knowledge17

WORK at LIGHTSPEED

Threat Hunting, Awareness, and Sharing with Security Operations

Alex Yupanqui
Senior Solutions Architect
ServiceNow

Antoni Kew
Advisory Solutions Architect
ServiceNow

Scott Lewis
Sr. Product Manager
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Speaker Introduction



Name: Alex Yupanqui

Title: Senior Solutions Architect

Function: Supporting Enterprise Customers in the West

Company: ServiceNow – Santa Clara Office

Experience: Alex has served for 5 years at ServiceNow where he has consistently been focused on helping our customers adopt the ServiceNow platform. Alex has held several pre-sales and development roles covering a wide range of solutions.

Current Projects: Working with several customers on Vulnerability Response

Interests: All things AUTOMATION!

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Antoni Kew

Title: Advisory Solution Architect

Function: Security Business Unit

Company: ServiceNow

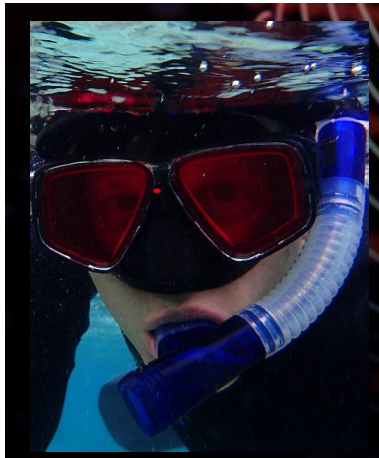
Experience: Held various positions in Security and Risk, Ops, and Service Delivery at several companies. Prior to ServiceNow, I was Sr Solutions Consultant at a threat intel startup, and prior to that I was a Security and Risk Program Manager on the Microsoft Azure Team.

Current Projects: Helping customers identify opportunities for streamlining Security Operations!

Interests: Building things, sailing, travel and spending time with my Family.

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Scott Lewis

Title: Sr. Product Manager

Function: Security Business Unit

Company: ServiceNow

Experience: VP, Product Delivery BrightPoint Security; Sr. Director Product Management LiveOps; Lead Program Manager, Microsoft MSN.

Current Projects: Optimizing the analyst experience when working through security incidents and adding more capabilities to threat intelligence sharing.

Interests: Nature photography, snorkeling, and tomatoes (lots of tomatoes)

© 2017 ServiceNow All Rights Reserved

Objectives and What You Will Learn

Objectives

- Learn how you can leverage Service Now to accelerate your incident response process using threat intelligence and by interacting with peers.

What you will learn

- You’re not alone!
- How to improve your situational awareness
- Benefits of shared threat intelligence
- Make sharing actionable

© 2017 ServiceNow All Rights Reserved

Why share threat intelligence?

- The bad guys share tools, tactics and procedures.
- When an attack is successful, the bad guys use the same attack on similar targets.
- Traditional threat intelligence providers do not necessarily provide intelligence that is timely or relevant enough to identify these attacks early.

Immunity by Community

© 2017 ServiceNow All Rights Reserved

Sharing Today

How do we share today?

- ISACs
- Infraguard
- Emails/Attachments
- Forums
- Open Source Feeds

Sharing is happening , but it is generally slow, manual and person-to-person. Not Scalable, consistent or measurable

© 2017 ServiceNow All Rights Reserved

ISACs

National Council of ISACs

HOME | ABOUT NCI | ABOUT ISACS | MEMBER ISACS | EVENTS | PUBLICATIONS | MEDIA | CONTACT



ISACs are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators.

Join your sector's ISAC today.

Sector-based Information Sharing and Analysis Centers collaborate with each other via the National Council of ISACs. Formed in 2003, the NCI today comprises 24 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. Critical infrastructure sectors and subsectors that do not have ISACs are invited to contact the NCI to learn how they can participate in NCI activities.

Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

© 2017 ServiceNow All Rights Reserved











































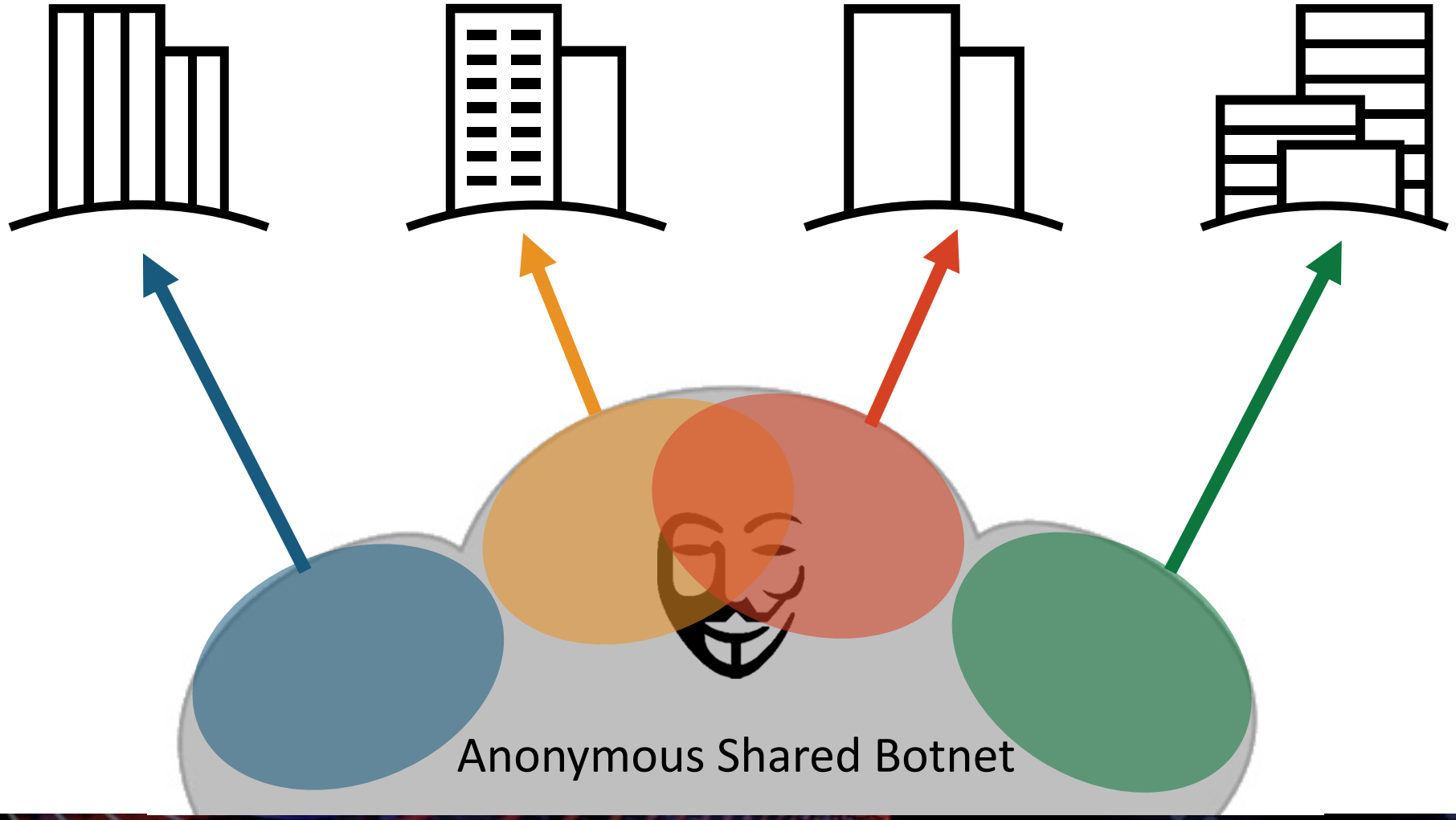
© 2017 ServiceNow All Rights Reserved

Operation Payback

- Series of DDoS attacks organized by users of 4chan's /b/ (random) board that started on September 17th, 2010
- Initial target was major entertainment industry websites such as the websites for the RIAA MPAA
- Beginning on December 7th, 2010, Anonymous led a series of DDos assaults under the moniker of Operation Avenge Assange and successfully brought down Paypal, Visa and MasterCard's websites. Other impacted sites were Amazon, Swiss Postal Finance as well as a number of U.S. government websites and various cybersecurity contractor firms

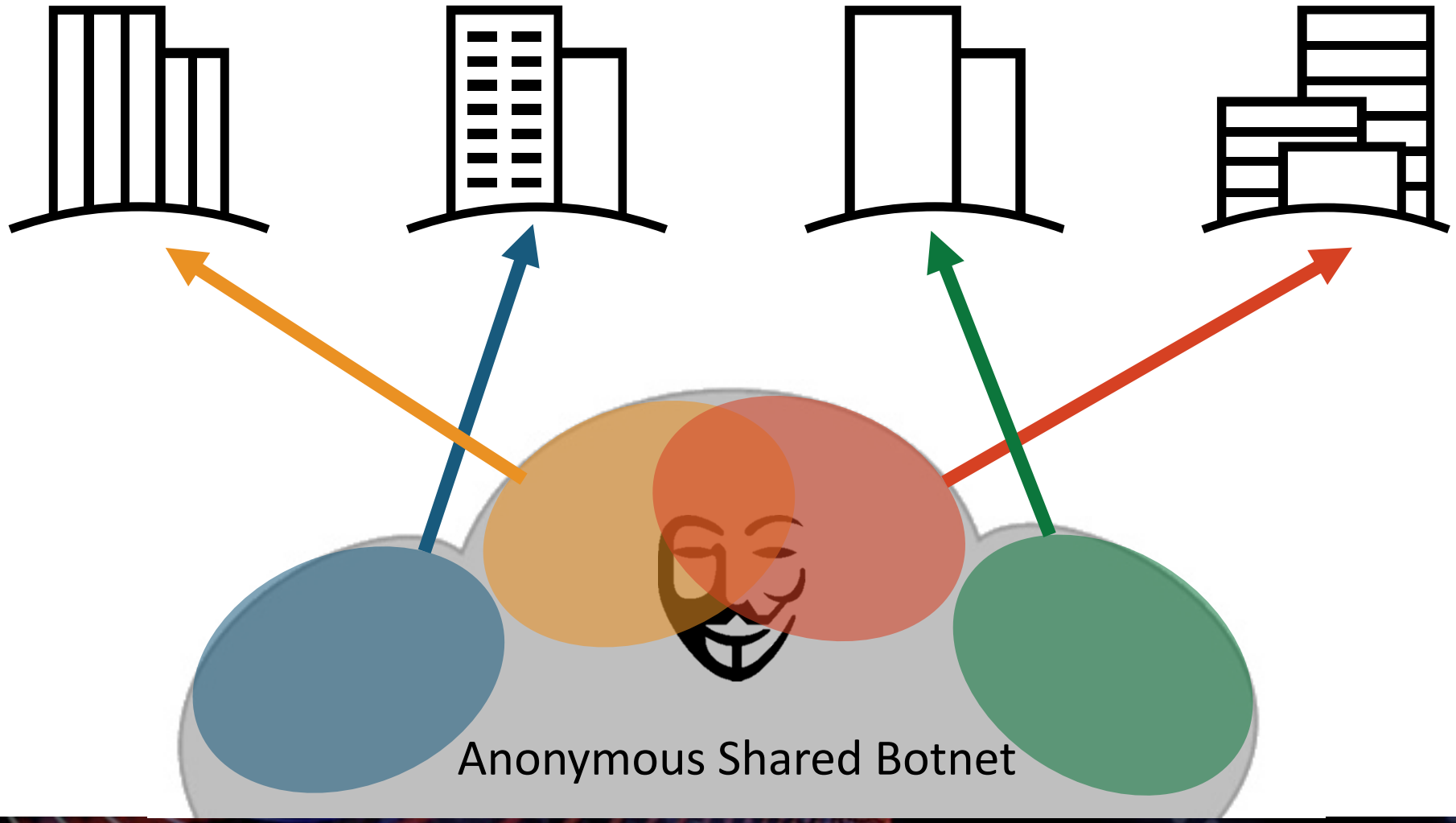
© 2017 ServiceNow All Rights Reserved

Operation Payback



© 2017 ServiceNow All Rights Reserved

Operation Payback



© 2017 ServiceNow All Rights Reserved

Improving the Response

- Sharing
- Automation
- Enrichment
- Context

© 2017 ServiceNow All Rights Reserved

The Importance of Situational Awareness – 3 Questions

- Is it happening to anyone else, or just me?
- What should I do about it?
- What is my response relative to my peers? How is the attack morphing around me? How can I respond in whole to the threat, instead of just the parts I can see?

© 2017 ServiceNow All Rights Reserved

How do we share at the speed of light?

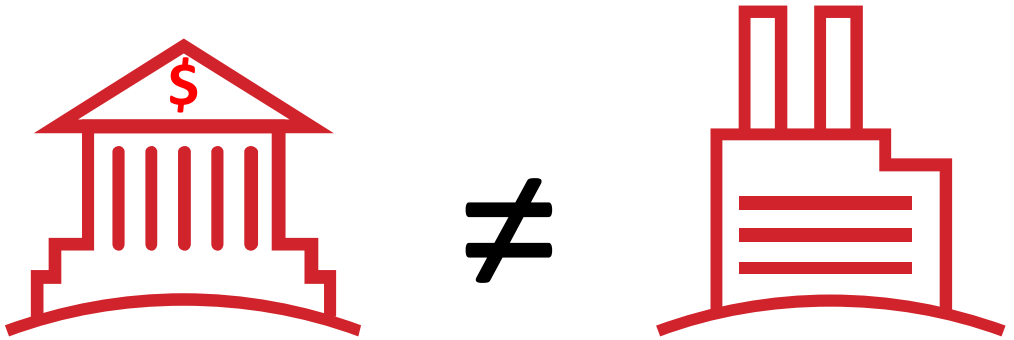
- Machine-to-machine sharing!
- Share **relevant/timely/highly contextual** intel
  - Relevant intel that applies to you and your industry
  - Timely intel that is fresh and still accurate
  - Contextual intel
- This is what the bad guys are doing

Human to human sharing is dependent on the individuals, their relationships and their process. It goes with them

© 2017 ServiceNow All Rights Reserved

What You Should Share and When

- Fresh data specific to you and your industry
- Share as part and parcel of your investigation—afterwards is too late!
- Fluid, interactive sharing provides insight into the ongoing tactics
- Share what you know:
  - Observables/Indicators of Compromise (IOCs)
  - Share context! Why am I sharing? What am I looking for?



© 2017 ServiceNow All Rights Reserved

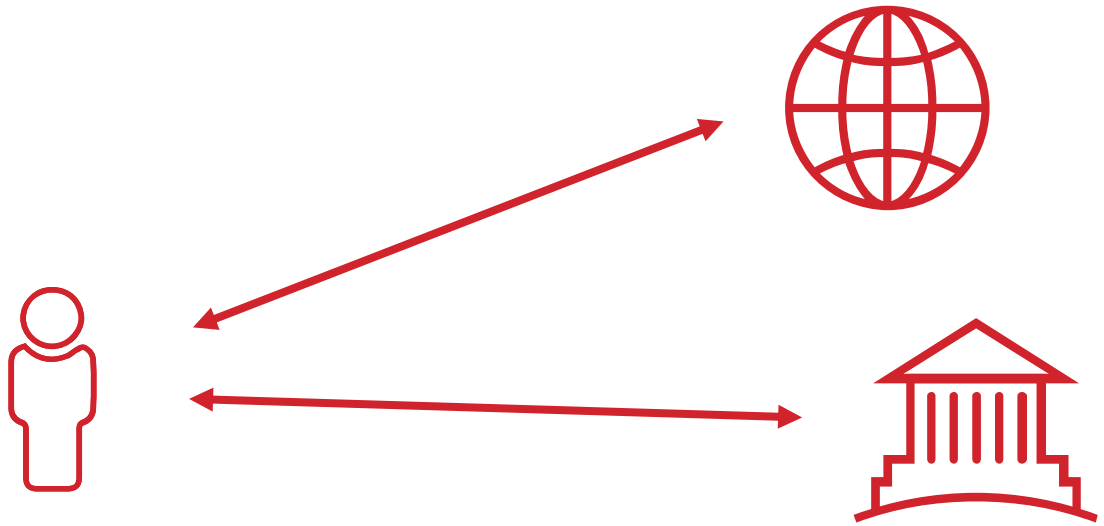
How? - ServiceNow Trusted Security Circles!

- A Trusted Security Circle is a channel of communication with a predefined set of peers, partners, etc.
- The information sent in this channel is a name, description, list of observables (IP addresses, URLs, domains, etc) and sightings.
- When received by the members of the Trusted Security Circle, the system can be configured to automatically search the members' local environment.
  - If local sightings are found and they cross a preset threshold, a Security incident can automatically be created.
  - In addition the results of this search are sent back to all members of the Trusted Security Circle
- By default this information is sent anonymously and is stripped of any observables that could identify the sender (using a whitelist).

© 2017 ServiceNow All Rights Reserved

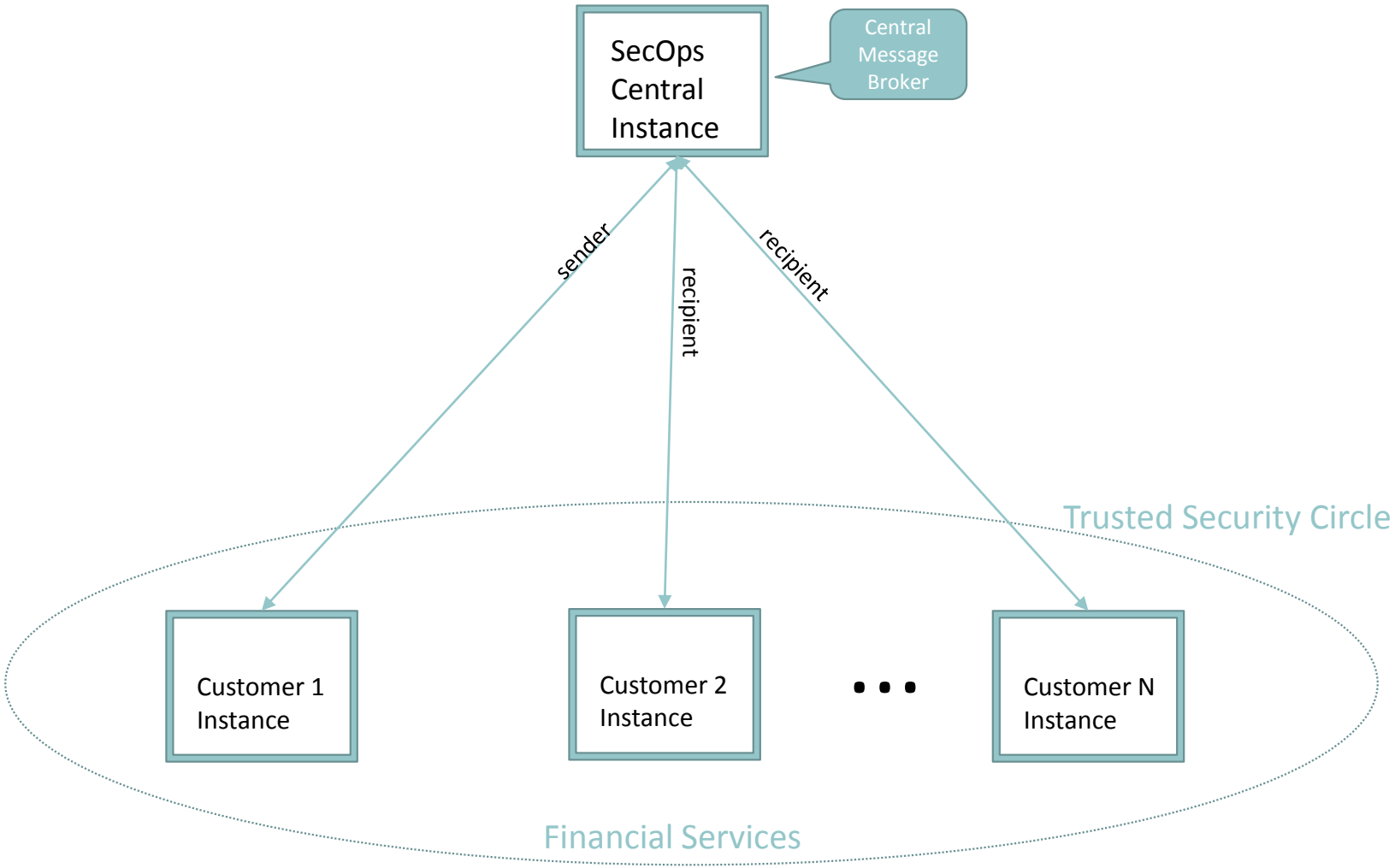
ServiceNow Trusted Security Circles

- Anonymous by default
- Automatic responses
- Sharing stays with your company
- Private circles option – controlled sharing
- Supports industry standards STIX/TAXII
- Integrated orchestration



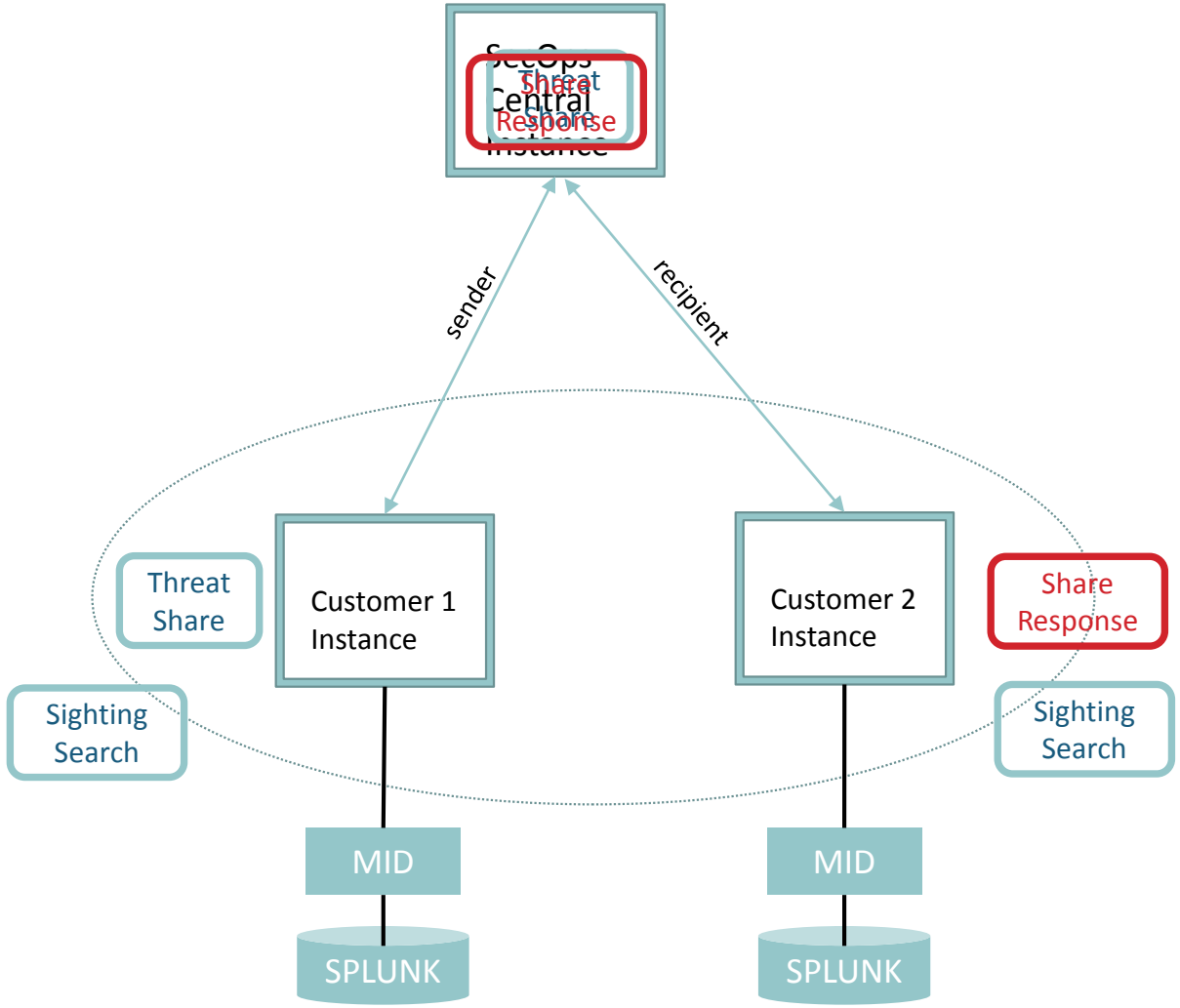
© 2017 ServiceNow All Rights Reserved

Trusted Circle Sharing



© 2017 ServiceNow All Rights Reserved

Trusted Circle Sharing (play animation to see how process works)



© 2017 ServiceNow All Rights Reserved

What is Sighting Search?

- Sighting Search is one of a set of integration capabilities implemented in Jakarta.
- Sighting Search allows us to search a supported SIEM or Log Store for occurrences (sightings) of observables.
- This allows you to proactively search your environment for emerging threats.
- Jakarta supports Sighting Search for Splunk, ElasticSearch, QRadar, HPE ArcSight Logger and McAfee ESM.

© 2017 ServiceNow All Rights Reserved

ServiceNow Security Operations – New Integrations



Vendor Product	SecOps Application	Use Cases	Integration Type
Malwarebytes	Security Incident	Email based incident creation & Powershell Script to kick-off a scan in Malwarebytes	Email/Script
Risk IQ – Passive Total	Threat Intelligence	Lookup observable- IP, Domain, File Hash	API
Cuckoo	Security Incident	Sending file/executables to Cuckoo and return results to SN	API
ThreatCrowd	Threat Intelligence	Look observables – Filehash, email, domain, url, AV detections	API
PhishTank	Threat Intelligence	Lookup suspected phishing site	API
GoogleSafeBrowsing	Threat Intelligence	Search URL against google list	API
Lastline	Security Incident	Incident creation via email	Email
VxStream	Threat Intelligence	Lookup hash, IP, Port, URL	API
Sumologic	Security Incident	Sightings Search	API
Shodan	Security Incident	Lookup IP's and URLs	API
IBM QRadar	Security Incident	Sightings Search	API
HPE Logger	Security Incident	Sightings Search	API
McAfee ESM	Security Incident	Sightings Search	API

© 2017 ServiceNow All Rights Reserved

ServiceNow Security Operations – New Integrations

Vendor Product	SecOps Application	Use Cases	Integration Type
Tripwire Enterprise	Security Incident	Bi-directional integation – open incidents in SN, perform lookups on TW Enterprise	Bi-Directional API
Anomoli	Threat Intelligence	Lookup Email, IP, URL	API
Kenna Security	Vulnerability Response	Pull scan data into ServiceNow and launch scans in Kenna from SN	API
Digital Shadows	Security Incident	Incident creation	API
CyberArk	Security Incident	Confirm SIR task/incident is validated before accessing credentials in CyberArk	API
Cylance	Security Incident	Consume alerts as security incidents or events	email
Phishme	Security Incident	Consume alerts as security incidents or events	email
Checkpoint & Passive Total	Security Incident	Workflow with block action	API
Slack	Security Incident	Multiple including creating channel for security incident, get transcripts	API
Reverse Whois	Security Incident	Lookup for enrichment	API
Tenable Nessus	Vulnerability Response	Request Scans	API
Splunk	Security Incident	Launch search in Splunk in context	API

© 2017 ServiceNow All Rights Reserved

Security Ecosystem Partners

Vulnerability	Enforcement	SIEM	Intelligence
QUALYS®	paloalto NETWORKS	splunk>	CROWDSTRIKE
RAPID7	BLUE COAT	Radar	Metascan®
tenable network security	Symantec	ArcSight	THREATCONNECT
FLEXERA SOFTWARE	McAfee	LogRhythm The Security Intelligence Company	CARBON BLACK ARM YOUR ENDPOINTS
tripwire	TANIUM		iSIGHTPARTNERS
	Check Point SOFTWARE TECHNOLOGIES LTD.		virustotal
	FireEye		SOLTRA A DTCC and FS-ISAC Company
	ForeScout		Recorded Future
	Infoblox		cuckoo
			STIX

© 2017 ServiceNow All Rights Reserved

Lab Time!

Saving Trees!

- Instead of handing out yet more paper, we decided to put any additional info you need in the Registration page. There is an updated Lab Guide at https://tinyurl.com/LAB132023

Changes to the Lab Guide

- In the interest of time and enjoyment we were able to remove a couple of steps from the original Lab Guide
- For those of your over achievers we have a couple of extra Bonus Labs that we added to the updated Lab Guide

© 2017 ServiceNow All Rights Reserved

Instance Registration URL

http://clabs.link/lab132023

Lab Guide

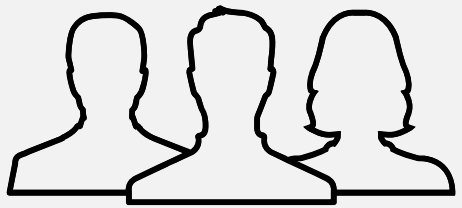
https://tinyurl.com/LAB132023

© 2017 ServiceNow All Rights Reserved

Key Takeaways

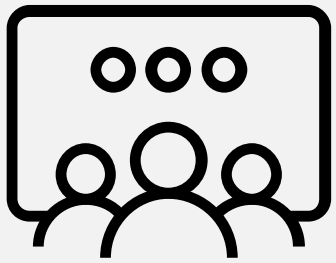
1

You are not alone!



2

Community improves awareness



3

Bad guys are sharing, why aren't you?



© 2017 ServiceNow All Rights Reserved

Thank You

Lab Sponsored by Amazon Web Services



Alex Yupanqui
Senior Solutions Architect
ServiceNow

Antoni Kew
Advisory Solutions Architect
ServiceNow

Scott Lewis
Sr. Product Manager
ServiceNow

#Know17 | http://clabs.link/lab132023

© 2017 ServiceNow All Rights Reserved