Cyber Threat Intelligence, the key to the SOC of the Future

Bret Jordan CISSP

Director Office of the CTO - Symantec

Problem #1

Networks are getting breached on a daily basis using TTPs that are months or years old

Copyright © 2018 Bret Jordan. All rights reserved.

Problem #2

Threat actors are advancing at a positive non-linear rate relative to cyber defense

Copyright © 2018 Bret Jordan. All rights reserved.

Problem #3

Organizations are increasingly unable to adequately respond to modern threats, vulnerabilities, and risks

Copyright © 2018 Bret Jordan. All rights reserved.

Problem #4

Currently we run the risk of losing the cyber war globally, and everyone is affected!

Copyright © 2018 Bret Jordan. All rights reserved.

WHY

is cyber defense failing?

Copyright © 2018 Bret Jordan. All rights reserved.

There are always gaps and vulnerabilities

Copyright © 2018 Bret Jordan. All rights reserved.

Traditional defense is inward focused

- Find all vulnerabilities
- Patch all vulnerabilities
- Magically secure

Copyright © 2018 Bret Jordan. All rights reserved.

Everything is outside the perimeter

- Users, Systems, and Content
- No single network perimeter to protect
- Organizations no longer own
  - All end points
  - The entire network
  - All servers
  - The content

Copyright © 2018 Bret Jordan. All rights reserved.

Attacks are big business

- Attacks and campaigns are very profitable
- More valuable data at stake than ever before
  - Compromise and steal
  - Hold for ransom
- Detection is measured in terms of months or years
- One organization's defense stays their defense

Copyright © 2018 Bret Jordan. All rights reserved.

WHAT

can we do about it?

Copyright © 2018 Bret Jordan. All rights reserved.

What can we do today?

- Understand the adversary
- We need to respond more quickly
- Shift burden of cost to the adversary
- Enable herd immunity

Copyright © 2018 Bret Jordan. All rights reserved.

Ask ourselves the question

How can my detection today aid your prevention tomorrow?

Copyright © 2018 Bret Jordan. All rights reserved.

We need information sharing

- Broad ecosystems and trust groups
- **Sharing Actionable CTI automatically**
- Across verticals and public / private sectors
- Not just IPs and URLs
- Near real-time

Copyright © 2018 Bret Jordan. All rights reserved.

Advantages of sharing CTI

- Gain proactive defense
- Reduce long-term risk
- Potentially lower your cyber insurance premiums
- Enable herd immunity
- Improve operational understanding of threats
- Increase the capabilities of SOC team members

Copyright © 2018 Bret Jordan. All rights reserved.

HOW

can STIX & TAXII help

Copyright © 2018 Bret Jordan. All rights reserved.

What is STIX?

- Graph based model for documenting threats with clear semantics
  - The model is described in JSON
- Includes a feature rich indicator patterning grammar
  - Allows both conditional and temporal logic
- Enables organizations to:
  - Learn from others
  - Share what they have learned
  - Understand how to defend the network

Copyright © 2018 Bret Jordan. All rights reserved.

Current Status of STIX

- STIX 2.0 was finalized in July of 2017
  - Many vendors and organizations are actively using it today
- The technical committee is actively working STIX 2.1 which will add some valuable features to the core specification
  - Translations and multiple languages
  - Confidence
  - Opinions
  - Notes
  - Malware and Infrastructure
- Interoperability Specifications

Copyright © 2018 Bret Jordan. All rights reserved.

The problems STIX solves

- Who is responsible for the attack?
  - Threat Actors
  - Intrusion Sets
  - Campaigns
  - Identity

Copyright © 2018 Bret Jordan. All rights reserved.

The problems STIX solves (cont.)

- How are they doing it, what is their modus operandi?
  - Attack Pattern
  - Malware / Infrastructure
  - Tools
  - Vulnerability

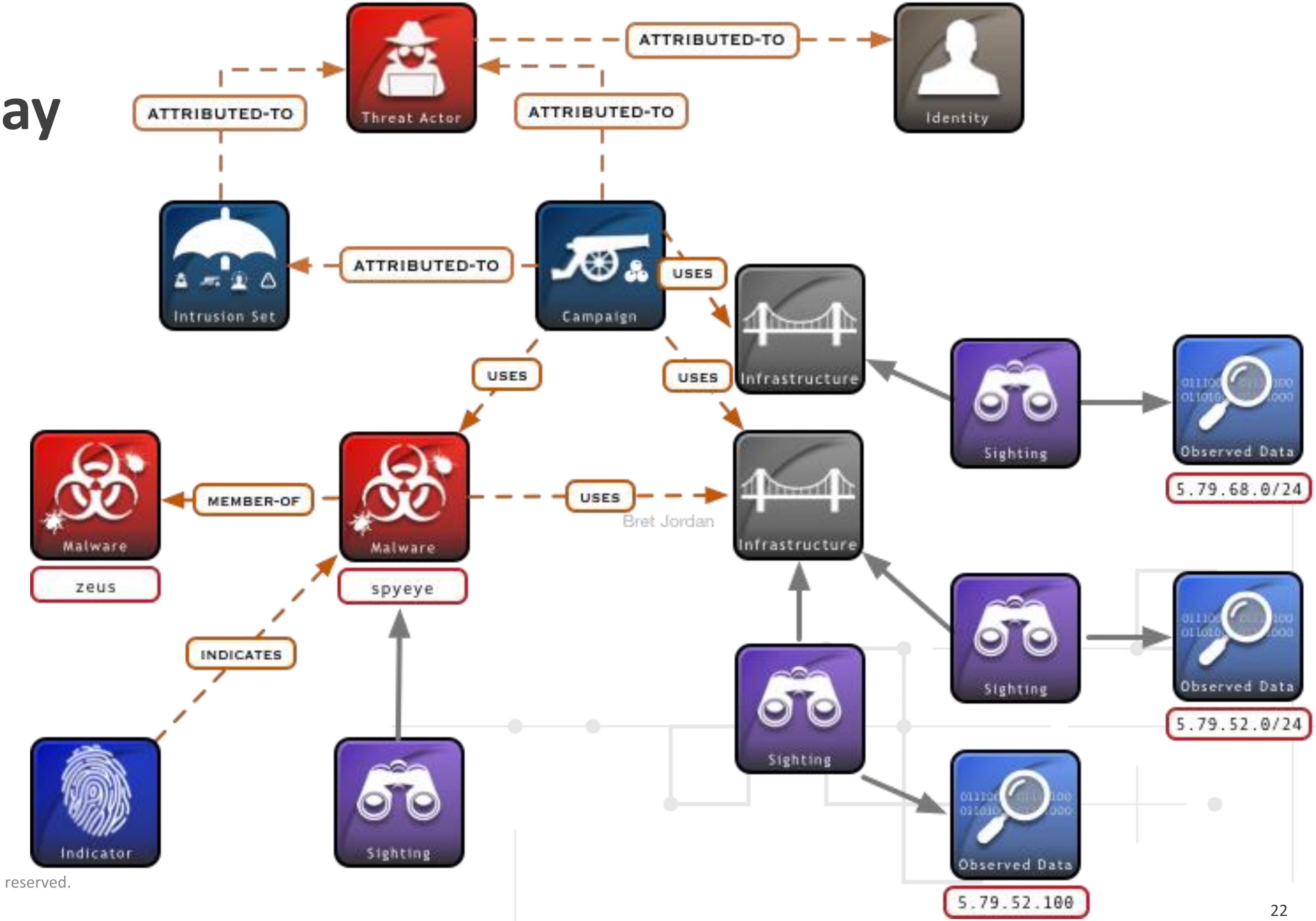
Copyright © 2018 Bret Jordan. All rights reserved.

The problems STIX solves (cont.)

- How do you detect it and stop it?
  - Indicator
  - Observed Data
  - Sighting
  - Course of Action

Copyright © 2018 Bret Jordan. All rights reserved.

The STIX way



Copyright © 2018 Bret Jordan. All rights reserved.

What is TAXII?

- A turn-key solution for devices to share threat intelligence
- Uses HTTPs and REST to transport CTI
- Supports the creation of multiple trust groups
- Currently supports Request – Response interactions
- Future support for Publish – Subscribe channels

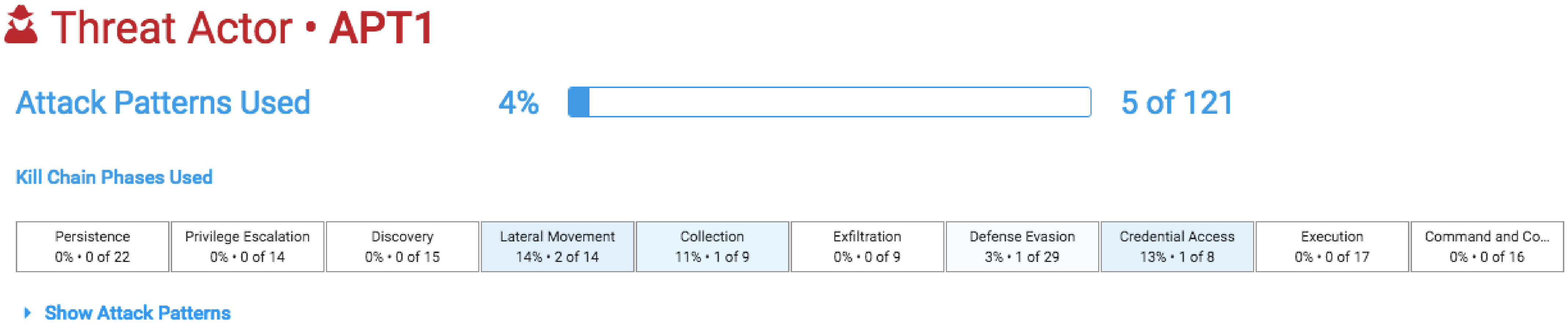
Copyright © 2018 Bret Jordan. All rights reserved.

Resources

to play with

Copyright © 2018 Bret Jordan. All rights reserved.

Gaining context through visualizations



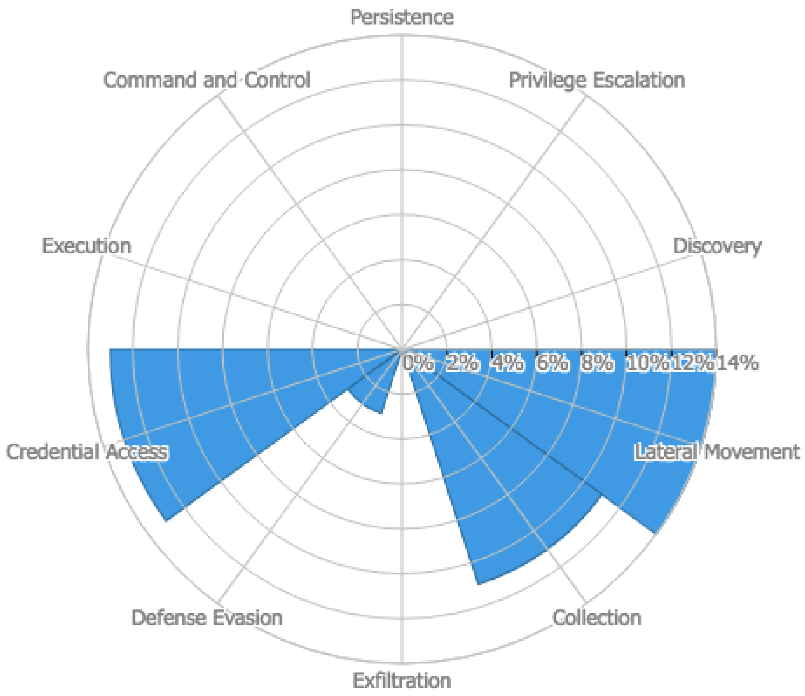
Threat Actor • APT1

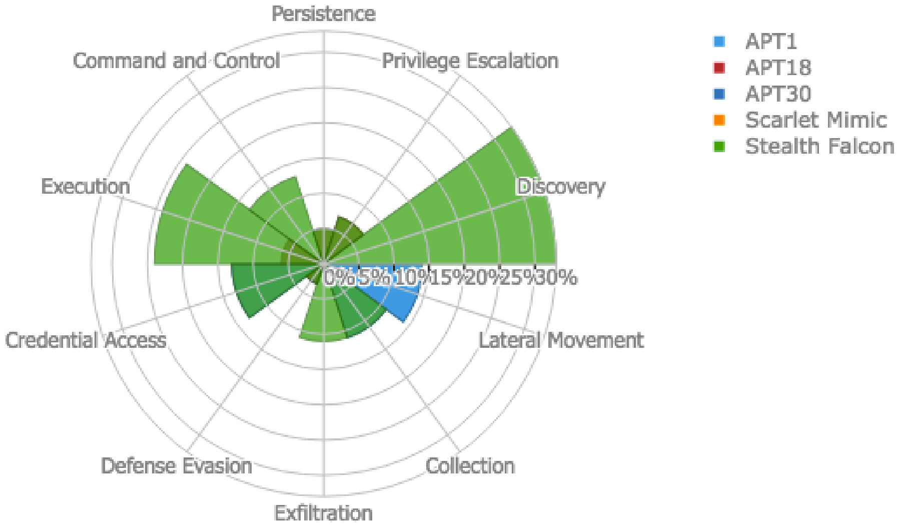
Attack Patterns Used 4% 5 of 121

Kill Chain Phases Used

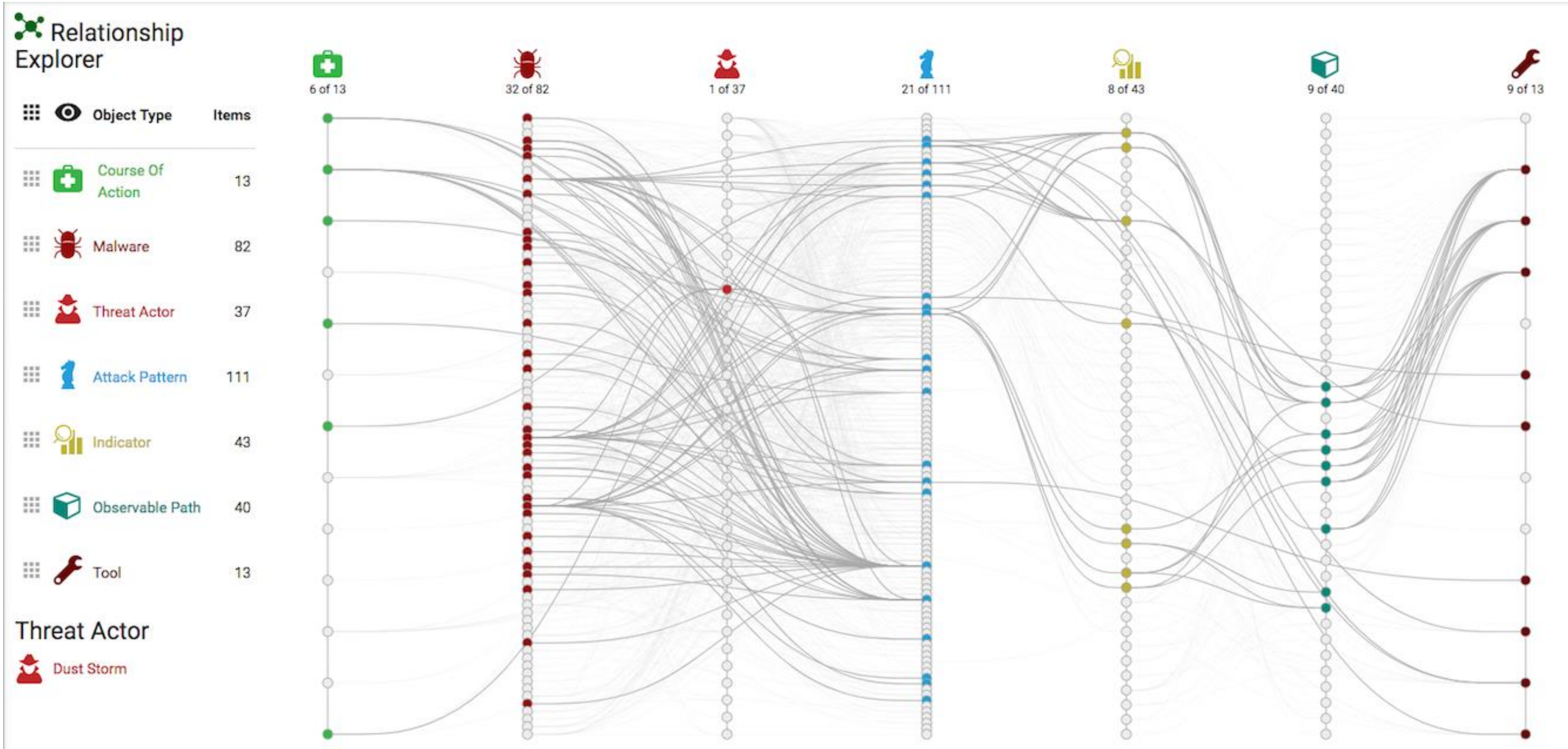
Persistence	Privilege Escalation	Discovery	Lateral Movement	Collection	Exfiltration	Defense Evasion	Credential Access	Execution	Command and Co...
0% • 0 of 22	0% • 0 of 14	0% • 0 of 15	14% • 2 of 14	11% • 1 of 9	0% • 0 of 9	3% • 1 of 29	13% • 1 of 8	0% • 0 of 17	0% • 0 of 16

Show Attack Patterns





Gaining context through visualizations



Relationship Explorer

Object Type	Items
Course Of Action	13
Malware	82
Threat Actor	37
Attack Pattern	111
Indicator	43
Observable Path	40
Tool	13

Threat Actor

Dust Storm

Conclusion

things to think about

Copyright © 2018 Bret Jordan. All rights reserved.

Threat Intelligence can…

- Give you a rich source of IOCs to block
- Help you better understand emerging threats
- Provide insight in to an attack to help you with incident response
- Tell you what to go look for based on what you have seen or found
- Help you understand what additional problems you may have
- Tell you how a given campaign or attack is being conducted
- Tell you what types of vulnerabilities and systems a given campaign is targeting

Copyright © 2018 Bret Jordan. All rights reserved.

The future

Why is this so important for the ITU and telecoms across the globe?

Copyright © 2018 Bret Jordan. All rights reserved.

The dream

This dream of herd immunity is **only** possible when we share CTI in an automated machine-to-machine structured format

Copyright © 2018 Bret Jordan. All rights reserved.

Q&A

Copyright © 2018 Bret Jordan. All rights reserved.