ISSA

Information Systems Security Association
International

www.issa.org

ISSA Thought Leadership Webinar

The Threat Intelligence Playbook: Keys to Building Your Own Threat Intelligence

November 7, 2018

Today’s web conference is generously sponsored by:

DOMAINTOOLS®

Domain Tools
https://www.domaintools.com/

Keys to Building Your Own Threat Intelligence

Moderator

Chanel-Alexandria “C-A” Washington

Chanel-Alexandria “C-A” Washington is the founder and president of the Image & Etiquette Institute, a personal image and organizational branding firm dedicated to empowering clients using Appearance, Relationships, and Credibility to achieve their most important goals. Prior to becoming an author, speaker, and trainer, C-A served in numerous leadership roles in both state and federal government agencies, as well as in the private sector. C-A is an associate of the Georgia Chapter of the National Speaker’s Association, Emily Post Institute trained business etiquette trainer, former board member of the Association of Image Consultant’s International - DC Chapter, and alumna of the Harvard Kennedy School’s Women and Power program. With her experience and expertise, C-A specializes in helping leaders and teams convey excellence with civility, style, and charm because she firmly believes that with the right techniques and habits, we can *all* communicate with confidence and connect more authentically.

Speaker

Taylor Wilkes-Pierce, Sales Engineer, Domain Tools

Taylor Wilkes-Pierce, Sales Engineer at DomainTools has over 10 years of experience in technology sales with stops at Verizon, Amazon, and Virtuozzo along the way to DomainTools. Although Taylor loves all things infosec, he has a fond spot for container virtualization, software defined storage, and basketball.

Keys to Building Your Own Threat Intelligence

Speaker

Greg Reith, Sr. Solutions Architect, CenturyLink

Greg Reith began his career with U.S. Army Special Forces with a specialty in Operations and Intelligence. Greg's experience includes counter intelligence, intelligence analysis and collection at both tactical and strategic levels. At the end of his career in the military, he transitioned into Information Technology and was the Information Systems Security Officer responsible for securing Special Operations classified and unclassified networks.

Prior to CenturyLink, Greg led the T-Mobile threat intelligence team and developed the T-Mobile threat intelligence strategy and capability. Throughout his career Greg has worked for or consulted to organizations to include federal agencies, state agencies, multi state lottery, Microsoft, AT&T, T-Mobile, power companies, banks and other organizations. Greg's capabilities include but are not limited to, risk management, penetration testing and red-teaming, vulnerability management, security architecture, threat intelligence proofing and deploying security technologies among others

Greg has written multiple patents in the fields of threat intelligence, big data security and identity management.

Greg has been a speaker at multiple venues to include the Cloud Security Alliance, RFUN (Recorded Future Conference), ISACA, AGORA and others.

Keys to Building Your Own Threat Intelligence

Speaker

Ken Dunham, Senior Director, Technical Cyber Threat intelligence, Optiv

Ken Dunham brings more than 28 years of business, technical and leadership experience in cyber security, incident response and cyber threat intelligence to his position as senior director of technical cyber threat intelligence for Optiv. In this role, he is responsible for the strategy and technical leadership to mature Optiv's data integration and innovation of intelligence-based security solutions. He also runs his own advanced intelligence response company, 4D5A Security LLC, and a non-profit for incident responders around the world called Rampart Research. Mr. Dunham has a long history of innovation for nascent technologies and solutions such as creation of training programs for U2, Warthog, and Predator systems for the USAF, responsible disclosure (iDEFENSE), and cyber threat intelligence (iSIGHT Partners). He is a widely published author with thousands of security articles and multiple books on topics ranging from Darknet disclosures to mobile threats and mitigation of malware.

Speaker

Taylor Wilkes-Pierce, Sales Engineer, Domain Tools

Taylor Wilkes-Pierce, Sales Engineer at DomainTools has over 10 years of experience in technology sales with stops at Verizon, Amazon, and Virtuozzo along the way to DomainTools. Although Taylor loves all things infosec, he has a fond spot for container virtualization, software defined storage, and basketball.

Threat Data Versus Intelligence

Threat Data

is a piece of information. Data must be analyzed to provide context.

Threat Intelligence

is the process of performing contextualized analysis against threat data

The difference between threat data and threat intelligence is **analysis**

Indicators of Compromise and Attack are part of **both**

Understanding IOCs

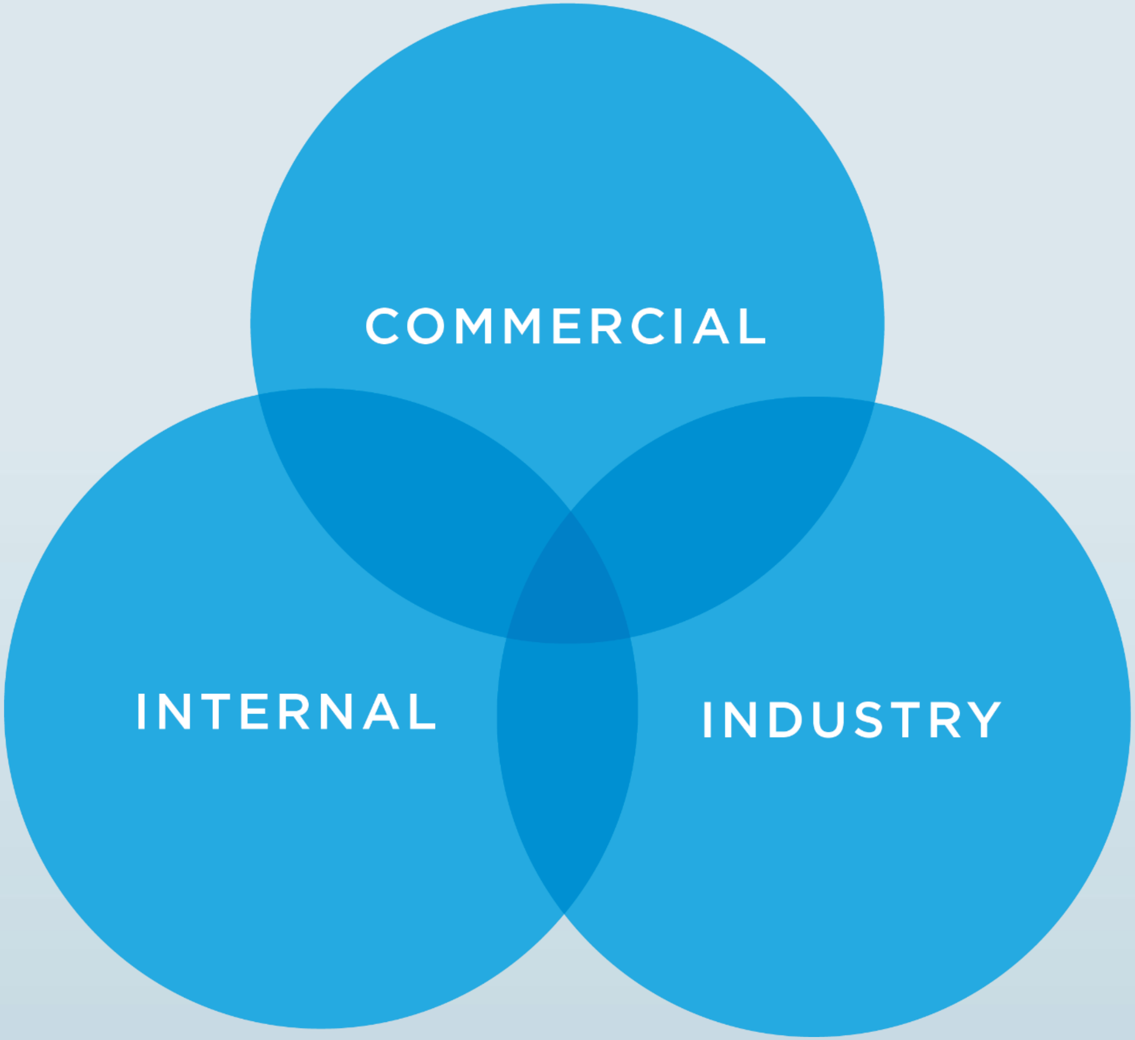
Command and control domains and DNS requests, which provide Pivot points to look for additional attacker infrastructure

File attributes, such as filenames, file languages and vulnerable file types that raise red flags

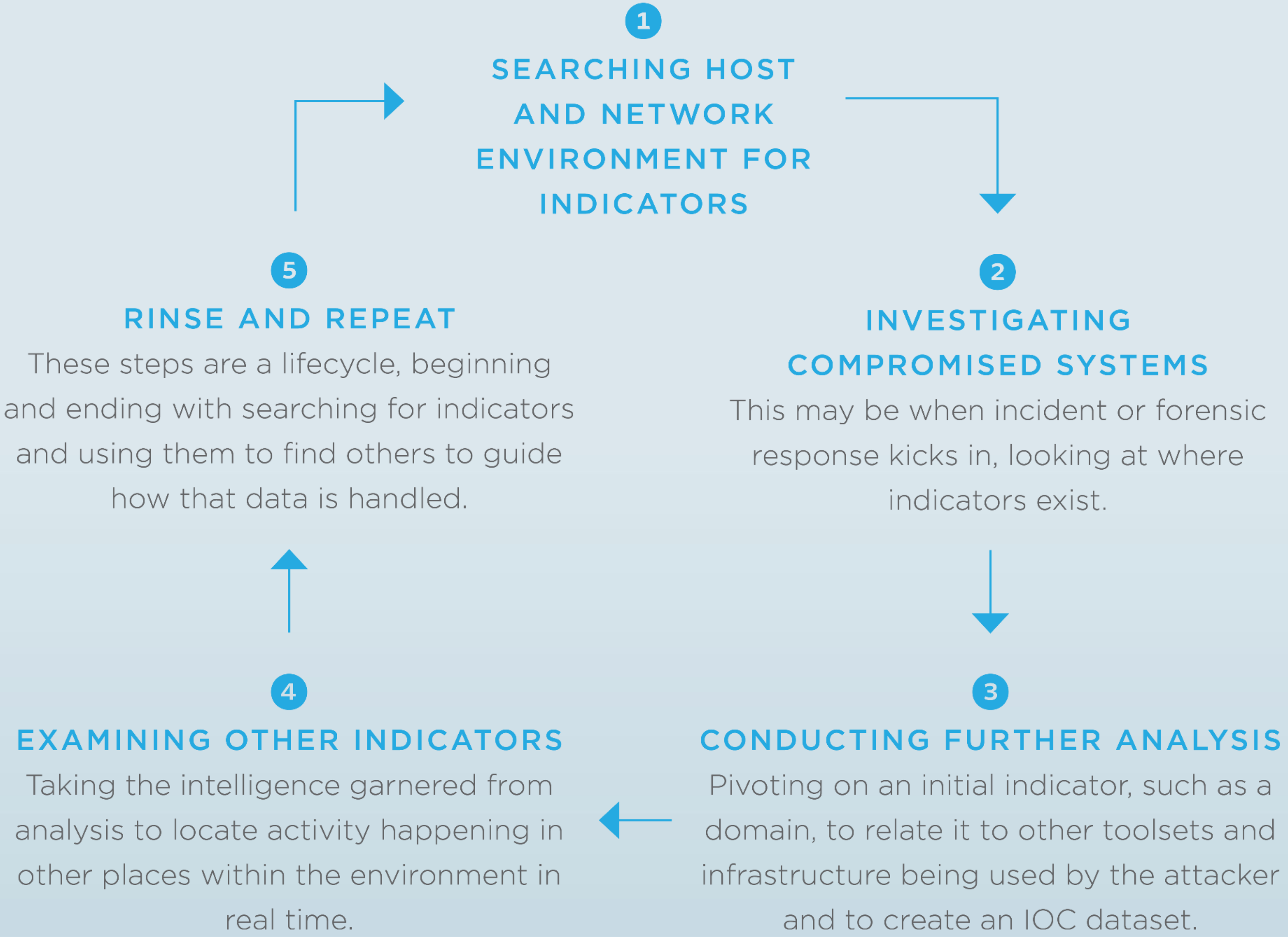
IP addresses, similar to domains, can be explored in Passive DNS to uncover more about an attacker

Hashes, when on a host or network can be analyzed for maliciousness – and because they are unique. They can quickly reveal additional important information

Where do IOCs Come From?



IOC Workflow



1 SEARCHING HOST AND NETWORK ENVIRONMENT FOR INDICATORS

2 INVESTIGATING COMPROMISED SYSTEMS

This may be when incident or forensic response kicks in, looking at where indicators exist.

3 CONDUCTING FURTHER ANALYSIS

Pivoting on an initial indicator, such as a domain, to relate it to other toolsets and infrastructure being used by the attacker and to create an IOC dataset.

4 EXAMINING OTHER INDICATORS

Taking the intelligence garnered from analysis to locate activity happening in other places within the environment in real time.

5 RINSE AND REPEAT

These steps are a lifecycle, beginning and ending with searching for indicators and using them to find others to guide how that data is handled.

Understanding IOAs

Unknown Attributes:

>> Firewall rule logs

>> SIEM logs

>> Proxy rule logs

IOC Analysis:

>> IDS/IPS logs

>> AV logs

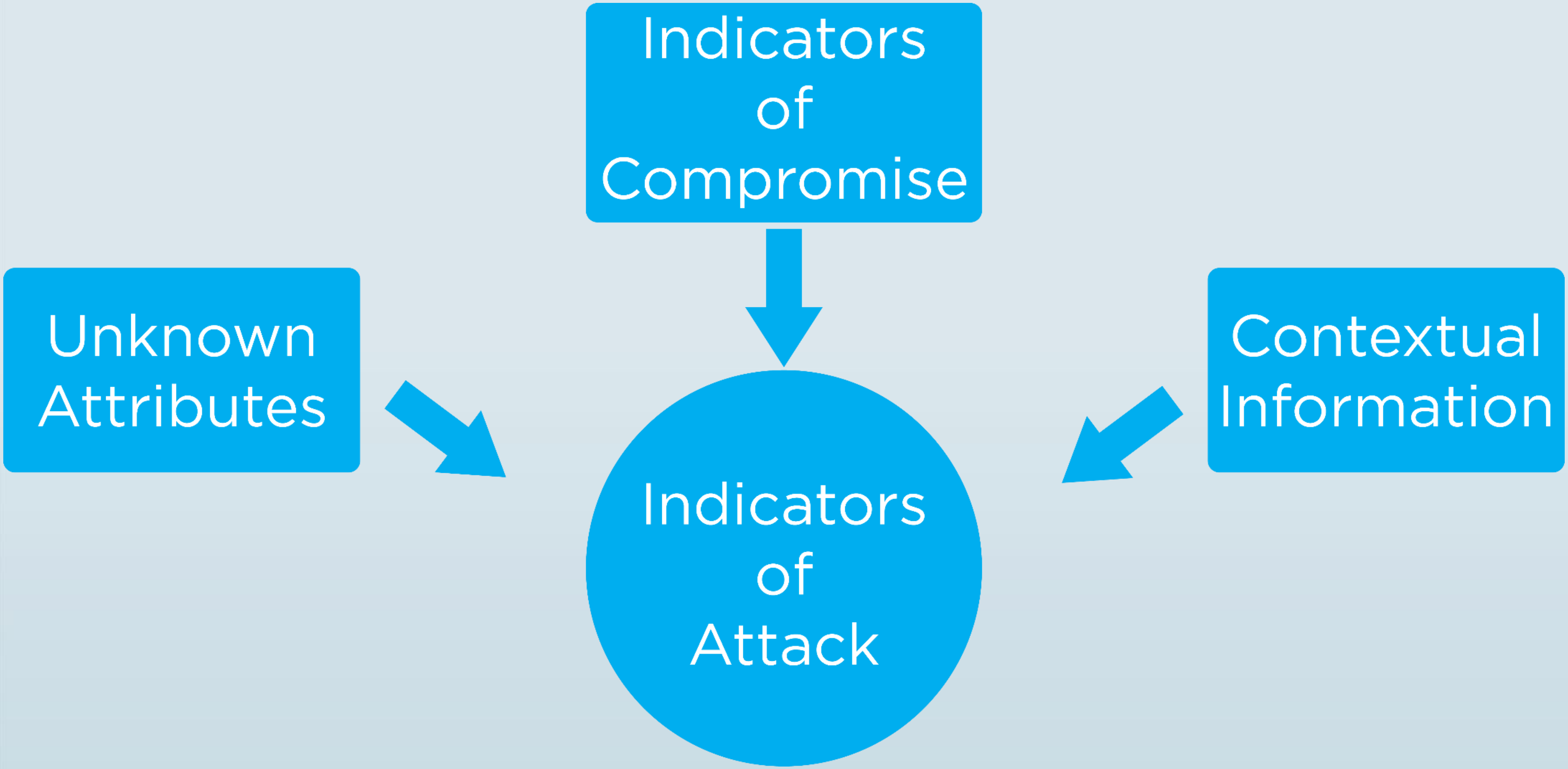
>> Endpoint security logs

Contextual Information:

>> Network Infrastructure logs

>> Application/Database/Web server logs

What is an IOA



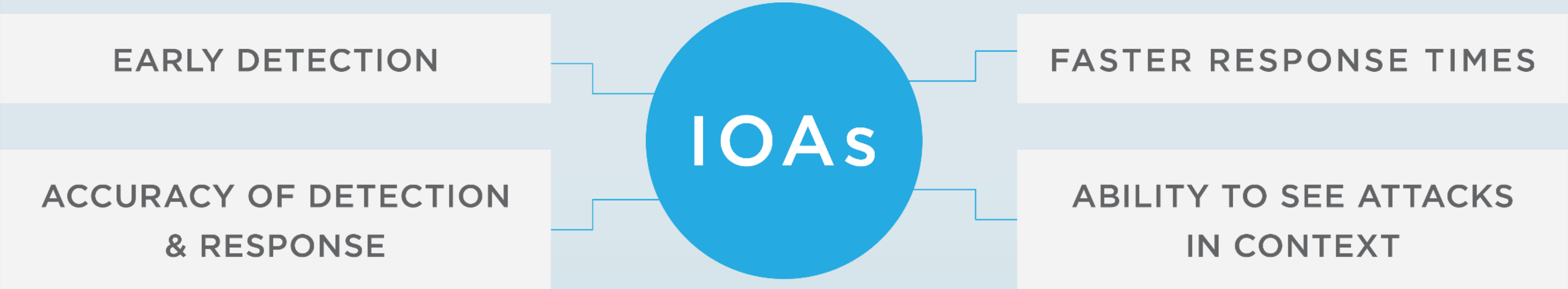
Indicators of Compromise

Unknown Attributes

Contextual Information

Indicators of Attack

Understanding IOAs



IOAs

EARLY DETECTION

ACCURACY OF DETECTION & RESPONSE

FASTER RESPONSE TIMES

ABILITY TO SEE ATTACKS IN CONTEXT

IOC Versus IOA

IOCs

- Reactive
- Historical
- Known Bad
- Malware
- Signatures
- IPs
- Domains
- Vulnerabilities

IOAs

- Proactive
- Real-time
- Own Environment
- Code execution
- User behavior
- Malware behavior
- Persistence
- Stealth

Your Threat Intelligence Playbook

Speaker

Greg Reith, Sr. Solutions Architect, CenturyLink

Greg Reith began his career with U.S. Army Special Forces with a specialty in Operations and Intelligence. Greg's experience includes counter intelligence, intelligence analysis and collection at both tactical and strategic levels. At the end of his career in the military, he transitioned into Information Technology and was the Information Systems Security Officer responsible for securing Special Operations classified and unclassified networks.

Prior to CenturyLink, Greg led the T-Mobile threat intelligence team and developed the T-Mobile threat intelligence strategy and capability. Throughout his career Greg has worked for or consulted to organizations to include federal agencies, state agencies, multi state lottery, Microsoft, AT&T, T-Mobile, power companies, banks and other organizations. Greg's capabilities include but are not limited to, risk management, penetration testing and red-teaming, vulnerability management, security architecture, threat intelligence proofing and deploying security technologies among others

Greg has written multiple patents in the fields of threat intelligence, big data security and identity management.

Greg has been a speaker at multiple venues to include the Cloud Security Alliance, RFUN (Recorded Future Conference), ISACA, AGORA and others.

Developing Warning Intelligence

Greg Reith CenturyLink NW SAT, advisor to Center for Threat Intelligence

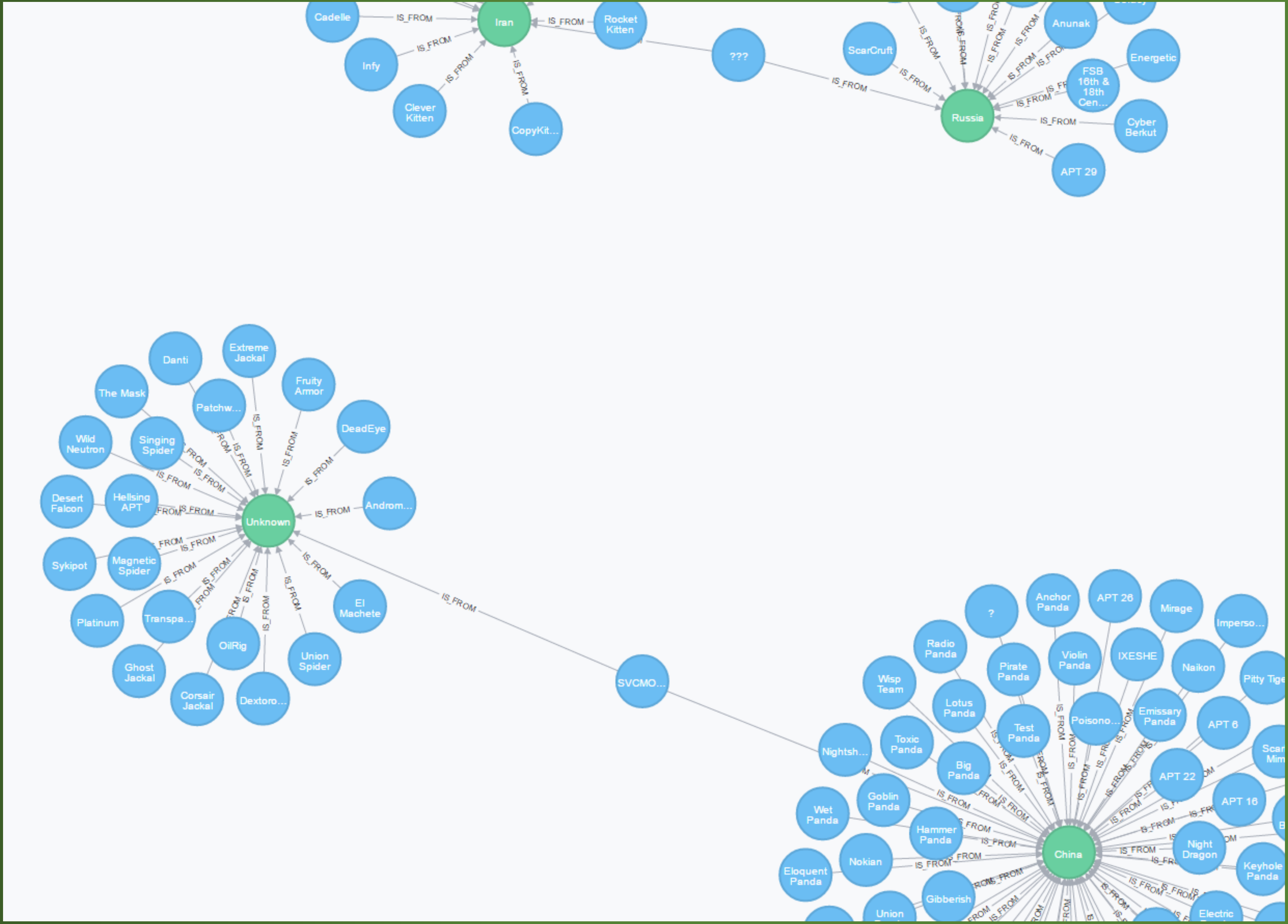
Warning Intelligence

- Predictive or pre-emptive intelligence, an educated prediction
- Tactical: Short term warning that attack is underway or so imminent that assets may not be brought to bear, requires dedicated response
- Strategic: Warnings or judgements made early enough to allow decision makers to take pre-emptive action
- Developed over time, in many cases historical data can be more relevant than current data
- IOAs and IOCs can provide indications as to how an adversary will act or react
- A primary goal of an intelligence team should be to provide Warning Intelligence

DEVELOPING EARLY WARNING

- Graph structures are good for developing unknowns via dynamic relationship linking on ingestion
- Attacks happen over time, Warning Intelligence has to be inclusive of over time indicators
- Management in many cases is not objective or goal based but managed by discovery

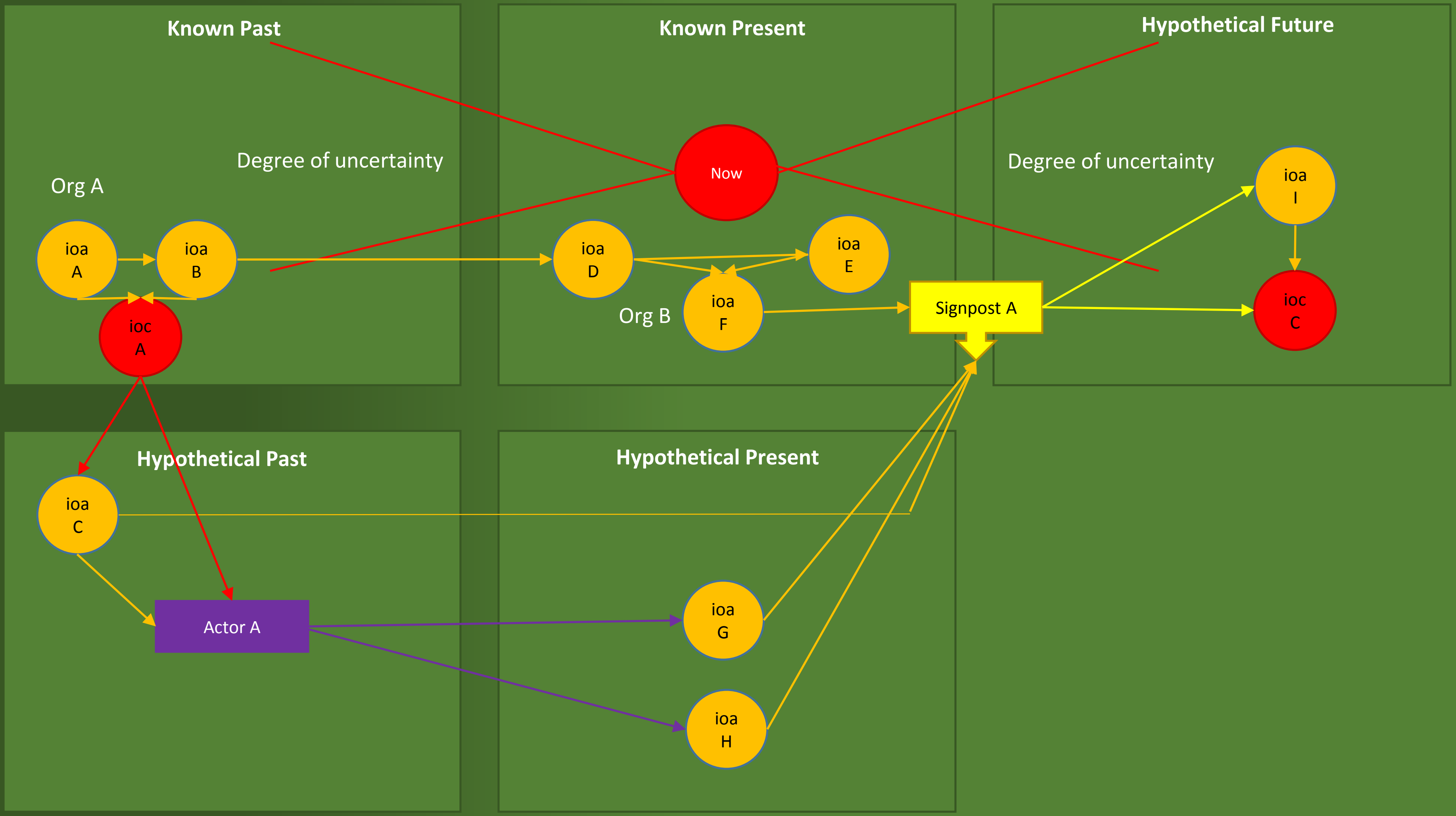
Graph Engines



COMPONENTS

- Known Components
  - Historical
  - Present
- Hypothetical components
  - Historical
  - Trending/present
- Hypothetical future

Warning Space and Time



REAL WORLD

- Organized crime group begins new POC
- IOAs and IOCs extraction
- Historical data correlation re: POC and timing of new campaigns
- Develop signposts for hypothetical components based on adversarial focus and tradecraft
- Detection of signpost crossings
- Monitor for indications of new IOAs and IOCs based on signpost indicators and newly developed IOAs and IOCs from signpost crossings

Keys to Building Your Own Threat Intelligence

Speaker

Ken Dunham, senior director of technical cyber threat intelligence for Optiv

Ken Dunham brings more than 28 years of business, technical and leadership experience in cyber security, incident response and cyber threat intelligence to his position as senior director of technical cyber threat intelligence for Optiv. In this role, he is responsible for the strategy and technical leadership to mature Optiv's data integration and innovation of intelligence-based security solutions. He also runs his own advanced intelligence response company, 4D5A Security LLC, and a non-profit for incident responders around the world called Rampart Research. Mr. Dunham has a long history of innovation for nascent technologies and solutions such as creation of training programs for U2, Warthog, and Predator systems for the USAF, responsible disclosure (iDEFENSE), and cyber threat intelligence (iSIGHT Partners). He is a widely published author with thousands of security articles and multiple books on topics ranging from Darknet disclosures to mobile threats and mitigation of malware.

Cyber Threat Intelligence Integration

Ken Dunham, Senior Director, MSS Technical Director

Technical Cyber Threat Intelligence

MTE, CISSP, GCFA Gold, GCIH Gold, GSEC, GREM Gold, GCIA, CISM

Cyber Threat Intelligence

- www.optiv.com/resources/blog
- Hint: How does information differ from intelligence (Intel)?
- Hint: How is an indicator of compromise (IOC) different from Intel?
- Hint: Think HOW you’ll get there and WHAT you want to do…ACTION

OPTIV DEFINITION OF CTI

***CTI** is an ecosystem supportive of the decision making process derived from the collection, analysis, dissemination and integration of threats and vulnerabilities to an organization and its people and assets.*

Optiv recommends considering four essential attributes of threat agents mapped back to a security posture, as well as six essentials courses of action, known as threat modeling, in order to properly produce, consume and act upon CTI.

https://www.optiv.com/blog/operationalizing-a-cyber-threat-intelligence-solution

Contextualized Risk Management

What am I trying to protect?

Have you identified your crown jewels and how they are both protected and at risk?

Do you know who/what you are protecting it from?

Do you have a plan for protecting your assets from actors or risk identified?

Threat Agents

Non-Hostile

- Reckless employee
- Untrained employee
- Partners

Hostile

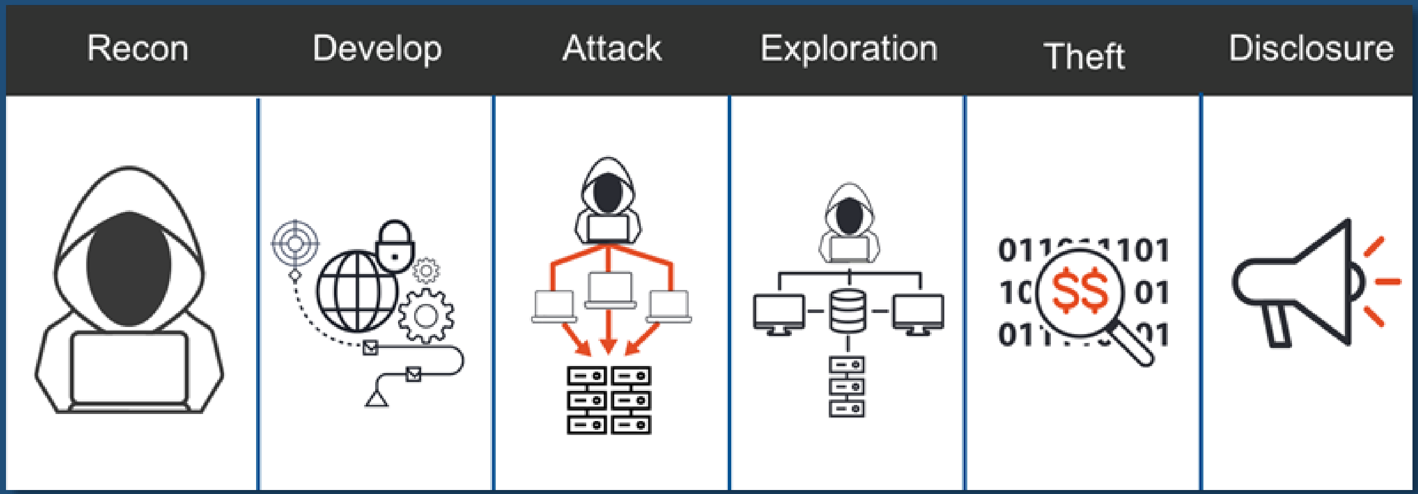
- eCrime
- Nation-state cyber warrior
- Industrial espionage
- …

Intent: theft, disruption, reputation …

Threat Agent Attributes

- **Composition and Strength**: individual or group/association?
- **Tactics**: historical or expected course of action?
- **Logistics**: infrastructure, architecture, operations
- **Effectiveness**: how effective are their attacks; in the future?

Threat Agent Courses of Action



Recon

Develop

Attack

Exploration

Theft

Disclosure

Actionability

Not just a buzz word.
Within CTI it must be:

- Timely
- Relevant and Specific
- Actionable
- Lower or Mitigate Risk

Agent.ABC

- “Agent“ downloader Trojan detected and removed.
  - Wipe & Forget attitude
  - What is it attempting to download?
  - Do we have any IOCs for that secondary+ payload?
  - It is common for other variants of Agent to bypass our security solutions, not being detected, how will you identify such risks and/or mitigate from your network?

“The threat of the *unknown* is one of our greatest risks…”

Real World Example: Email Found on DarkWeb

YourName@company.com

- Date & Time?
- Where and who had this on the DarkWeb?
- Captured for spam?
- Stolen credentials?
    - Universal Credentials?
- Targeted campaign?
- Without any context what will you do?

Oregon Trail Priorities

What Are Your Priorities?

Collect global IOCs to supplement your software and solutions?

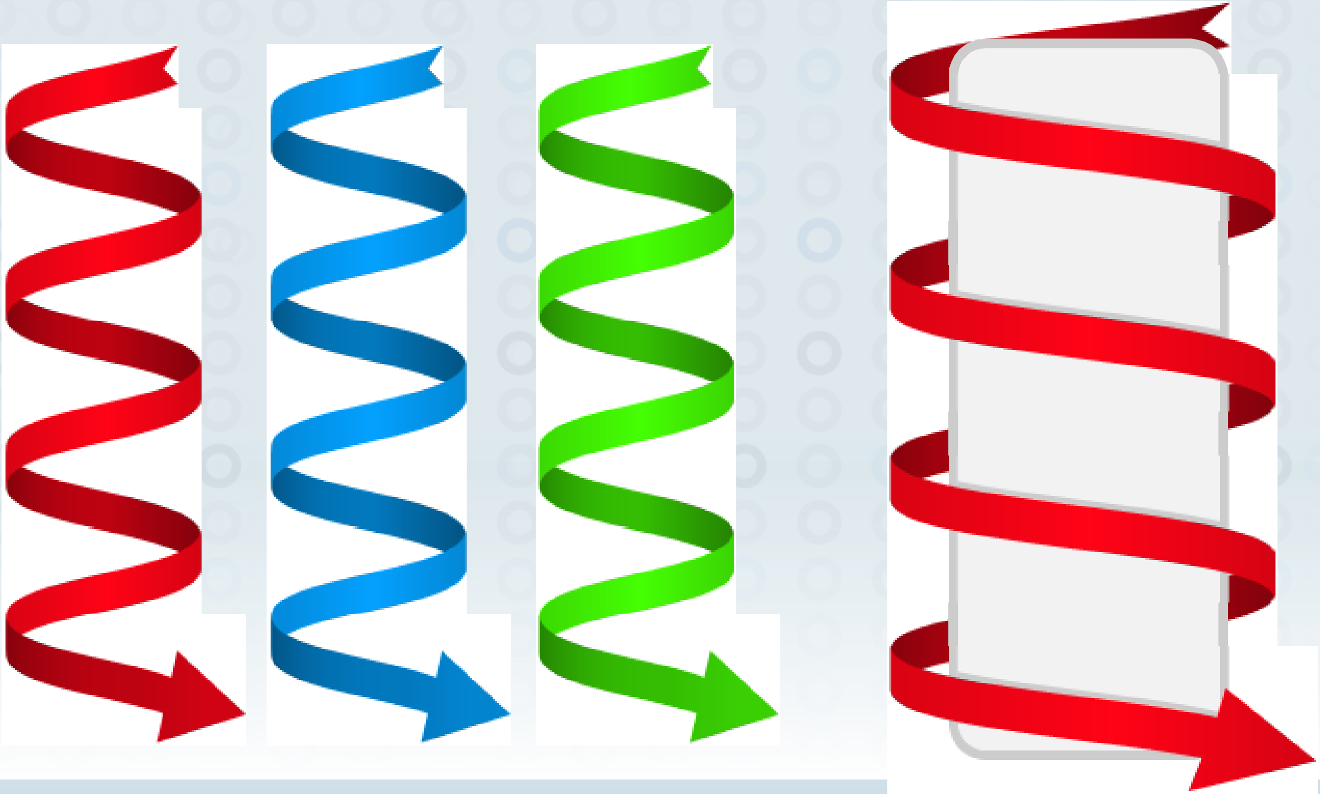
Mistake: TTPs often include one time use of domains and IPs or abuse of legitimate websites. How does global IOC data aid in fighting against these types of threats? Useful but should *not* be the focus.

Manage Internally SIEM/SOC operations and optimize?

Mistake: Internal resources are best spent on advanced analysis and integrated risk management. Most mature organizations use third-party providers for low skill high volume roles such as this. There are *few* too many trained and experienced experts; use them wisely.

Efficiently and effectively LOWER RISK against crown jewels!

Bi-Direction Intelligence Enablement



You NEED Dedicated Staff

You NEED community and sharing within your sector, especially with friendenemies.

(ISC)²®
ISSA™
Information Systems Security Association
The Global Voice of the Information Security Profession
High Technology Crime Investigation Association
HTCIA
INFRAGARD
PARTNERSHIP FOR PROTECTION
ISACA®
Trust in, and value from, information systems
28

Leadership Is Your Most Important Priority

This Guy?

Or This Guy?

Most people fail not because they aim too high and miss, but because they aim too low and hit.

– Les Brown

Questions

Ken Dunham

Senior Director

MSS Technical Director

Technical Cyber Threat Intelligence

MTE, CISSP, GCFA Gold, GCIH Gold, GSEC, GREM Gold, GCIA, CISM

Ken.Dunham@optiv.com

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?