# Cyber Security: It's about the Network, Silly

NASA Supply Chain Conference
NASA Goddard Space Flight Center
October 26, 2016

# The @Cold War+" Begins

**September 5, 2016**

Washington Post

*Intelligence and law enforcement acknowledge investigate a "broad Russian covert operation in the United States to sow public distrust in the upcoming presidential election"*

**October 11, 2016**

Washington Post

*White House Press Secretary Josh Earnest promised the U.S. would deliver a "proportional" response to Russia's alleged hacking of American computer systems.*

**October 18, 2016**

Wall Street Journal

*Salesforce board Member Colin Powell's email hacked. "M&A Target Review" and marked "draft and confidential," identified 14 possible targets, from Adobe Systems to LinkedIn*

## October 24, 2016

Politico

IoT Driven DDOS Attack. *“There might be a long way to go before the U.S. government is prepared to deal with anything similar.”*

*DHS Secretary Johnson said the DHS is working with law enforcement and the private sector to defend against Mirai and similar threats. He pledged that DHS would produce a strategic plan "in the coming weeks" to protect internet of things devices.*

# The 9 most terrifying words in the English language are:

The 9 most terrifying words in the English language are:

# “I’m from the government and I’m here to help”

President Ronald Reagan

# What if?

"I'm from government, and I *can't* help"

President Reagan – slightly revised for Internet era

*  *  *

We may yearn for the old days…

*“…the speed of networks now outstrips the velocity of our decisions…”*

Joshua Cooper Ramo, The Seventh Sense

# This Cold War Will be Different

Guess where the front line is now…?

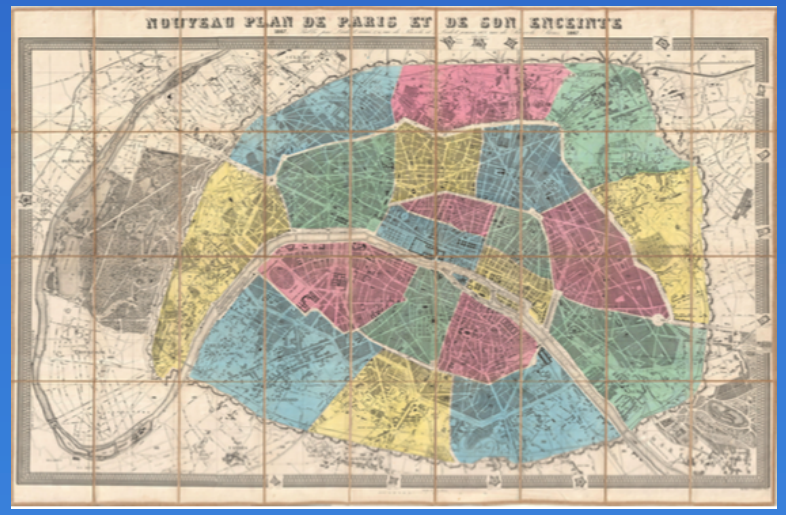
# Your Network

So how did we get here?

Learn from past networks

# Learning from Past Networks

Paris 1860's




USA Rail Networks 1870s


USA Interstate 1970


**Built for Commerce and Defense**

# Airline Networks

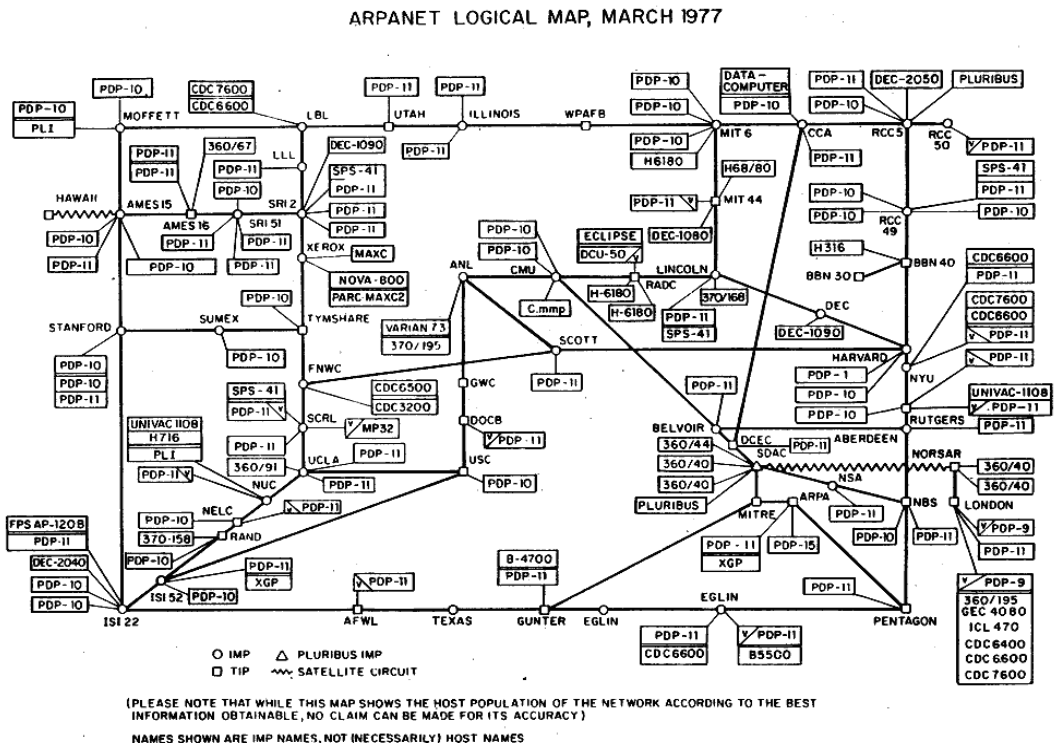
## Global Airline Network 1960


## Global Airline Network Today

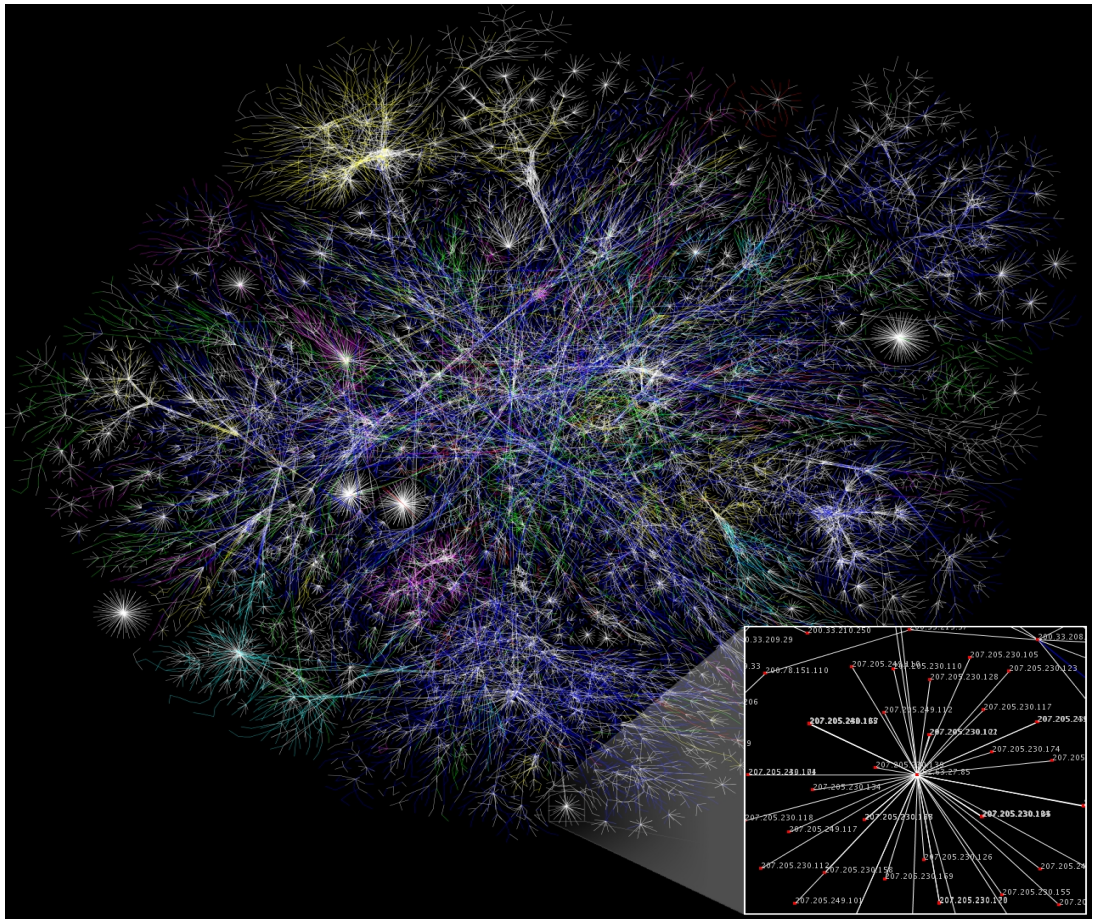
**Built for Commerce and Defense Purposes**

# The Internet

## ARPANET 1977




## The Internet Today



# Built for Commerce and Defense Purposes

# Dr. Paul Baran:
# Certain types of networks represent an "irreversible transition"

You can't go back from a town that has a phone to one that does not

You can't go back from Google to the Encyclopedia Britannica

You can't go back to the old-style stock markets

**Government's ability to help is limited**

# The Power of the Internet Network

## Positive

- Instantaneous
- Distributes power in ways new in human history
- Efficiencies
- Explosive growth
  - +10K devices a minute
- Constant connections

## Negative

- Complex (not complicated)
- Always changing
- Challenges traditional institutions and protocols
  - Indictments, Sanctions, and Regulations
  - Intelligence & Military action
  - Alliances

**We have Forgotten about The Internet Being for Defense Purposes**

# Networks

"We will come to see why they will enforce, whether we like it or not, a complete change in the apparatus of power, politics, economics, and military power."

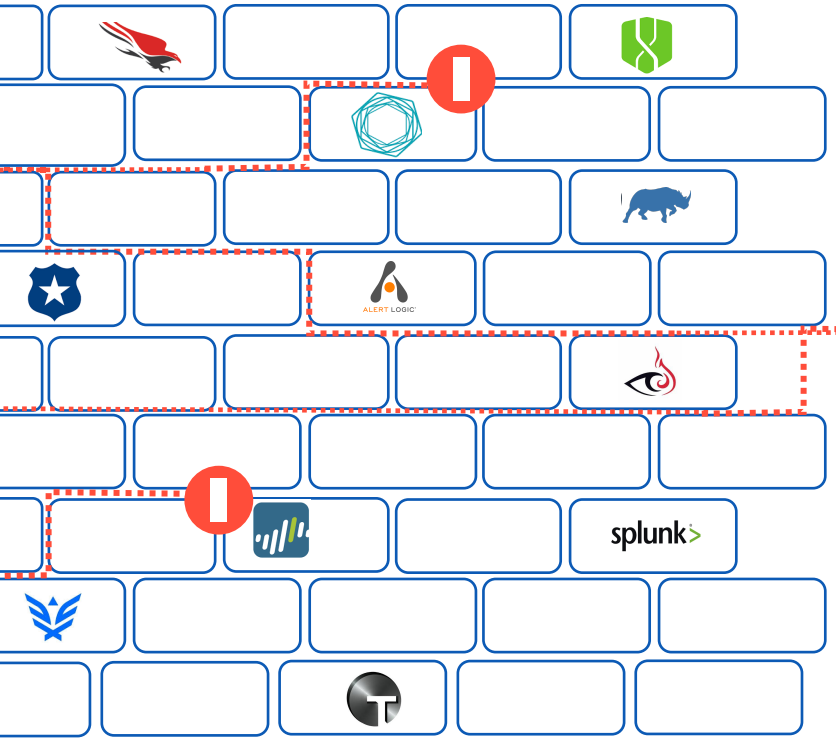
Ramo, The Seventh Sense

So why don’t we use networks to address cybersecurity?

We use the Internet for commerce, but not for defense

# How does security work today?

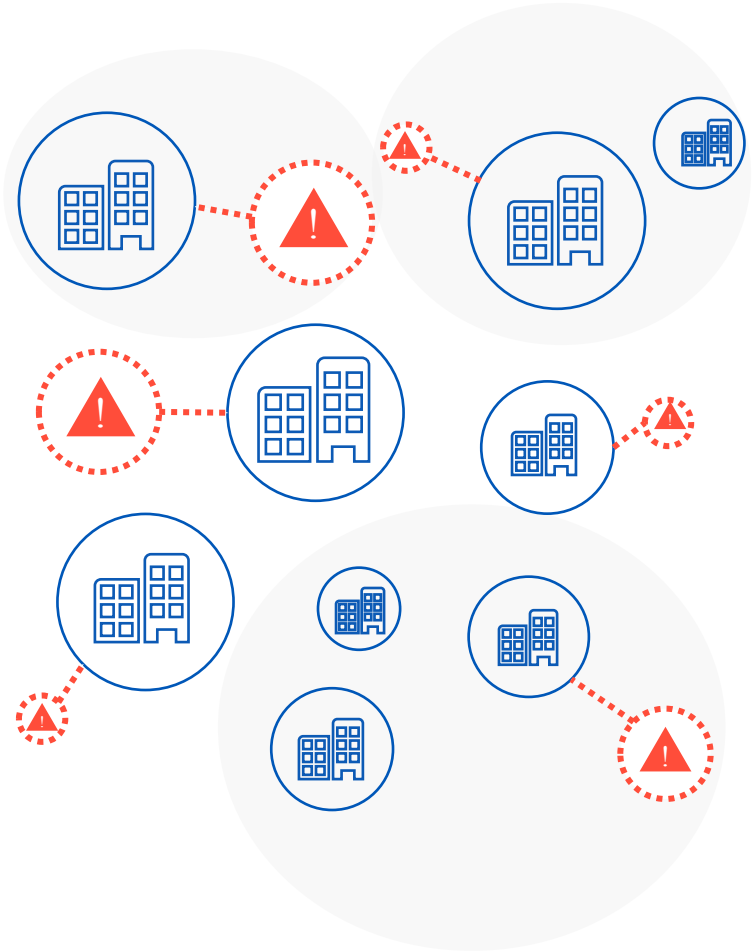
**WE SPEND LOTS OF MONEY**
on tools to protect ourselves.



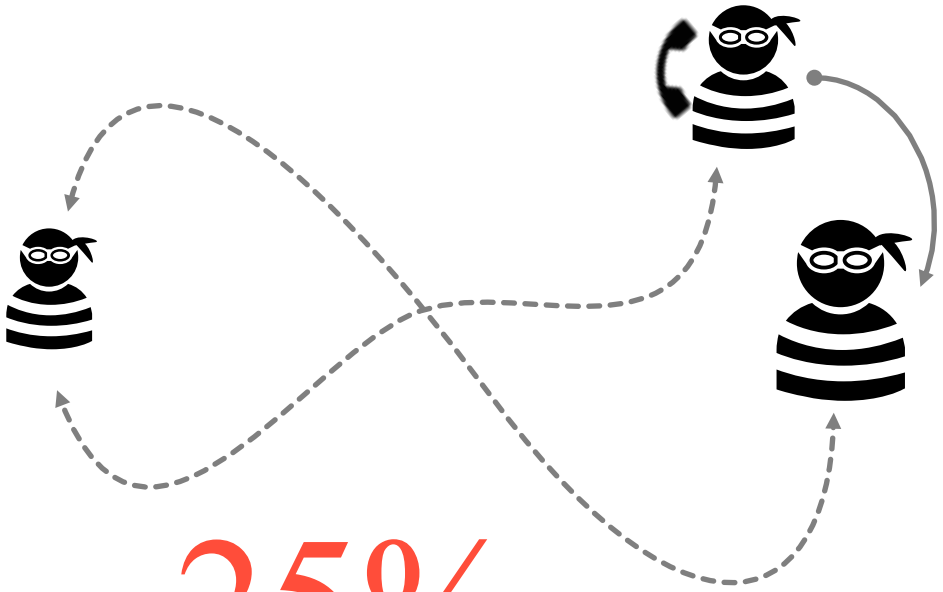

But, inevitably,
**THINGS GET THROUGH**
all the time…

…and we **CLOSE OURSELVES OFF**
to deal w/ security incidents in silos.

Meanwhile other companies across sectors experience **THE SAME EVENT!**



# So, what's wrong?

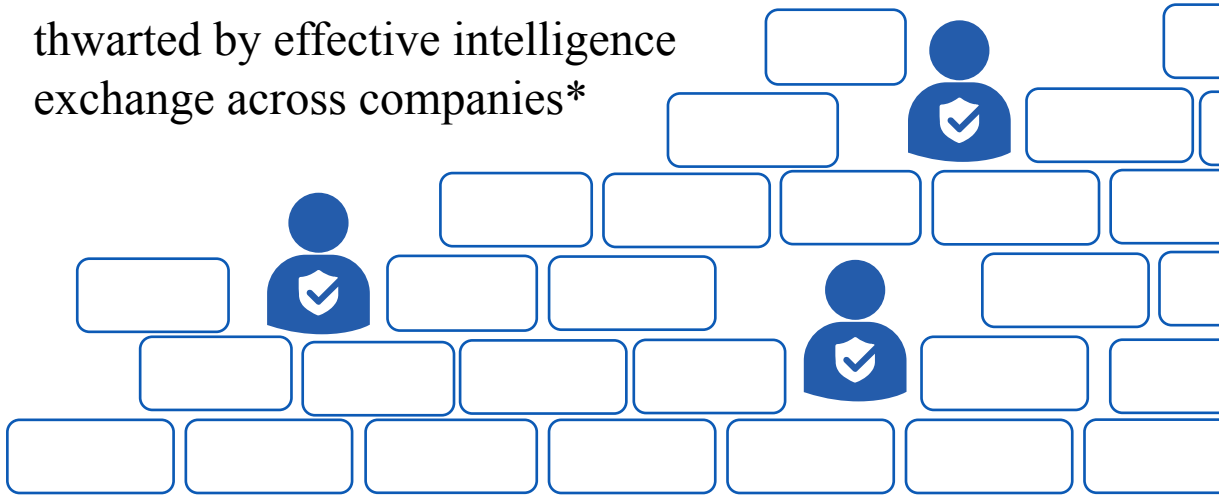


25%

Cyber attackers claim the #1 reason for their success is increased collaboration*

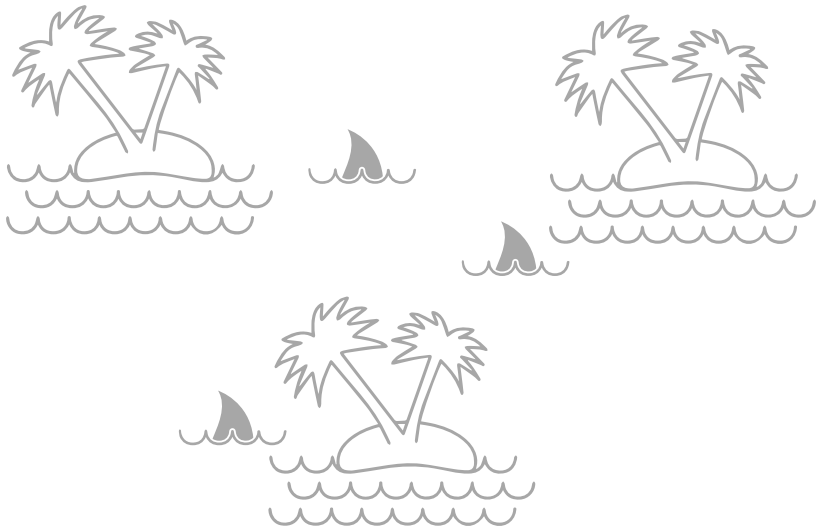
39%

Attacks that would have been thwarted by effective intelligence exchange across companies*

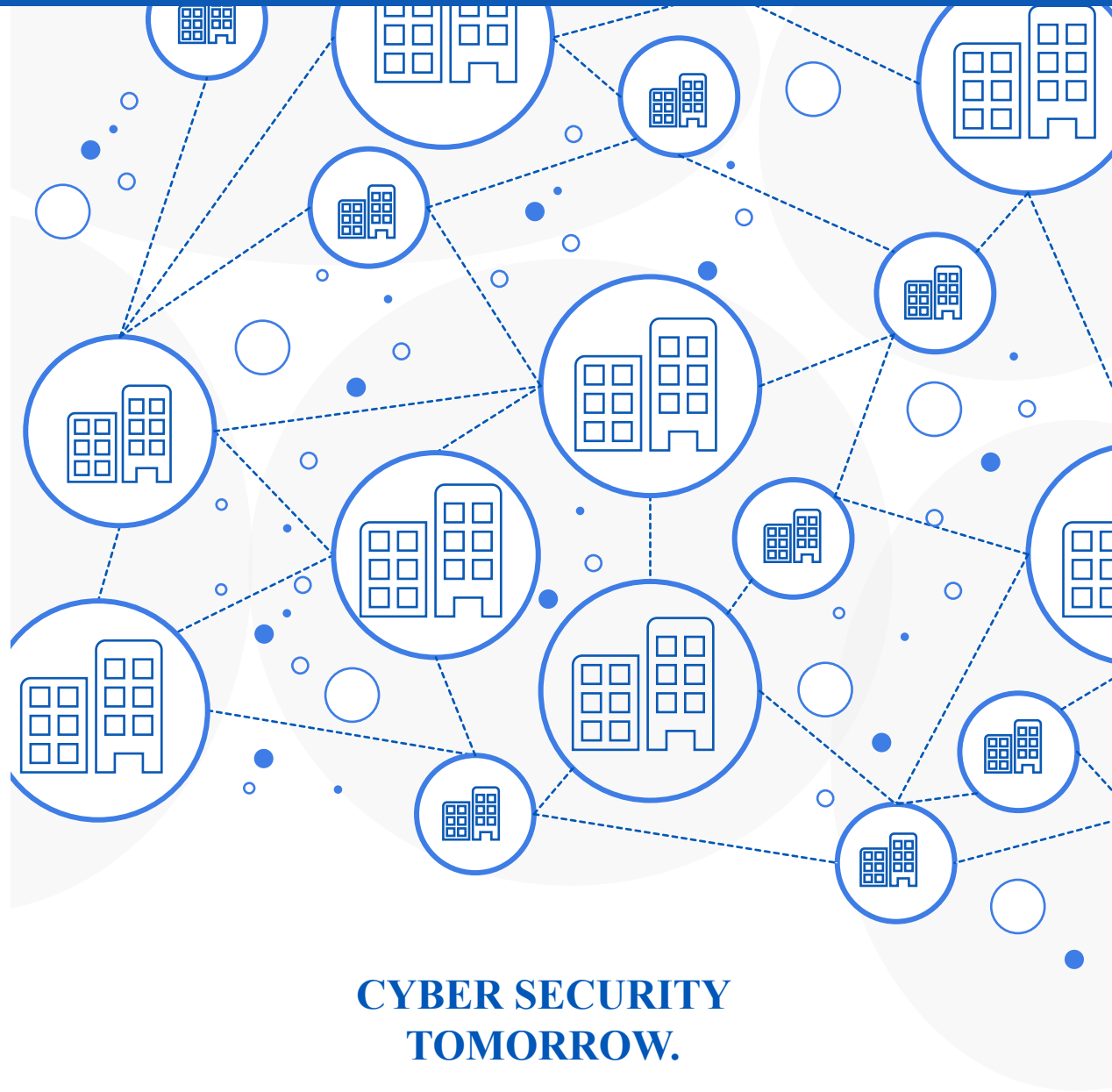


*2016 Flipping the Economics of Cyber Attacks - Ponemon + Palo Alto Networks

# We have to change.



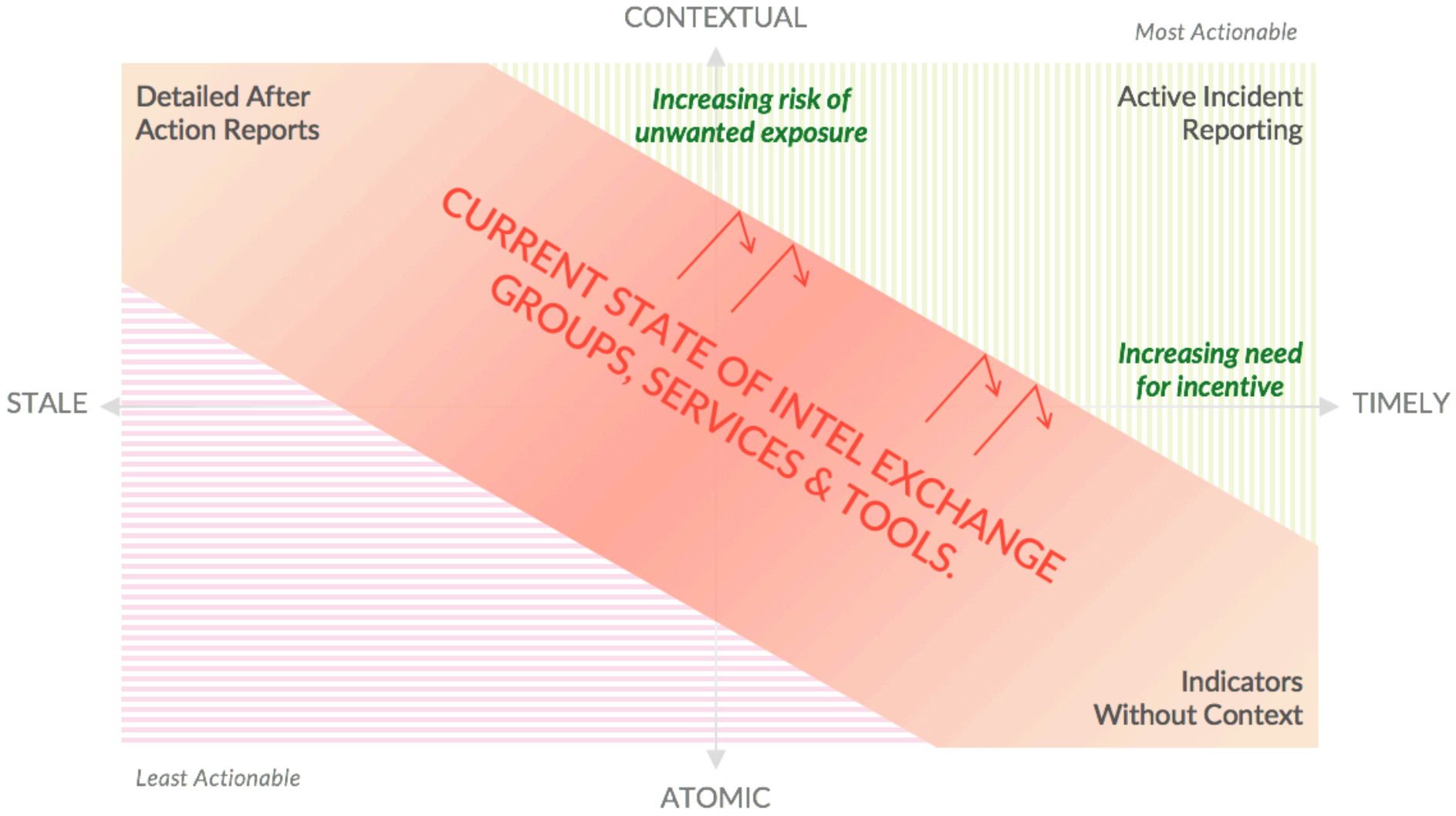
CYBER SECURITY TODAY



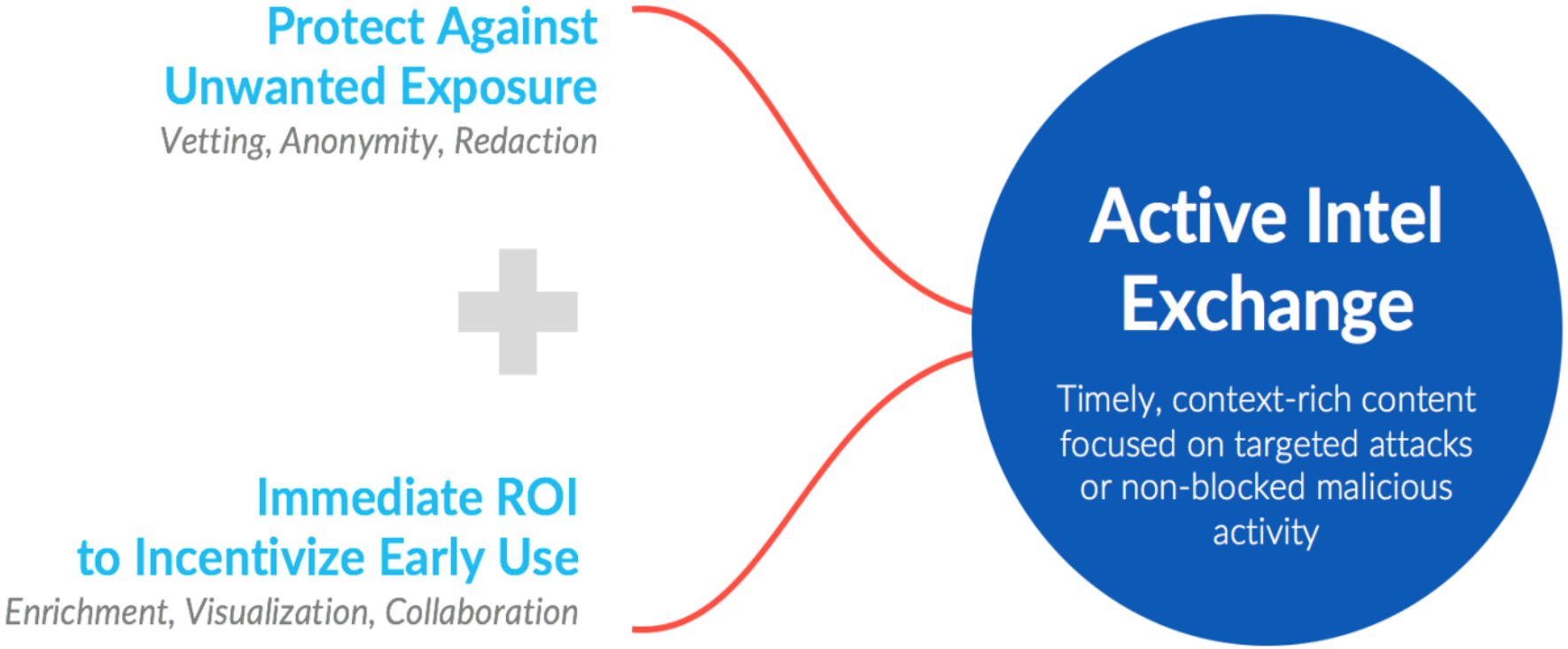
CYBER SECURITY
TOMORROW.

So, why hasn’t this happened yet?

# 15 years and still significant challenges in information “sharing”



# Exchange Network – Two key components



# Address protection against risk and incentive for operators in one solution.

## Manage Corporate Risk

*Innovative privacy-preserving technology addresses corporate risks*

## Provide Real Incentive

*Immediate value back incentivizes operators to exchange early in the IR process.*

**Auto-redaction sanitizes sensitive customer data client-side.**

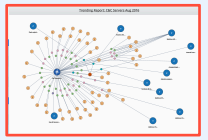
**Anonymous transport protocol authenticates data transmission without attribution.**

**Plug-&-play proxy capability obfuscates sending IP for the most sensitive of transmissions.**

## Incident Exchange Platform

**Timely, context-rich intelligence exchanged across teams, partners, groups and our global, vetted community.**

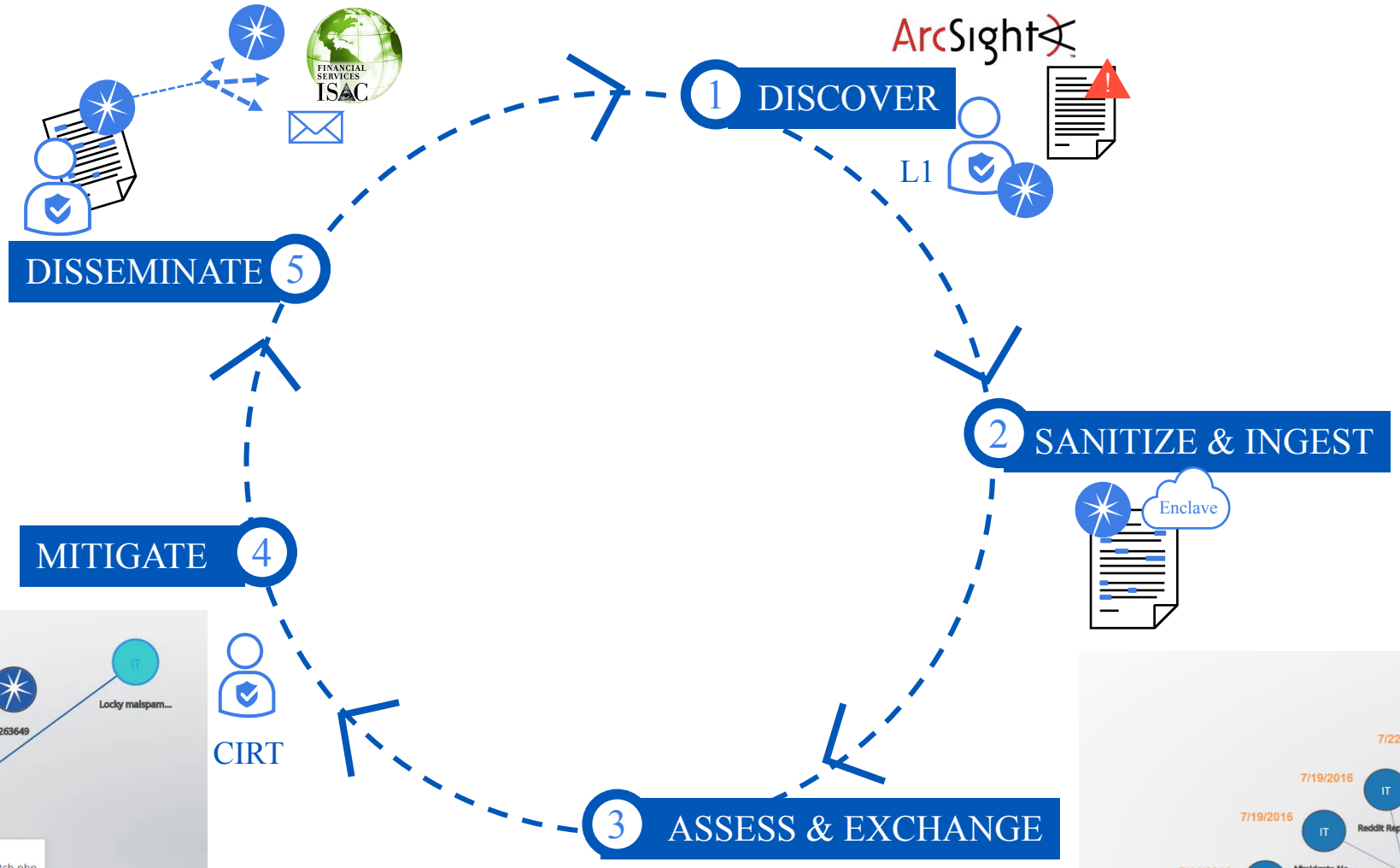
**Auto-extraction and correlation links to other incidents and other intel sources.**



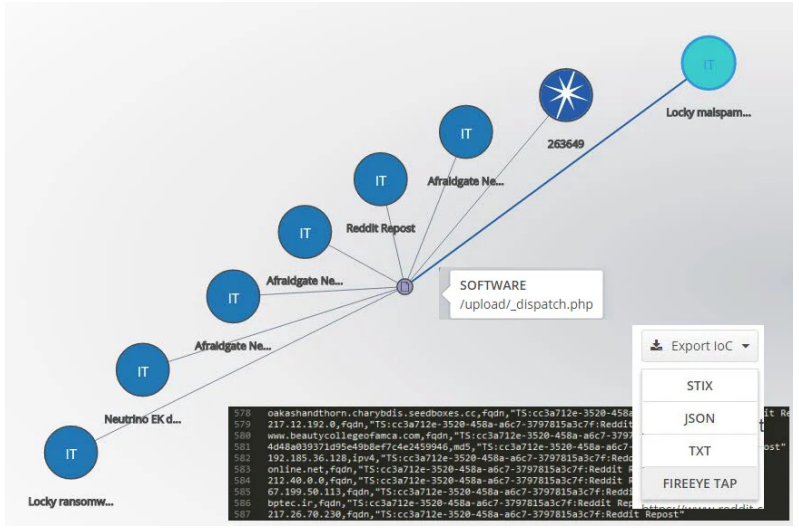
**Graph-based visual interface empowers the human infosec analyst.**

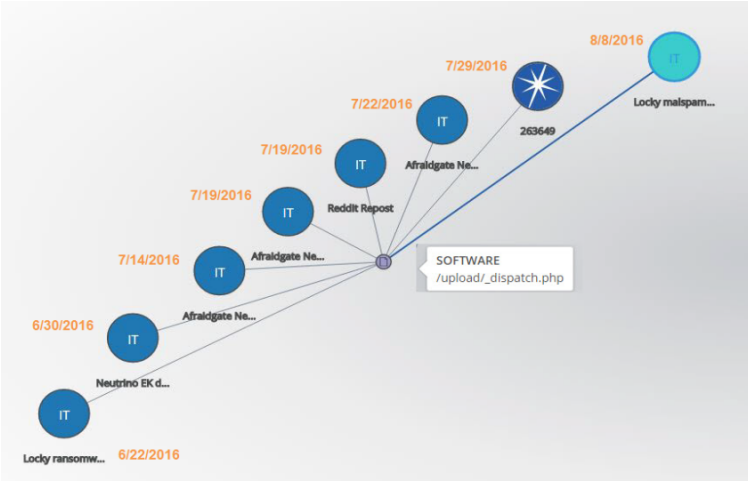

**Distro to multiple targets to scale collaboration across teams, partners, and groups.**

# So, how does it work?

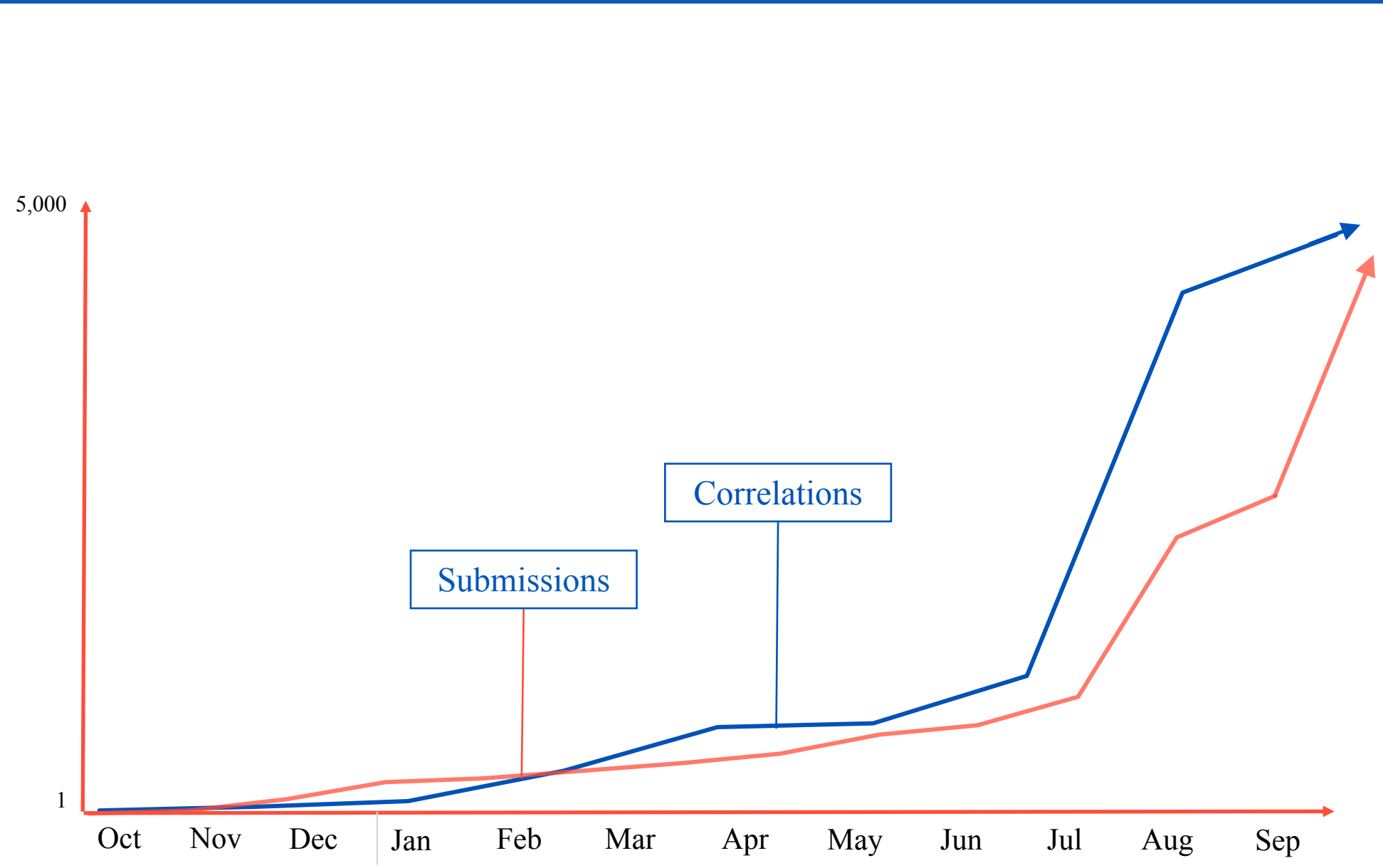



Threat: Locky Ransomware
Vulnerability: Adobe Flash
Campaign: Afraidgate
Exploit Kit: Neutrino



# The network effect drives a virtuous cycle.




## Context

**93%**

**Include valuable context**

## Timely

**43%**
**< 4hrs**

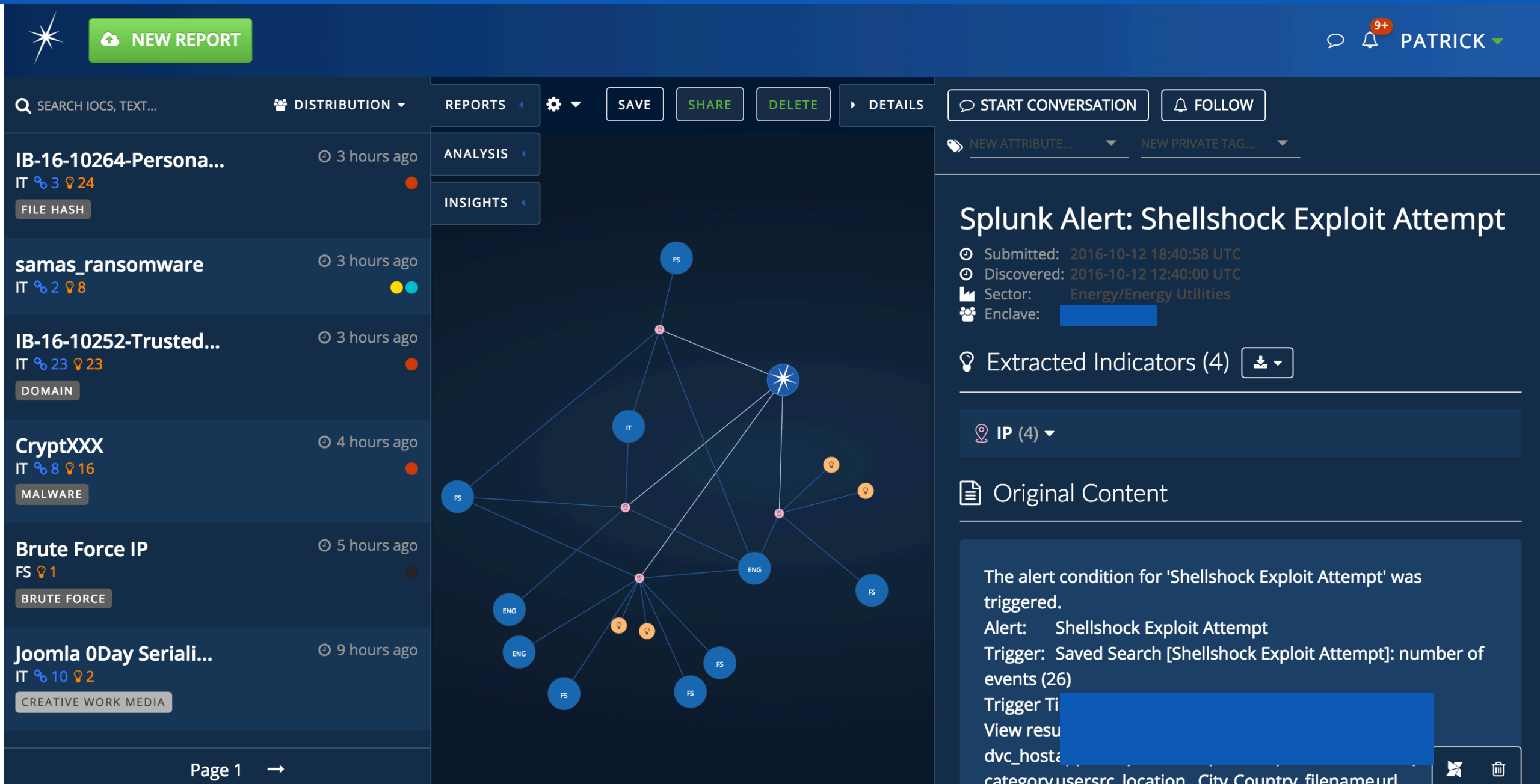
**87%**
**< 12hrs**

## Value

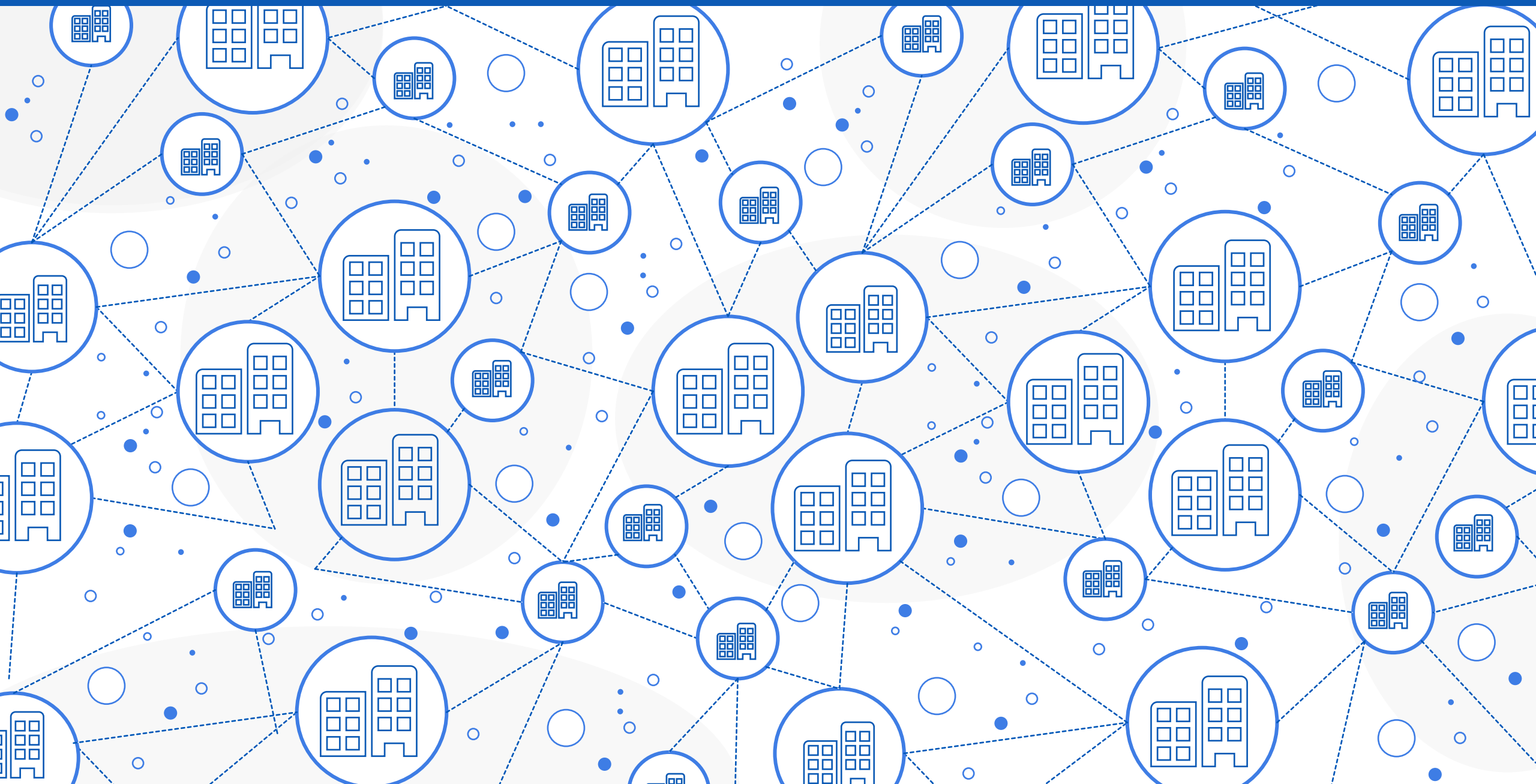
**15% → 65%**

**January Correlation %** | **September Correlation %**

# The Exchange



# This is the future.



A supply chain is a network between a company and its suppliers to produce and distribute a specific product, and the supply chain represents the steps it takes to get the product or service to the customer.

Supply Chain Definition | Investopedia

# Closing Quotes

“There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.”

Secretary Rumsfeld

An addition for cybersecurity….

“There is absolutely no reason to not to know what you can know.”

# What does this mean for the supply chain?

Recommendations:

- Establish a cyber security supply chain network to enable "connective defense" for space-related assets and systems.
- "Wrap up" your supply chain network to reduce risks and expedite investigation and mitigation.
- Ensure you know what you ~~should~~ must know.


# THANK YOU

pkurtz@trustar.co

# Massively Parallel Incident Exchange