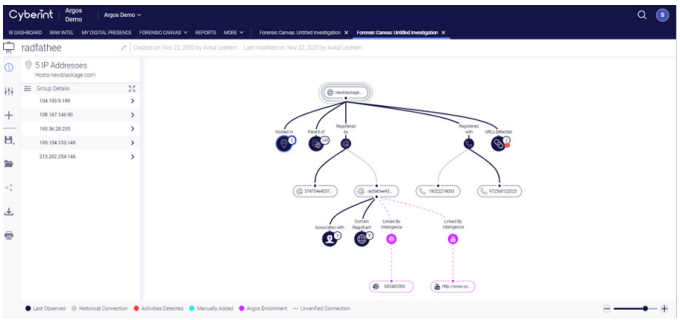
2

EXPAND TO INVESTIGATE THE ATTACK INFRASTRUCTURE

3

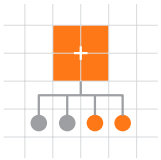
PROFILE AND IDENTIFY ANY THREAT ACTORS





4

REVIEW THE ENHANCED INTELLIGENCE FROM MULTIPLE DATA SOURCES, INCLUDING ARGOS™ THREAT INTELLIGENCE ENRICHMENT



FORENSIC CANVAS
HELPING ANALYSTS SEE DEEPER, UNCOVER MORE

With Forensic Canvas, you analysts can transform siloed, independent data points into genuine insights, yielding better, faster, and more optimal decisions. To learn more about Forensic Canvas, contact us.

> *We are drowning in information, while starving for wisdom.*
>
> E.O. Wilson

FROM OUR CUSTOMERS

> *Forensic Canvas reveals the deeper story and the relationships behind seemingly independent data points. This enriched perspective gives our team the insights we need to make optimal decisions and mitigate events before damage is done."*

IN SUMMARY:

- **Research and investigate specific IOCs: IPs, Domains, Threat Actors, etc.**
- **Get robust visualization capabilities for triage and incident response**
- **Use automatic tools to discover relationships and additional data, per IOC investigated**
- **Extended coverage for newly registered domains, passive DNS, malicious file hashes, social network accounts, etc.**

USE CASES:

- **ATTACK INFRASTRUCTURE INVESTIGATION**

  GAIN DEEP VISIBILITY INTO METHODS, MALWARE, ENTITIES, AND THEIR RELATIONSHIPS FOR ENHANCED UNDERSTANDING

- **THREAT ACTOR PROFILING AND IDENTIFICATION**

  AUTOMATICALLY GATHER INFORMATION THROUGH THREAT INTELLIGENCE AND SOCIAL MEDIA DISCOVERY

- **COLLECTION OF THREAT DETAILS FOR CURRENT AND FUTURE REFERENCE**

  CLASSIFY SPECIFIC ATTACKS BASED ON TECHNICAL DETAILS, CHARACTERISTICS, AND BEHAVIORS, AND ASSIGN TO THREAT ACTOR GROUPS AND CERTAIN INDUSTRIES FOR FUTURE USES

CONTACT US

https://www.cyberint.com | sales@cyberint.com | https://blog.cyberint.com

USA
214 W 29th St
New York, 10001
Tel: +1-646-568-7813

Israel
17 Ha-Mefalsim St
4951447 Petah Tikva
Tel: +972-37-286-777

United Kingdom
6 The Broadway, Mill Hill
NW7 3LL, London
Tel: +44-203-514-1515

France
67 Avenue de Wagram
75008 Paris
Tel: +33 1 77 50 58 91

Singapore
135 Cecil St. #10-01
MYP PLAZA 069536
Tel: +65-3163-5760

Cyberint