透過知識圖介面掌握數據關聯後的關鍵資安含義

Henry Hu / CTO

GEMINI

GEMINI DATA

GEMINI

The Pain Points

DATA COLLECTION

Collect necessary security logs and machine data from your environment. Including network, endpoint, authentication, and web activity data. Move these critical activity logs to a location that cybercriminals can't easily access.

DATA NORMALIZATION

Apply a standard security taxonomy. Fields with common values like user timestamp, name, source IP address, and port have common names regardless of who created them or what device was used.

EXPANSION

Collect additional data that unlocks new capabilities. This builds a foundation for the advanced detection capabilities and contextual insights that will identify patterns and correlations in your security data.

ENRICHMENT

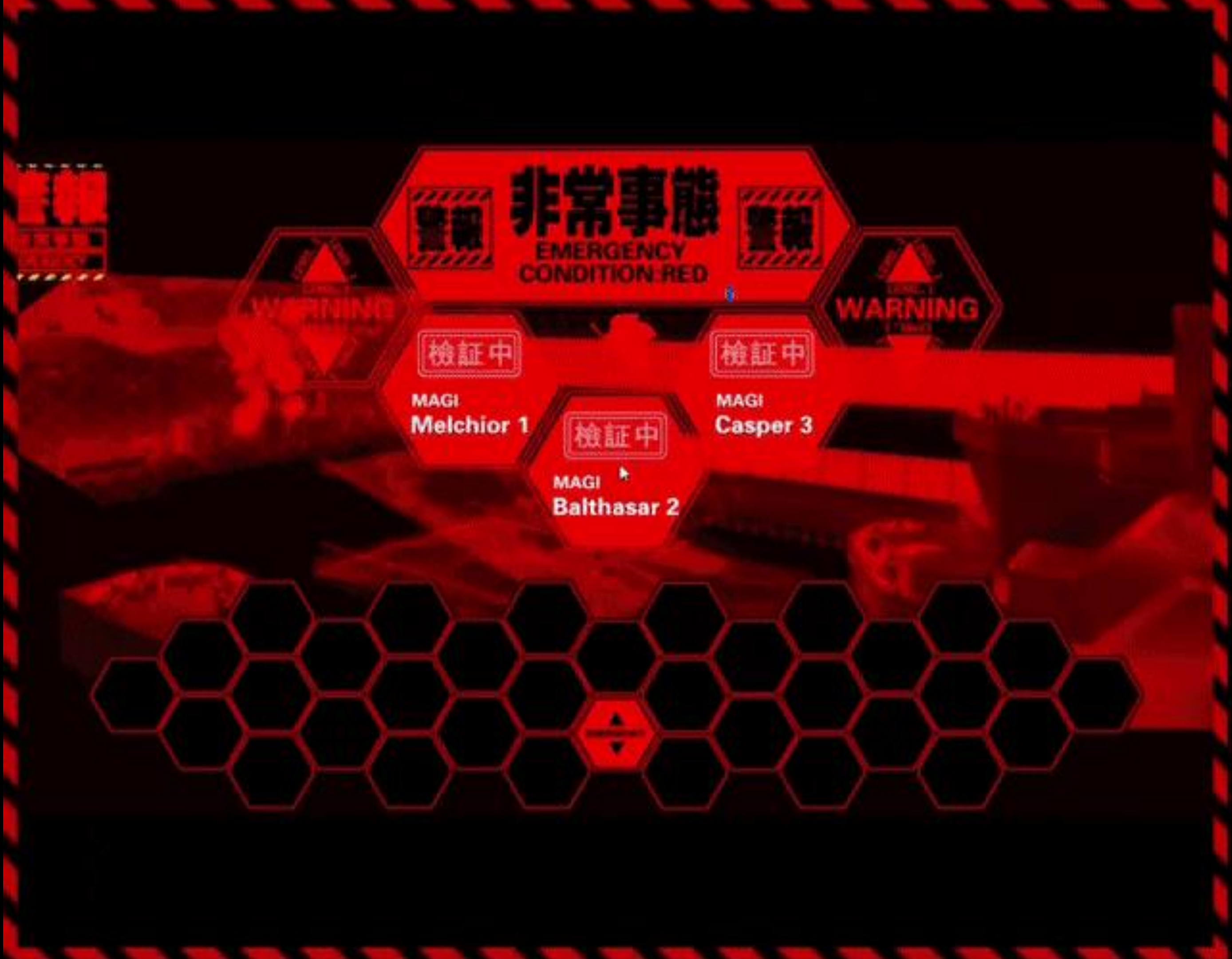
Augment the security data you've collected with data from internal sources like business tools, website data, logs, and access controls and external sources like open-source and threat-intelligence feeds, machine data, etc.

AUTOMATE & STANDARDIZE

Cybersecurity success hinges on automation. Organizations not only need actionable insights in real-time, but they also need to be able to automate tasks.

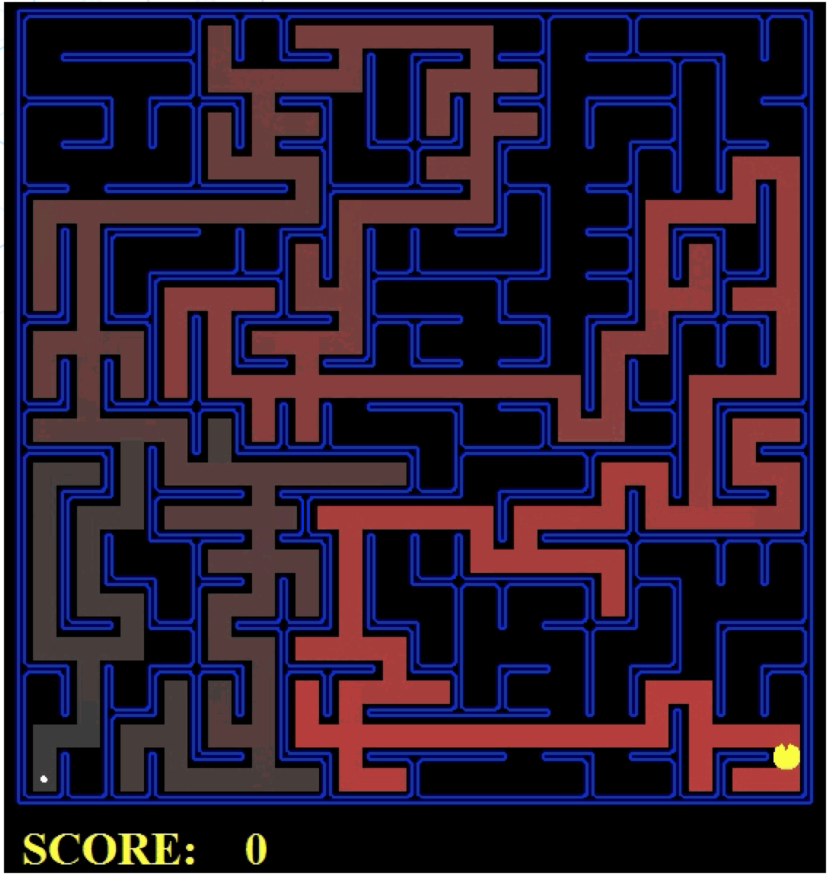
ADVANCED DETECTION

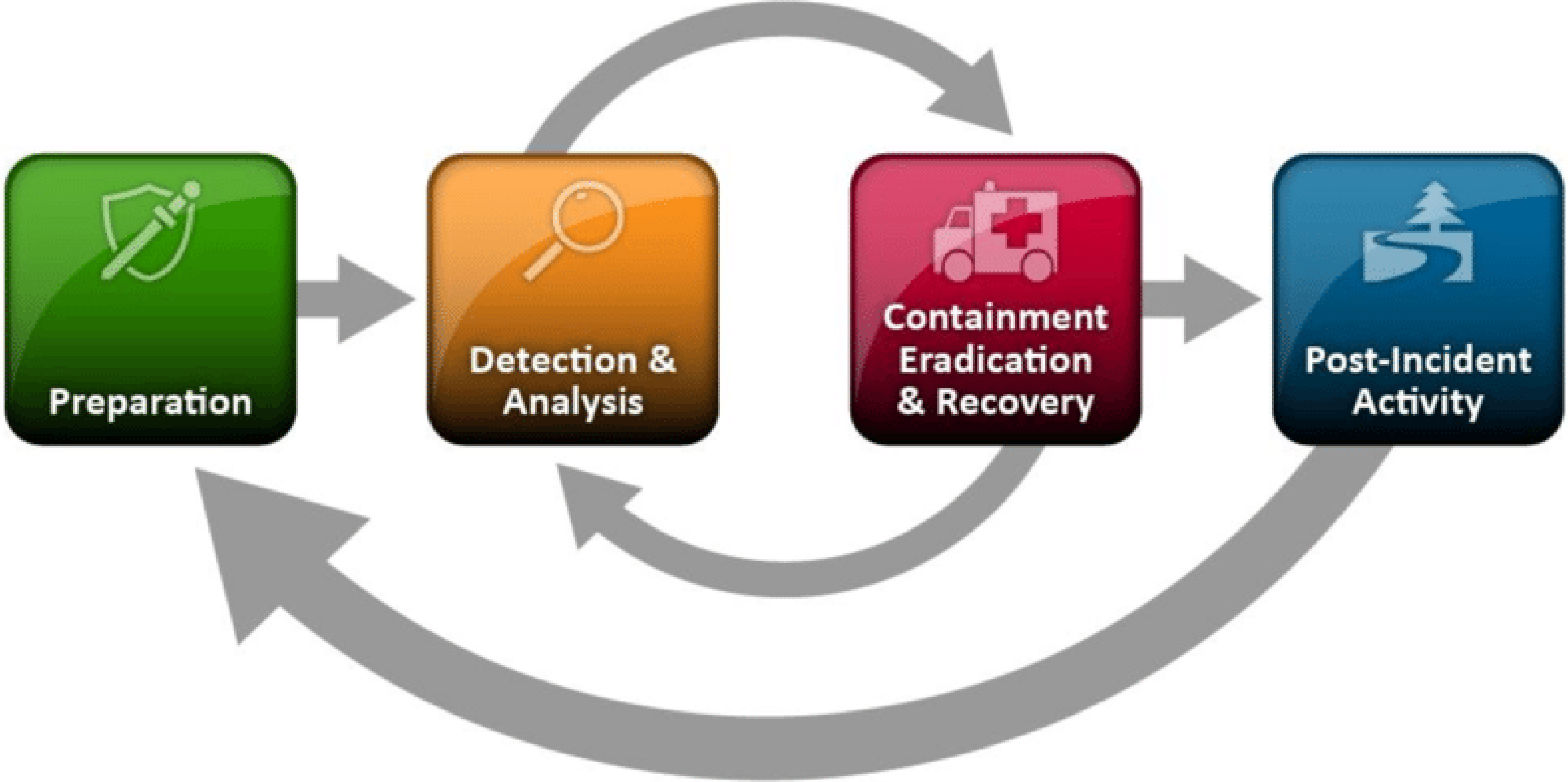
This stage will be aligned to the identified risks that harm your business, and teams should prioritize performing new research, refining queries, and building on existing capabilities.



警報
非常事態
EMERGENCY
CONDITION:RED
警報
警報
WARNING
WARNING
檢証中
MAGI
Melchior 1
檢証中
MAGI
Casper 3
檢証中
MAGI
Balthasar 2

Investigation - Finding the Path On Time





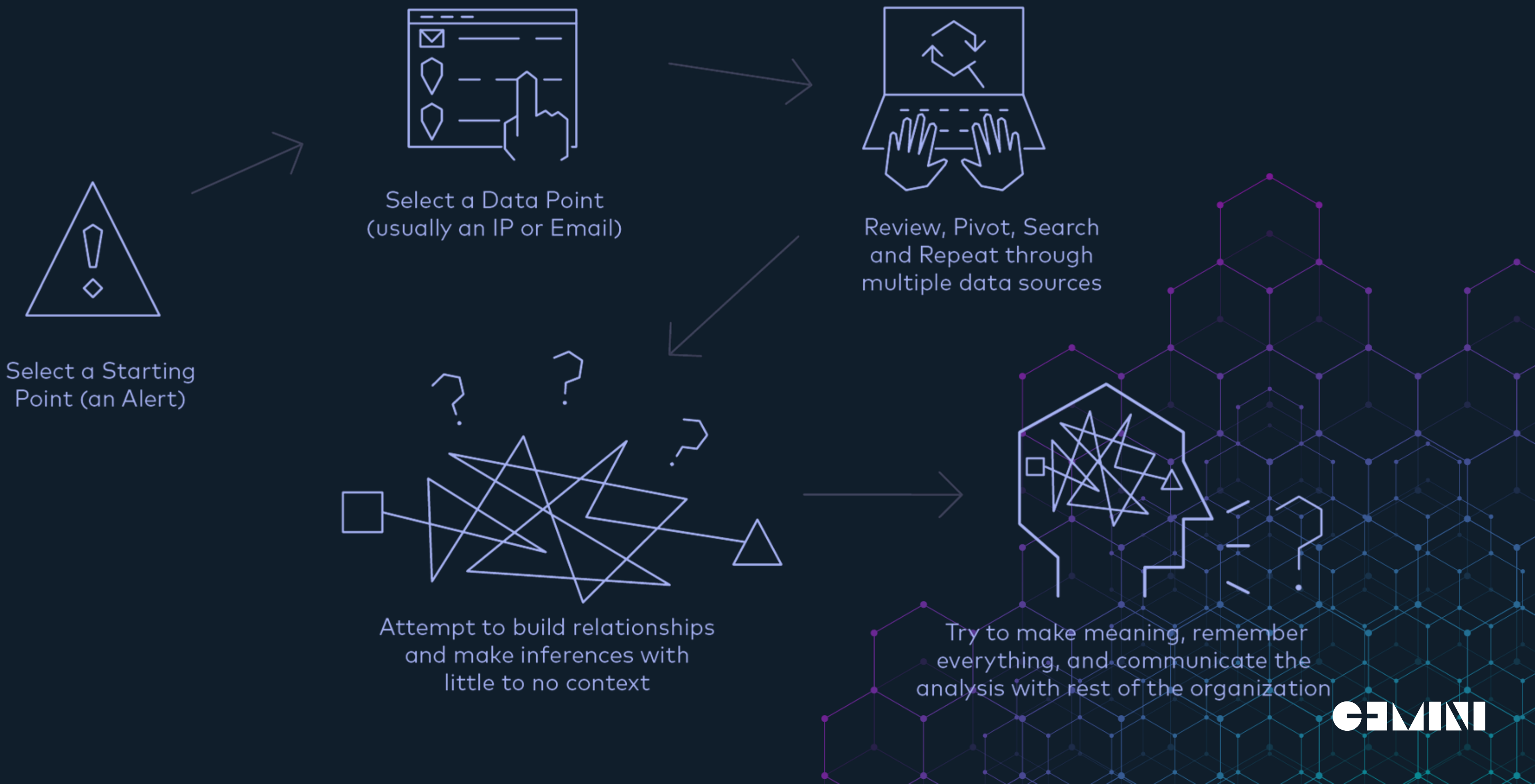
Preparation

Detection & Analysis

Containment Eradication & Recovery

Post-Incident Activity

A Journey of Cyber Security Investigation



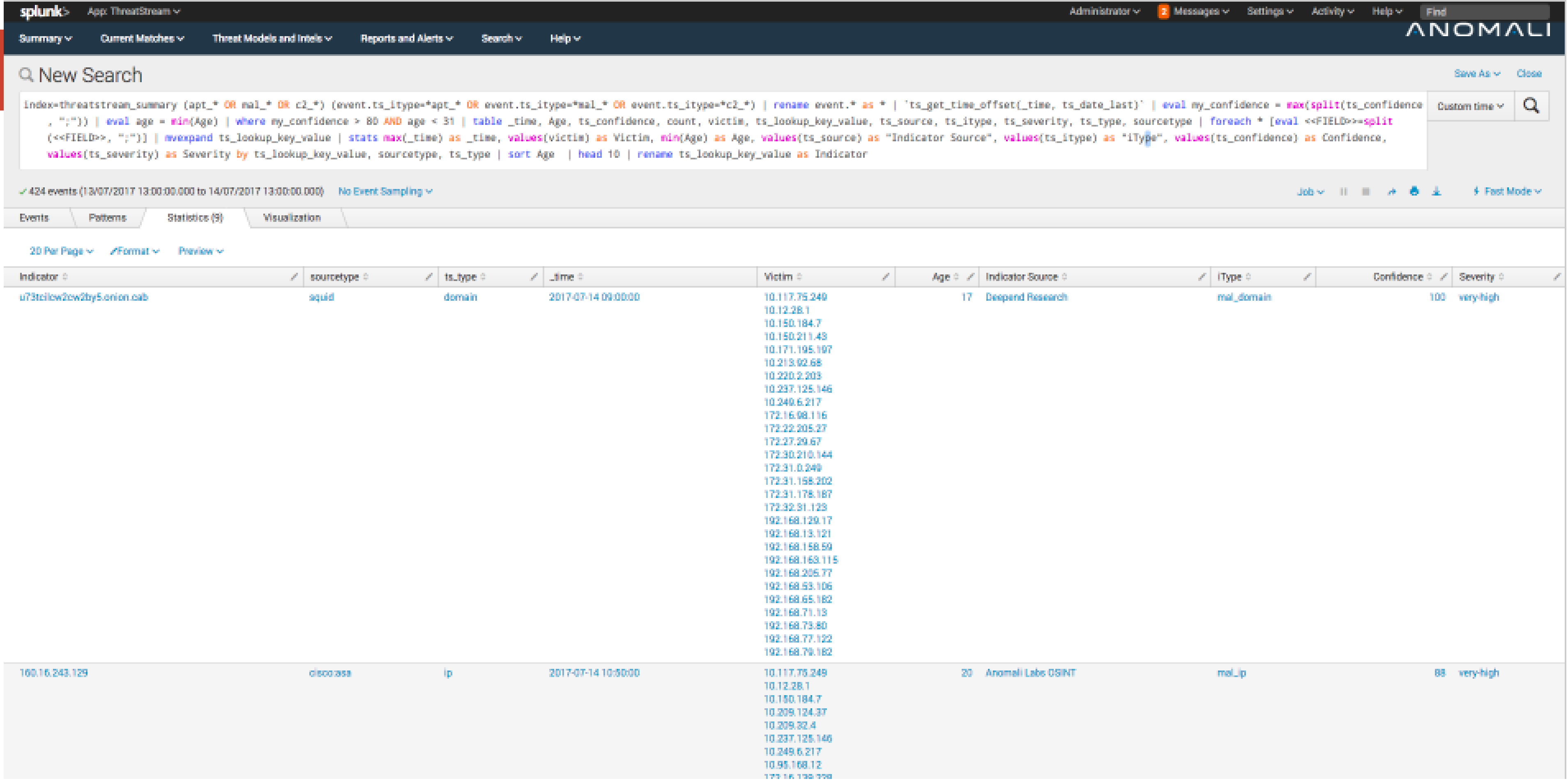
Select a Starting Point (an Alert)

Select a Data Point (usually an IP or Email)

Review, Pivot, Search and Repeat through multiple data sources

Attempt to build relationships and make inferences with little to no context

Try to make meaning, remember everything, and communicate the analysis with rest of the organization

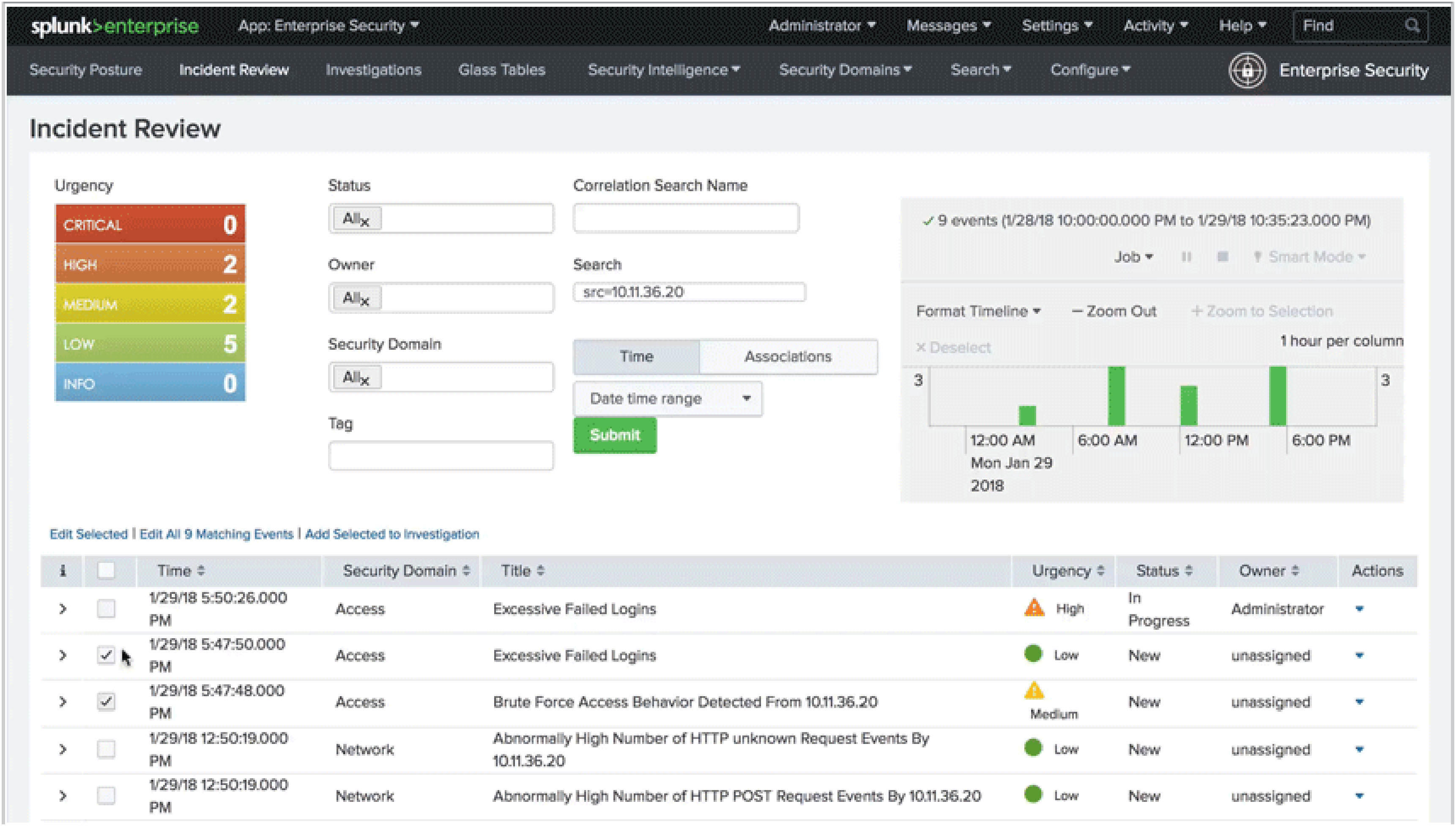


```
index=threatstream_summary (apt_* OR mal_* OR c2_*) (event.ts_itype=*apt_* OR event.ts_itype=*mal_* OR event.ts_itype=*c2_*) | rename event.* as * | `ts_get_time_offset(_time, ts_date_last)` | eval my_confidence = max(split(ts_confidence
  , ";")) | eval age = min(Age) | where my_confidence > 80 AND age < 31 | table _time, Age, ts_confidence, count, victim, ts_lookup_key_value, ts_source, ts_itype, ts_severity, ts_type, sourcetype | foreach * [eval <<FIELD>>=split
  (<<FIELD>>, ";")] | mvexpand ts_lookup_key_value | stats max(_time) as _time, values(victim) as Victim, min(Age) as Age, values(ts_source) as "Indicator Source", values(ts_itype) as "iType", values(ts_confidence) as Confidence,
  values(ts_severity) as Severity by ts_lookup_key_value, sourcetype, ts_type | sort Age  | head 10 | rename ts_lookup_key_value as Indicator
```

✓ 424 events (13/07/2017 13:00:00.000 to 14/07/2017 13:00:00.000) No Event Sampling

Indicator	sourcetype	ts_type	_time	Victim	Age	Indicator Source	iType	Confidence	Severity
u73tcilcw2cw2by5.onion.cab	squid	domain	2017-07-14 09:00:00	10.117.75.249 10.12.28.1 10.150.184.7 10.150.211.43 10.171.195.197 10.213.92.68 10.220.2.203 10.237.125.146 10.249.6.217 172.16.98.116 172.22.205.27 172.27.29.67 172.30.210.144 172.31.0.249 172.31.158.202 172.31.178.187 172.32.31.123 192.168.129.17 192.168.13.121 192.168.158.59 192.168.163.115 192.168.205.77 192.168.53.106 192.168.65.182 192.168.71.13 192.168.73.80 192.168.77.122 192.168.79.182	17	Deepend Research	mal_domain	100	very-high
160.16.243.129	cisco:asa	ip	2017-07-14 10:50:00	10.117.75.249 10.12.28.1 10.150.184.7 10.209.124.37 10.209.32.4 10.237.125.146 10.249.6.217 10.95.168.12	20	Anomali Labs OSINT	mal_ip	88	very-high

Now it’s time to run searches for each one of those IP addresses…



Incident Review

Urgency	
CRITICAL	0
HIGH	2
MEDIUM	2
LOW	5
INFO	0

Status: All×

Owner: All×

Security Domain: All×

Tag:

Correlation Search Name:

Search: src=10.11.36.20

Time | Associations

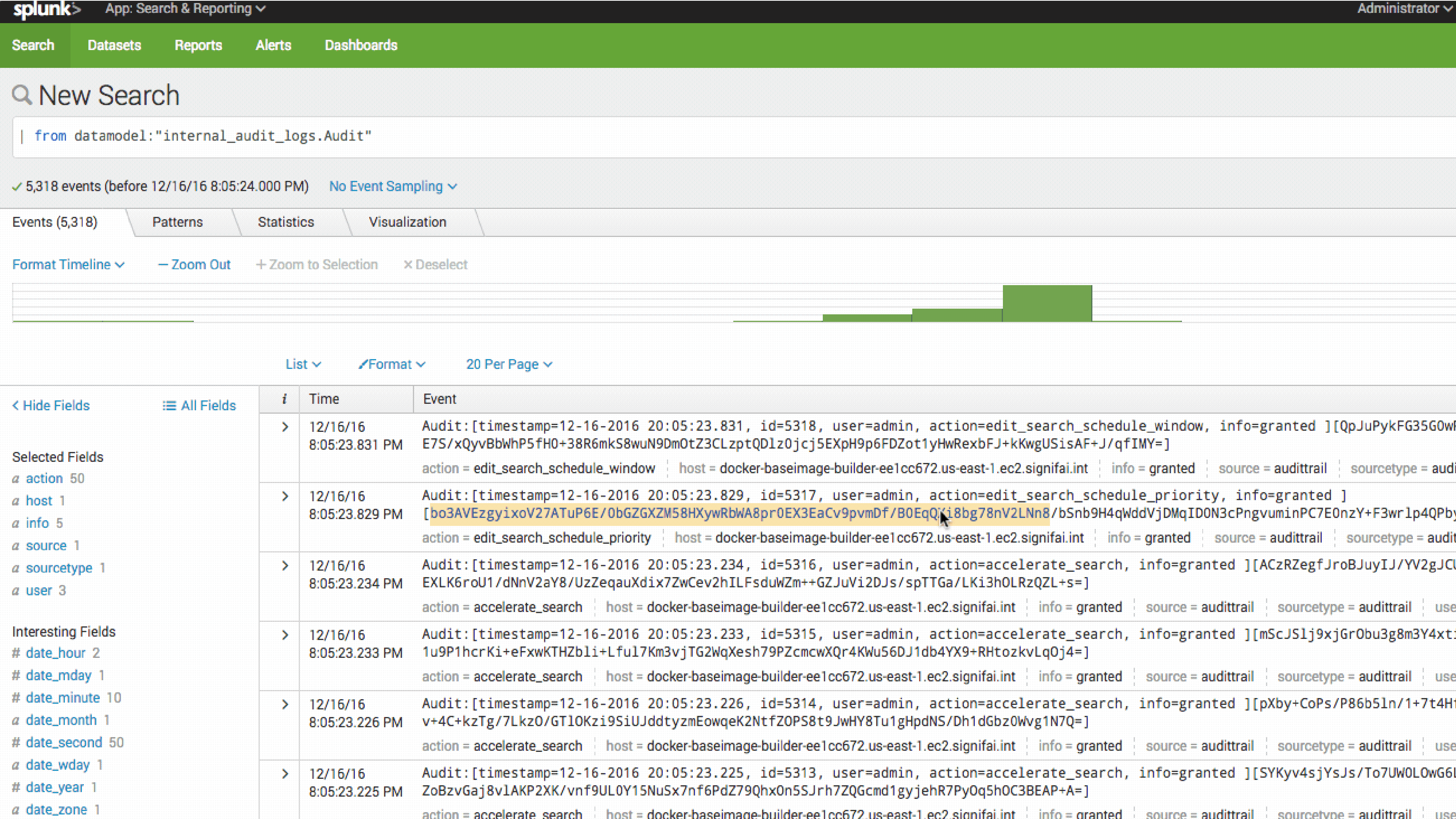
Date time range ▾

Submit

✓ 9 events (1/28/18 10:00:00.000 PM to 1/29/18 10:35:23.000 PM)

Edit Selected | Edit All 9 Matching Events | Add Selected to Investigation

i	□	Time ⇕	Security Domain ⇕	Title ⇕	Urgency ⇕	Status ⇕	Owner ⇕	Actions
›	□	1/29/18 5:50:26.000 PM	Access	Excessive Failed Logins	⚠ High	In Progress	Administrator	▾
›	☑	1/29/18 5:47:50.000 PM	Access	Excessive Failed Logins	● Low	New	unassigned	▾
›	☑	1/29/18 5:47:48.000 PM	Access	Brute Force Access Behavior Detected From 10.11.36.20	⚠ Medium	New	unassigned	▾
›	□	1/29/18 12:50:19.000 PM	Network	Abnormally High Number of HTTP unknown Request Events By 10.11.36.20	● Low	New	unassigned	▾
›	□	1/29/18 12:50:19.000 PM	Network	Abnormally High Number of HTTP POST Request Events By 10.11.36.20	● Low	New	unassigned	▾



```
| from datamodel:"internal_audit_logs.Audit"
```

✓ 5,318 events (before 12/16/16 8:05:24.000 PM)

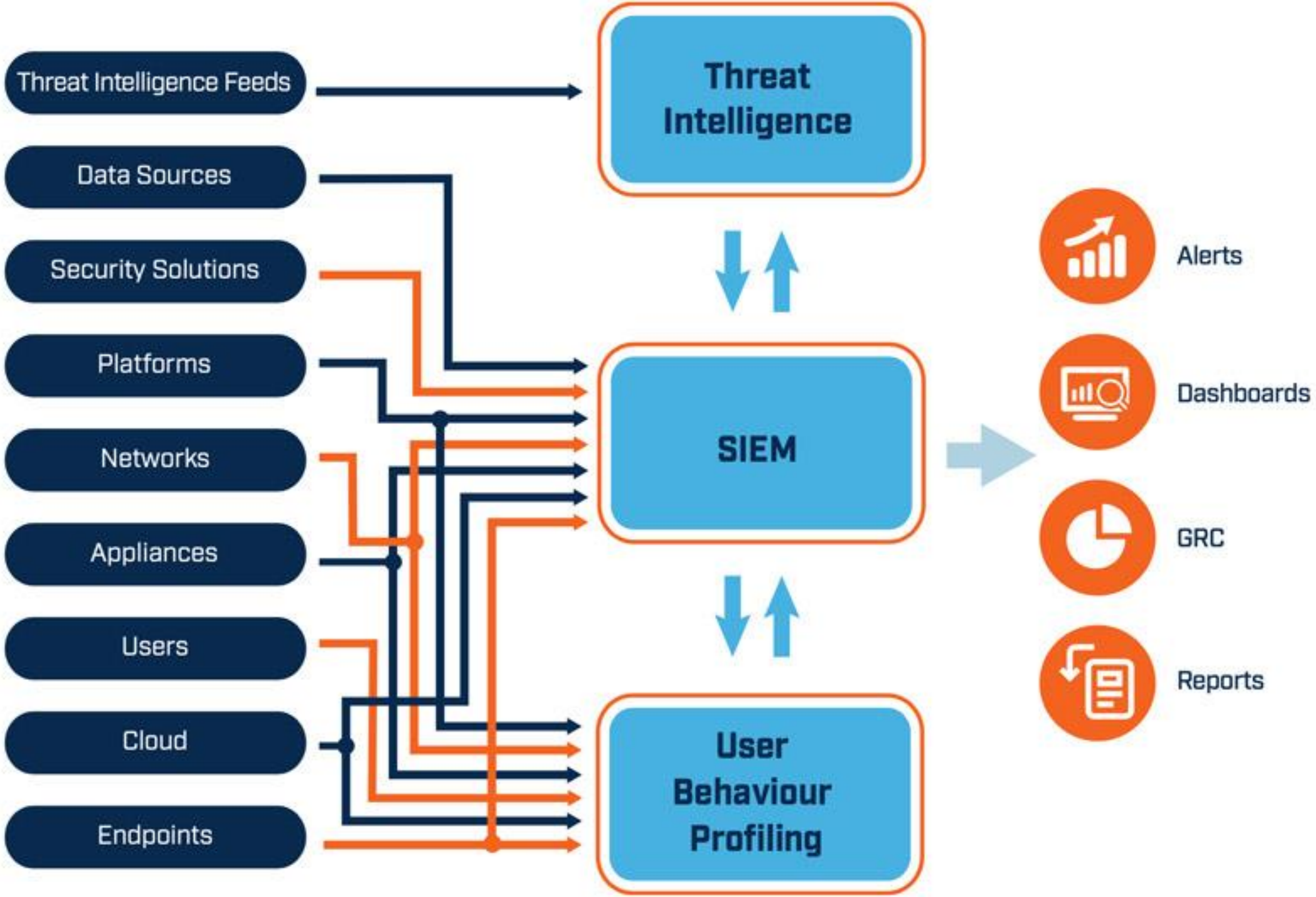
Selected Fields

a action	50
a host	1
a info	5
a source	1
a sourcetype	1
a user	3

Interesting Fields

# date_hour	2
# date_mday	1
# date_minute	10
a date_month	1
# date_second	50
a date_wday	1
# date_year	1
a date_zone	1

```
i  Time                  Event
>  12/16/16              Audit:[timestamp=12-16-2016 20:05:23.831, id=5318, user=admin, action=edit_search_schedule_window, info=granted ][QpJuPykFG35G0w
   8:05:23.831 PM        E7S/xQyvBbWhP5fH0+38R6mkS8wuN9DmOtZ3CLzptQDlz0jcj5EXpH9p6FDZot1yHwRexbFJ+kKwgUSisAF+J/qfIMY=]
                         action = edit_search_schedule_window | host = docker-baseimage-builder-ee1cc672.us-east-1.ec2.signifai.int | info = granted | source = audittrail | sourcetype = audi
>  12/16/16              Audit:[timestamp=12-16-2016 20:05:23.829, id=5317, user=admin, action=edit_search_schedule_priority, info=granted ]
   8:05:23.829 PM        [bo3AVEzgyixoV27ATuP6E/0bGZGXZM58HXywRbWA8pr0EX3EaCv9pvmDf/B0EqQXi8bg78nV2LNn8/bSnb9H4qWddVjDMqID0N3cPngvuminPC7E0nzY+F3wrlp4QPby
                         action = edit_search_schedule_priority | host = docker-baseimage-builder-ee1cc672.us-east-1.ec2.signifai.int | info = granted | source = audittrail | sourcetype = audit
>  12/16/16              Audit:[timestamp=12-16-2016 20:05:23.234, id=5316, user=admin, action=accelerate_search, info=granted ][ACzRZegfJroBJuyIJ/YV2gJC
   8:05:23.234 PM        EXLK6roU1/dNnV2aY8/UzZeqauXdix7ZwCev2hILFsduWZm++GZJuVi2DJs/spTTGa/LKi3hOLRzQZL+s=]
                         action = accelerate_search | host = docker-baseimage-builder-ee1cc672.us-east-1.ec2.signifai.int | info = granted | source = audittrail | sourcetype = audittrail | use
>  12/16/16              Audit:[timestamp=12-16-2016 20:05:23.233, id=5315, user=admin, action=accelerate_search, info=granted ][mScJSlj9xjGrObu3g8m3Y4xt
   8:05:23.233 PM        1u9P1hcrKi+eFxwKTHZbli+Lful7Km3vjTG2WqXesh79PZcmcwXQr4KWu56DJ1db4YX9+RHtozkvLqOj4=]
                         action = accelerate_search | host = docker-baseimage-builder-ee1cc672.us-east-1.ec2.signifai.int | info = granted | source = audittrail | sourcetype = audittrail | use
>  12/16/16              Audit:[timestamp=12-16-2016 20:05:23.226, id=5314, user=admin, action=accelerate_search, info=granted ][pXby+CoPs/P86b5ln/1+7t4H
   8:05:23.226 PM        v+4C+kzTg/7LkzO/GTlOKzi9SiUJddtyzmEowqeK2NtfZOPS8t9JwHY8Tu1gHpdNS/Dh1dGbz0Wvg1N7Q=]
                         action = accelerate_search | host = docker-baseimage-builder-ee1cc672.us-east-1.ec2.signifai.int | info = granted | source = audittrail | sourcetype = audittrail | use
>  12/16/16              Audit:[timestamp=12-16-2016 20:05:23.225, id=5313, user=admin, action=accelerate_search, info=granted ][SYKyv4sjYsJs/To7UW0LOwG6
   8:05:23.225 PM        ZoBzvGaj8vlAKP2XK/vnf9UL0Y15NuSx7nf6PdZ79QhxOn5SJrh7ZQGcmd1gyjehR7PyOq5hOC3BEAP+A=]
                         action = accelerate_search | host = docker-baseimage-builder-ee1cc672.us-east-1.ec2.signifai.int | info = granted | source = audittrail | sourcetype = audittrail | use
```


Threat Intelligence Feeds
Data Sources
Security Solutions
Platforms
Networks
Appliances
Users
Cloud
Endpoints
Threat Intelligence
SIEM
User Behaviour Profiling
Alerts
Dashboards
GRC
Reports

Challenges to Cyber Security Investigation

- Data volume and diversity
- Time consuming
- Analysis driven by Intuition and Biases
- Link the information manually
- Lacking of contextual awareness
- Visualize the findings
- Inconsistency of transferring the whole picture

What is Explore for Capable of?

- Link the data with reasoning
- Turn syntax into clicks
- Investigate by following data relationships
- Visualize the tracking & footprints
- Enrich the context
- Save & Share

GEMINI DATA

How Do Humans Tell a story?

We Define Relationships.

Telling the Story of ‘Steve’

- ‘Steve’ (person) Resides_At ‘Old Colonial’ (building)
- ‘The Old Colonial’ (building) Has_Address ‘15 Funston’ (address)
- ’15 Funston (address) Has_State ‘Foreclosed’ (state)

Key Value Pairs

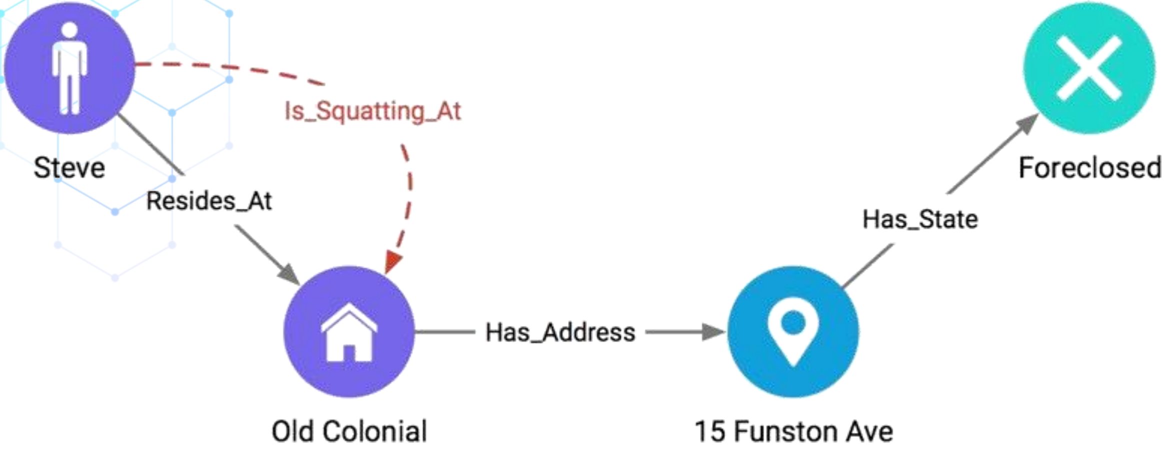
Stories have Elements and Relationships

Noun, Verb, Direct Object

TRIPLES

Element	Relationship	Element
Steve	Resides_At	Old Colonial
The Old Colonial	Has_Address	15 Funston
15 Funston	Has_State	Foreclosed

Telling the Story of ‘Steve’



Harnessing the Tribal Knowledge

Unlike Database Schema design, Ontology design can largely be done by people with no special knowledge outside of the topic.

Good semantic design is a matter of capturing logical statements about a field of knowledge, and encoding chains of elements and constraints.

Done right, triples produce natural-language statements

“Windows XP SP2”	“is a”	“Operating System”
“Windows XP SP2”	“is vulnerable to”	“ms08-67”
“ms08-67”	“is a”	“vulnerability”
“ceobobspc”	“is a”	“host”
“ceobobspc”	“runs on OS”	“Windows XP SP2”
“ceobobspc”	“connected to”	“yourcomputer”
“yourcomputer”	“is now infected with”	“conficker”

Let’s look at a security incident as an example

Various Event Types

Email

action	dest	dest_buit	File_hash	File_name	File_size	Email_subject	Orig_dest	protocol	recipient	Vendor
sent	10.10.142.5	marketing	0A566B1616C8AFEEF214372B1A0580C7	2016 Recruitment Plan.html	147 KB	Hello Their	rdobbs	SMTP	rdobbs@geminidata.com	MS Exchange
received	10.10.142.27	marketing	0A566B1616C8AFEEF214372B1A0580C7	2016 Recruitment Plan.html	147 KB	Hello Their	amichaels	SMTP	amichaels@geminidata.com	MS Exchange

Malware

action	category	date	dest	File hash	File_name	sender	signature	src	Vendor
Violation Blocked	Black hole Exploit	2017_08_08	RDOBBS-PC01	0A566B1616C8AFEEF214372B1A0580C7	2016 Recruitment Plan	rdobbs@geminidata.com	Backdorr.W32/Duqu	10.10.142.5	McAfee Endpoint Security

Vulnerability

cve	cvss	dest	msft	signature	Vendor
CVE-2015-2360	7.2	10.10.142.27	MS15-061	win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2	Qualys
CVE-2012-4681	10	10.10.142.27	null	Multiple vulnerabilities in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 6 and earlier	Qualys

Various Event Types

DHCP (not CIM compliant)

action	date	time	description	IP address	hostname	MAC Address
leased	2017_08_01	14:37	MACBOOKPRO-5D26	10.10.142.5	RDOBBS-PC01	78:4f:43:a3:5d:26
leased	2017_08_04	9:09	MACBOOKPRO-9R20	10.10.142.27	AMICHAELS-PC01	78:47:43:f6:3e:56

AD (not CIM compliant)

DN	SAMID	CN	empid	email	OU	OU	DC	DC	Phone
Nacho.geminidata	Robert Dobbs	DOBBS Robert	rdobbs	rdobbs@nacho.geninidata.com	MGR	MKT	Gemini.	com	650-777-7777
Nacho.geminidata	Alice Michaels	MICHAELS Alice	amichaels	amichaels@nacho.geminidata.com	Designer	MKT	Gemini.	com	650-986-6785

From Key Value Pair to Triples

ELEMENTS	RELATIONSHIP	ELEMENTS
Noun	**Verb**	**Direct Object**
Email	Contains subject	Hello There
Email	Contains attachment	2016 Recruitment Plan
2016 Recruitment Plan	Contains File	Mal/frame-W script
Violation Blocked	Detected by	McAfee Endpoint Security
CVE-2012-4681	Can be exploited by	Black Hole Exploit Kit
Email	Addressed to	Alice Michaels
Hello there	Sent from	rdobbs@nacho.geminidata.com
rdobbs@nacho.geminidata.com	Belongs to	Robert Dobbs

What will Explore benefit to cyber security investigation?

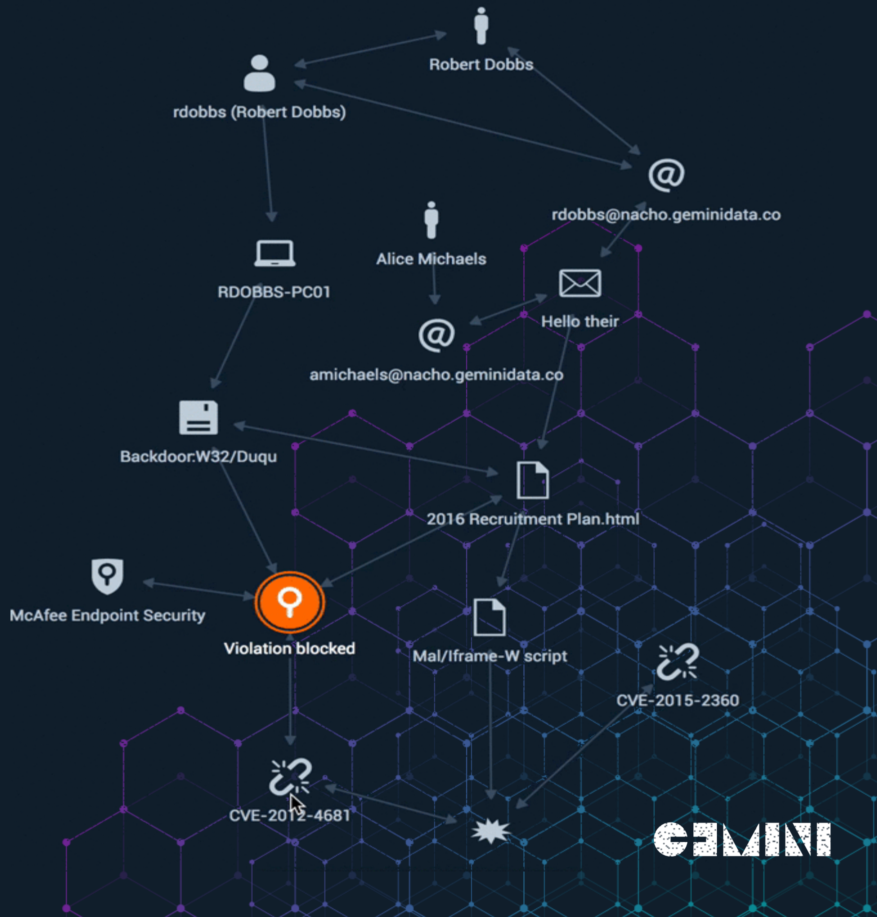
- Drill down the investigation quickly
- Reveal the scope of impacts
- Spot the threats & risky items
- Take notes on interesting data
- Visualize the findings and attack maps

GEMINI DATA

Graphical Representation of A Story

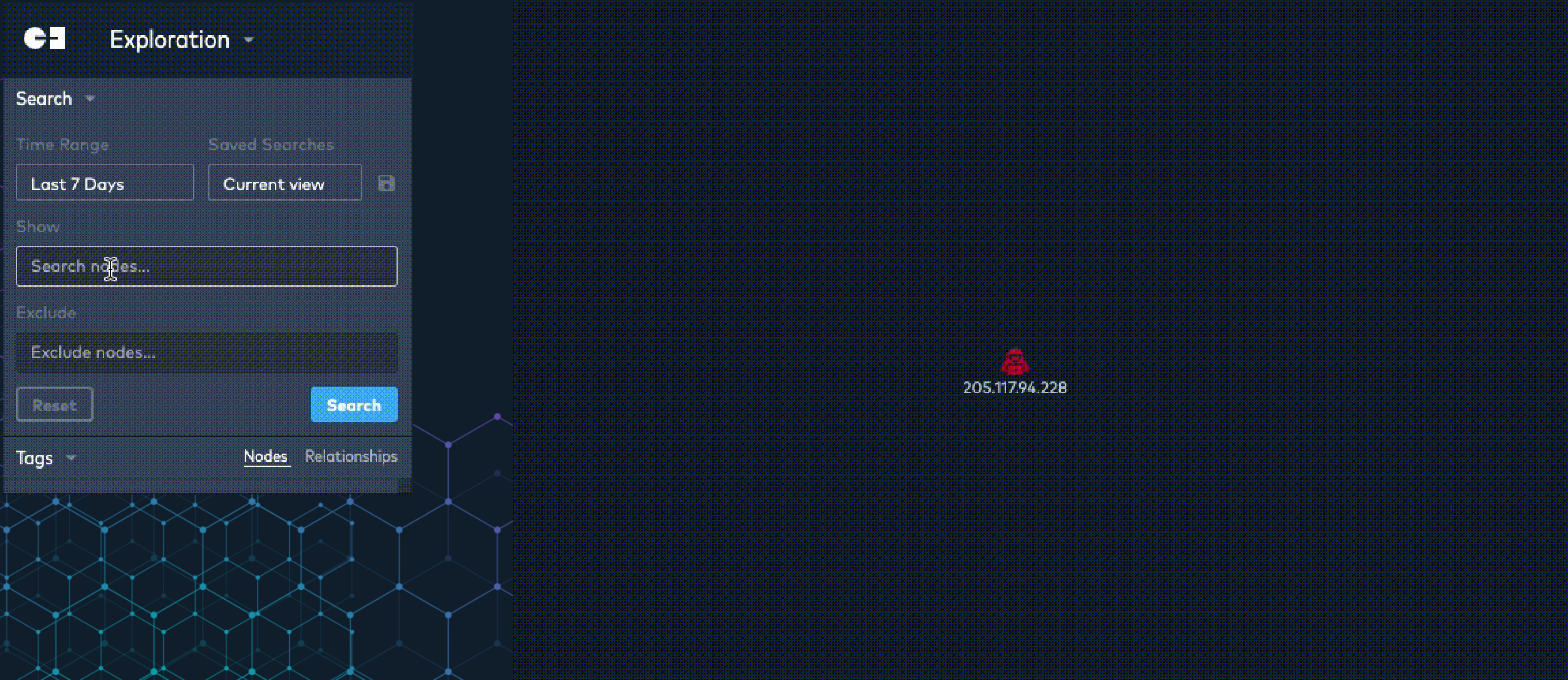
“Robert’s computer sent an email to Alice with an attachment called 2016 Recruitment Plan.html. The attachment contained a malware script that is associated with a particular vulnerability related to a Black Hole Exploit Kit that was blocked by McAfee Endpoint.”

- **Visualization tells a more powerful story**
- **Can be saved for further use**
- **Easy to communicate with others**
- **Story can tell itself**



Drill Down the Investigation Quickly

Keyword Search + Drill down



Exploration

Search

Time Range: Last 7 Days

Saved Searches: Current view

Show: Search nodes...

Exclude: Exclude nodes...

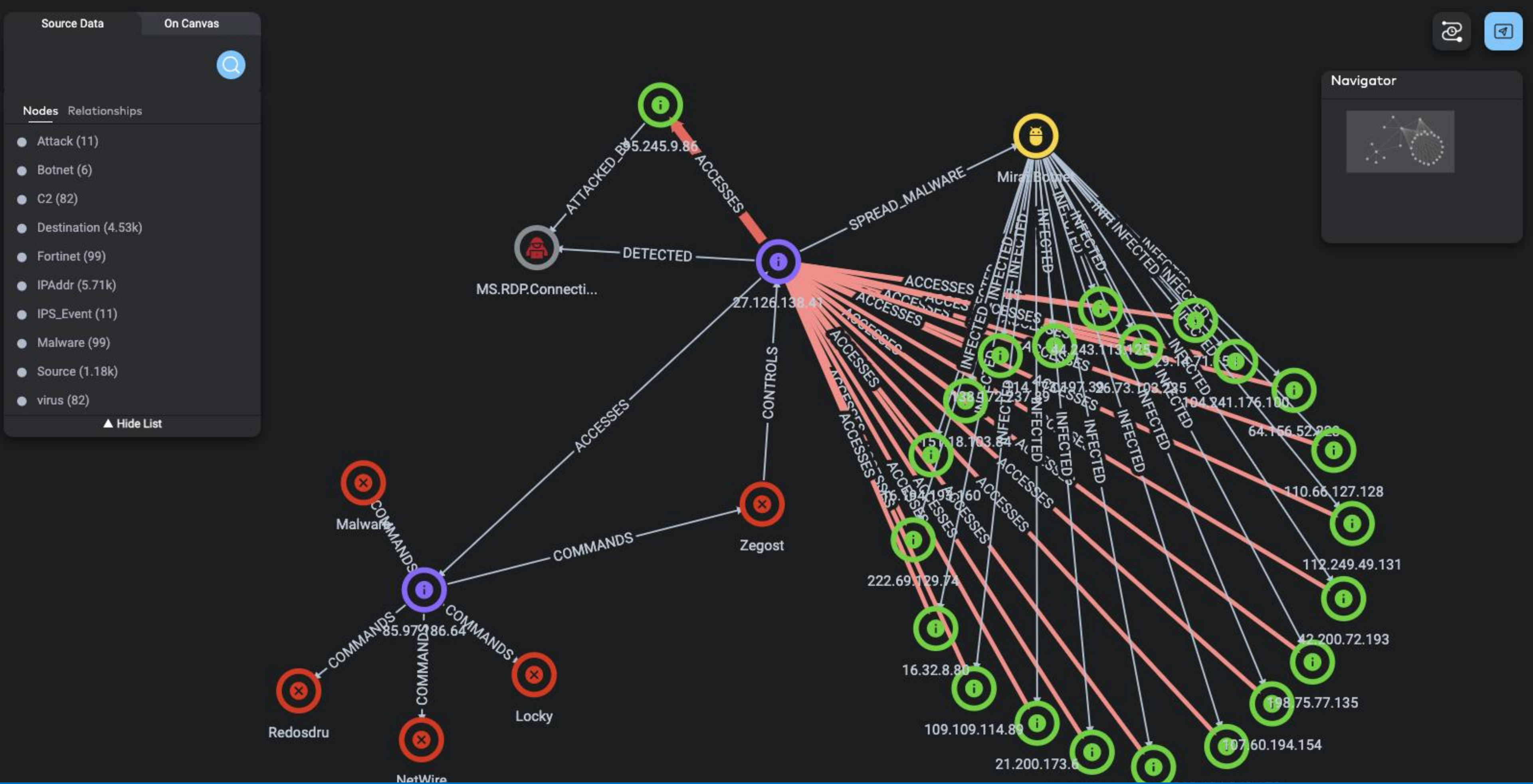
Reset

Search

Tags

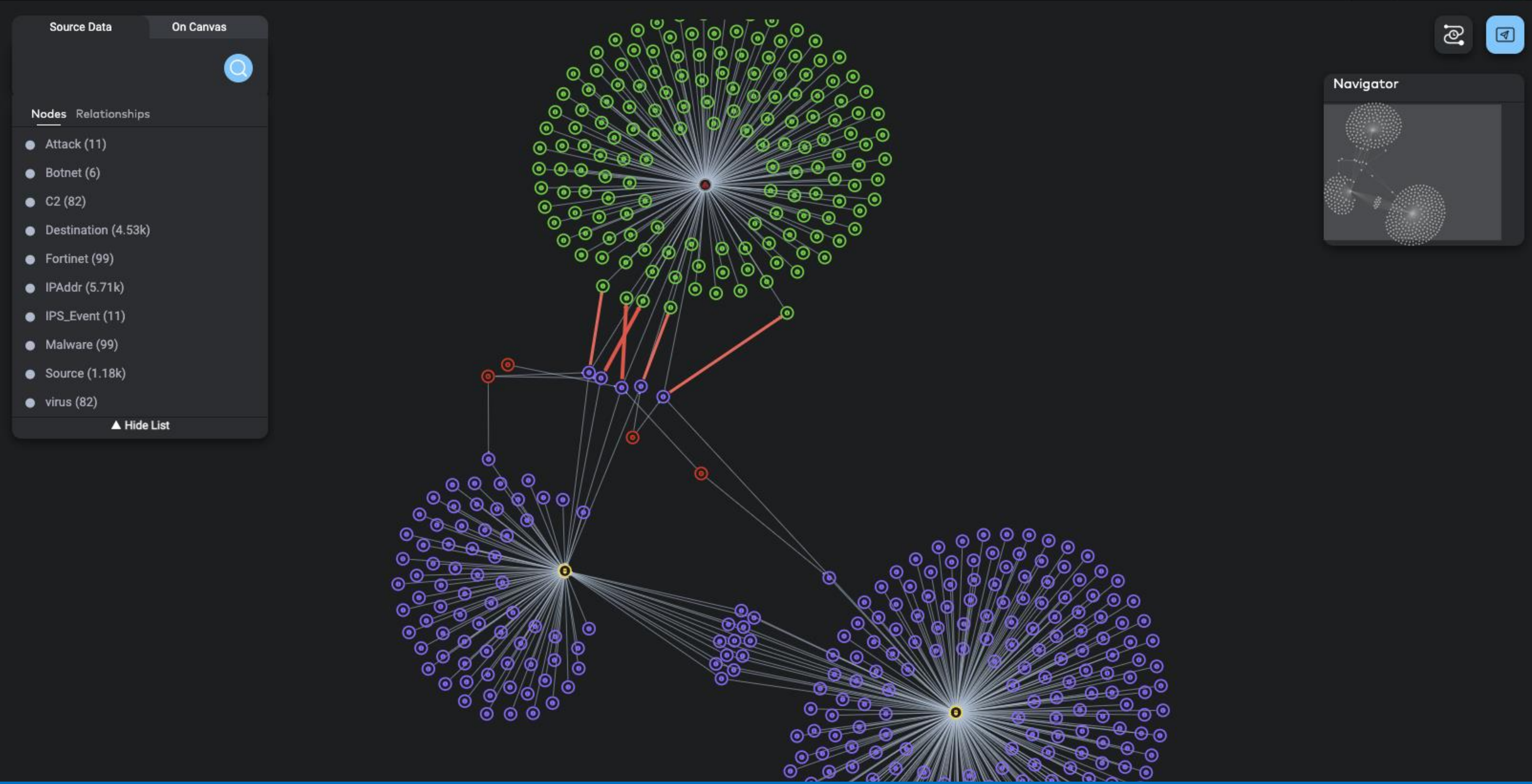
Nodes

Relationships



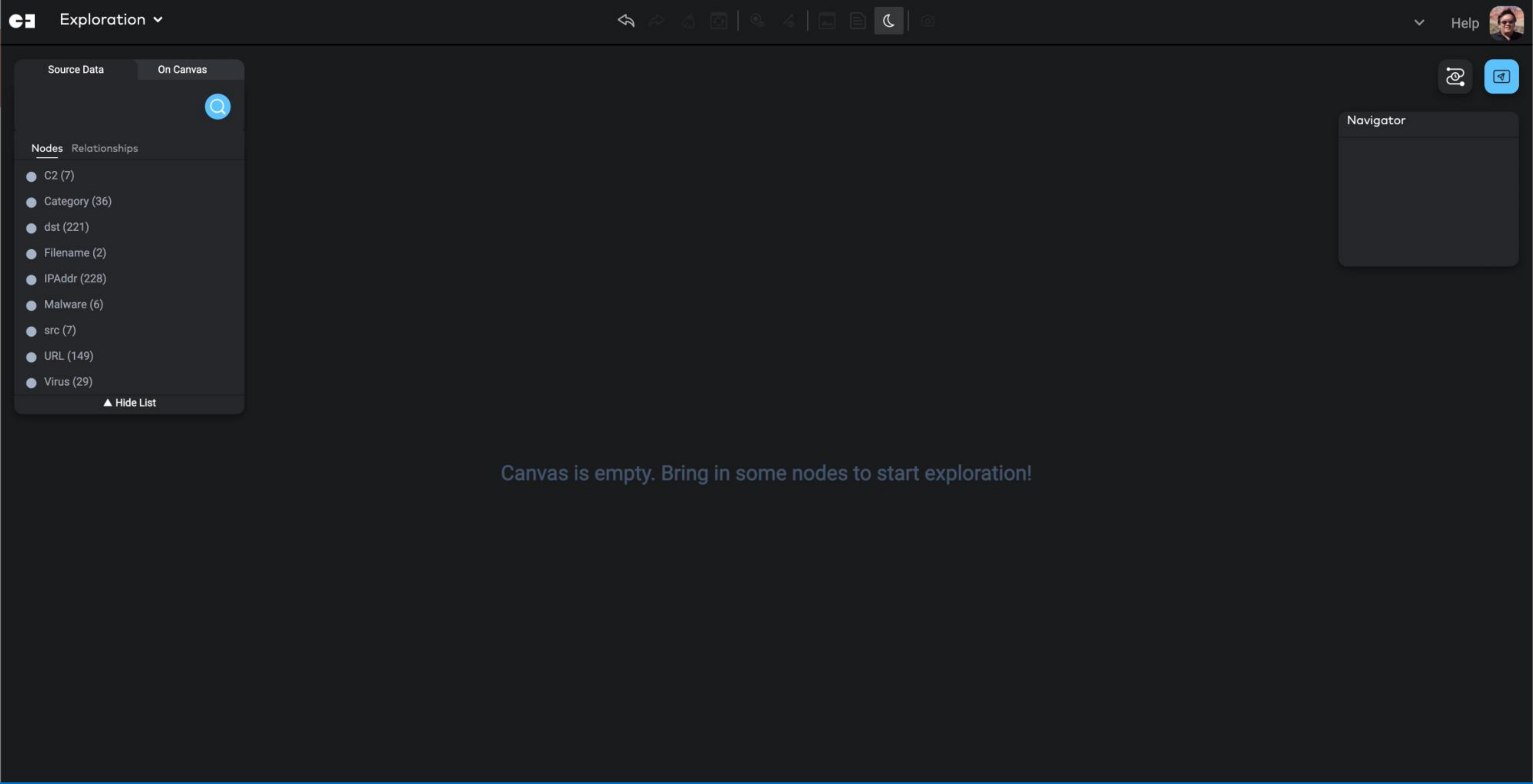
● Attack (11)
● Botnet (6)
● C2 (82)
● Destination (4.53k)
● Fortinet (99)
● IPAddr (5.71k)
● IPS_Event (11)
● Malware (99)
● Source (1.18k)
● virus (82)

Spot Risky Assets



- ● Attack (11)
- ● Botnet (6)
- ● C2 (82)
- ● Destination (4.53k)
- ● Fortinet (99)
- ● IPAddr (5.71k)
- ● IPS_Event (11)
- ● Malware (99)
- ● Source (1.18k)
- ● virus (82)

Reveal Scope of Impact

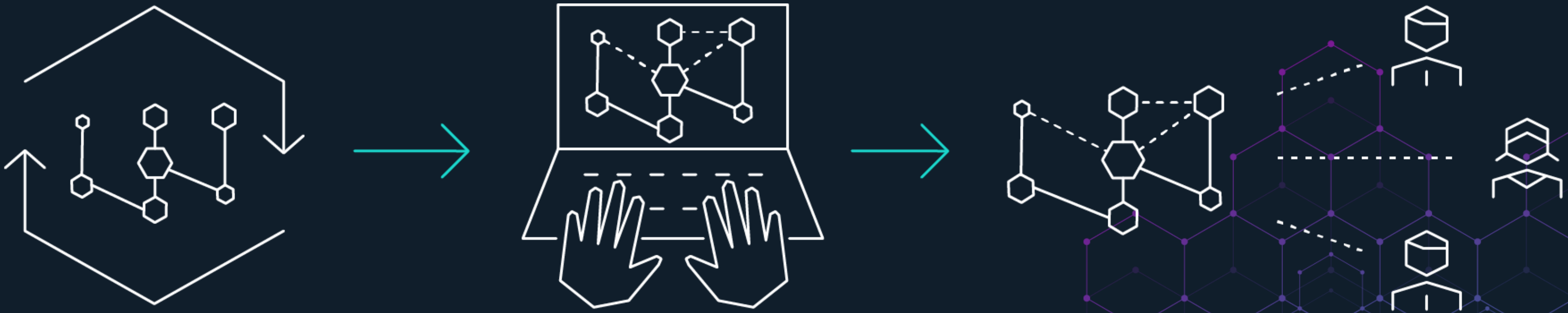


- ● C2 (7)
- ● Category (36)
- ● dst (221)
- ● Filename (2)
- ● IPAddr (228)
- ● Malware (6)
- ● src (7)
- ● URL (149)
- ● Virus (29)

Canvas is empty. Bring in some nodes to start exploration!

Dive Into Threat Intelligence

The Analyst Journey with Gemini Explore



Machine reasoning discovers relationships between elements

Analyst reviews elements and relationships to create the analysis story

Analysis story is shared across organization

Thank You

GEMINI

Questionnaire