knowledge17

WORK at LIGHTSPEED

Threat Intelligence Sharing: How Participation Will Dramatically Improve Your Security Posture

RICH REYBOK
Sr. Director, Software Engineering
ServiceNow

SCOTT LEWIS
Sr. Product Manager
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Speaker Introduction



NAME: Rich Reybok

TITLE: Sr. Director, Software Engineering

FUNCTION: Security and Compliance Products R&D

COMPANY: ServiceNow

Experience: CISO, Asurion; CISO, Merrill Lynch CICG; CTO, BrightPoint Security (acquired by ServiceNow); Founding member of OASIS Common Security Advisory Framework (CSAF) TC

Current Projects: Working on K! Investigating and researching methods of applying artificial intelligence to SOC operations management

Interests: Soccer, drummer in punk band, r/c car racer, and video games. Anyone up for a round of FIFA after this?

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



NAME: Scott Lewis

TITLE: Sr. Product Manager

FUNCTION: Product Management

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

- Think differently about how you run security operations

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

History of Threat Intel Sharing



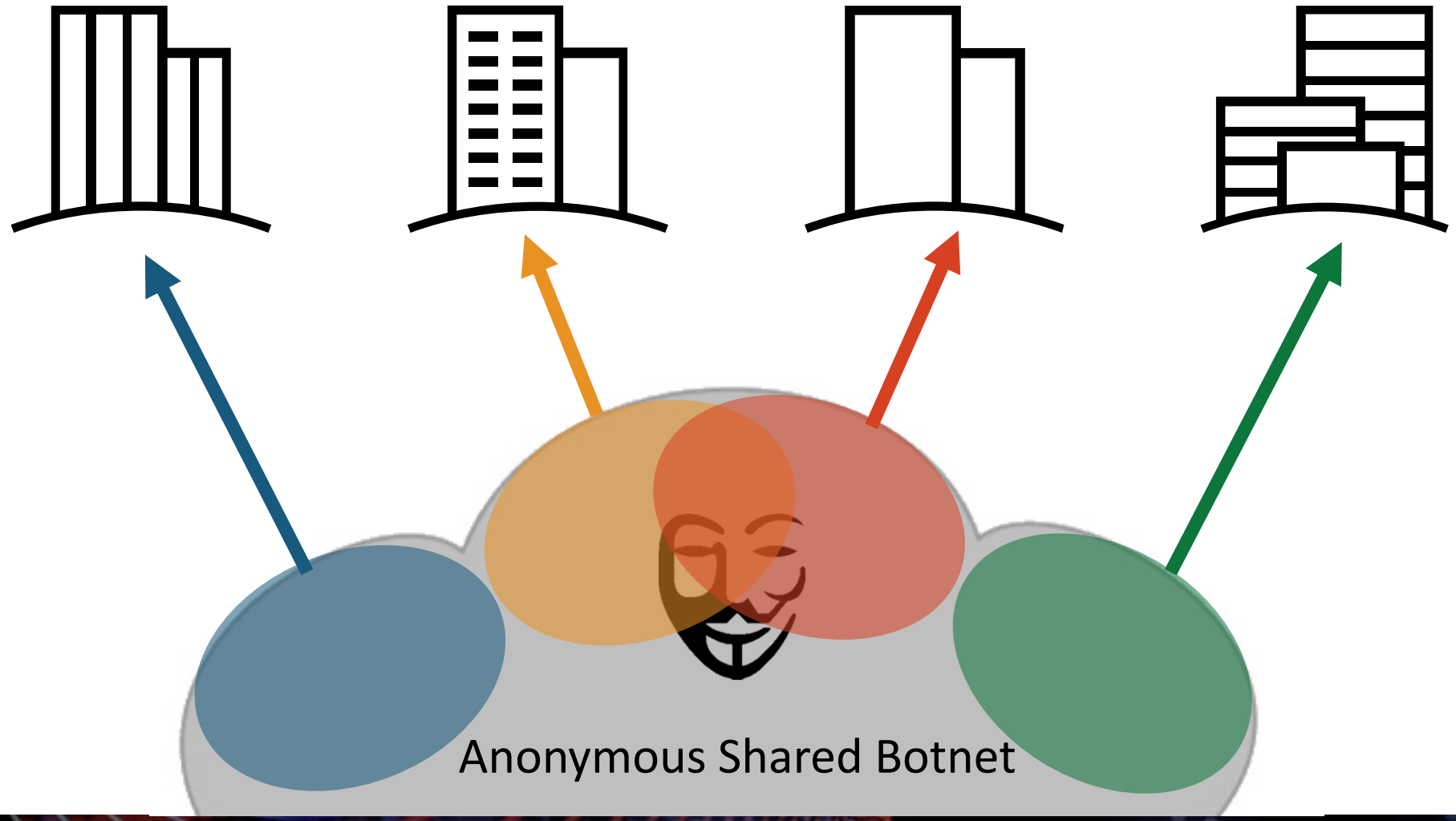
© 2017 ServiceNow All Rights Reserved

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?

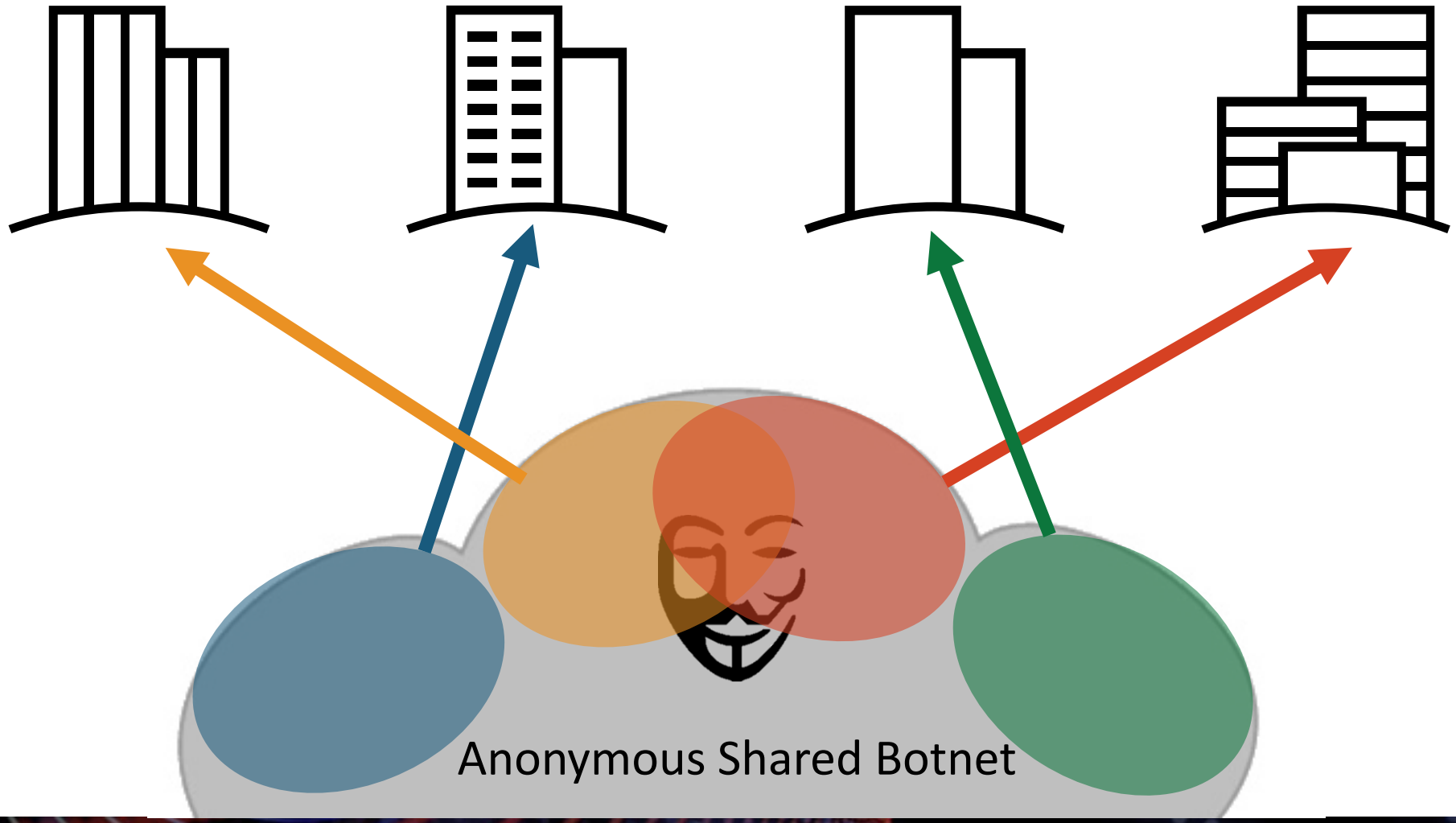
© 2017 ServiceNow All Rights Reserved

Operation Payback



© 2017 ServiceNow All Rights Reserved

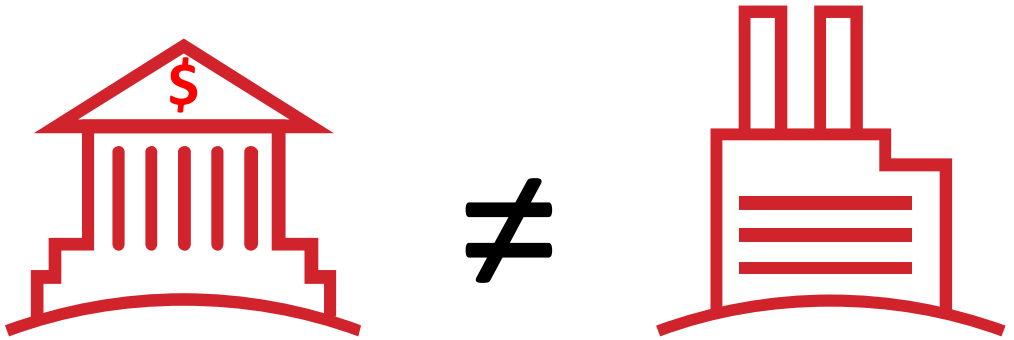
Operation Payback



© 2017 ServiceNow All Rights Reserved

What You Should Share and When

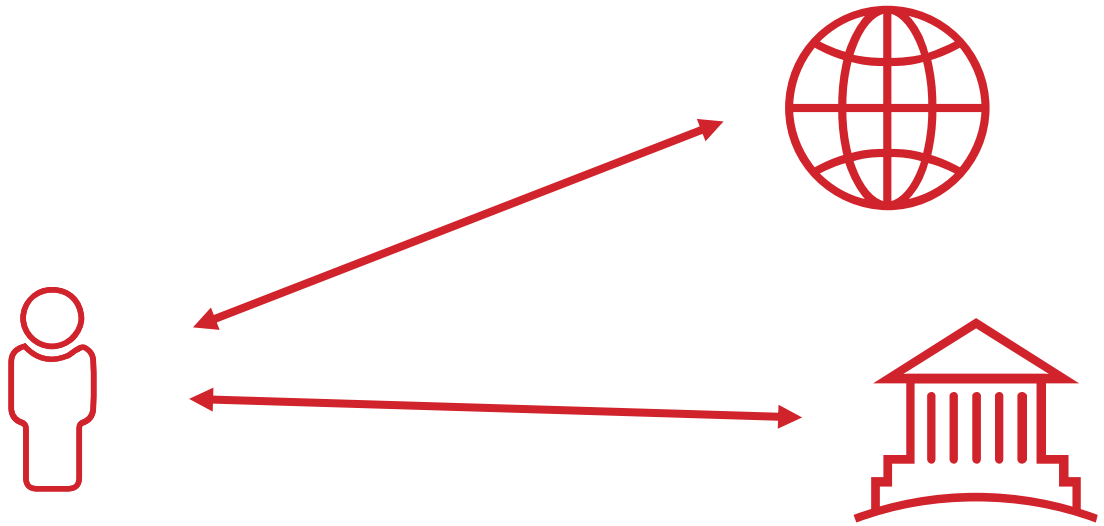
- Fresh data specific to you and your industry
- Share as part and parcel of your investigation—afterwards is too late!
- Fluid, interactive sharing provides insight into the ongoing tactics
- Share what you know:
  - Indicators of Compromise (IOCs)
  - Share context! Why am I sharing? What am I looking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



© 2017 ServiceNow All Rights Reserved

ServiceNow Trusted Security Circles

- You can also have that Johnney's Fish Grill experience
- We do the vetting
- 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

Use Case – Fish Restaurant Attack

© 2017 ServiceNow All Rights Reserved

FG-ISAC

(Fish Grill Information Sharing and Analysis Center)

```
<stix:STIX_Package >
    <stix:Incidents>
        <stix:Incident id='example:incident-8236b4a2-abe0-4b56-9347-288005c4bb92" timestamp="2014-11-18T23:40:08.061362+00:00" xsi:type='in
cident:IncidentType' version='1.2">
            <incident:Title>Breach of Cyber Tech Dynamics</incident:Title>
            <incident:Time>
                <incident:Initial_Compromise precision="second">2012-01-30T00:00:00</incident:Initial_Compromise>
                <incident:Incident_Discovery precision="second">2012-05-10T00:00:00</incident:Incident_Discovery>
                <incident:Restoration_Achieved precision="second">2012-08-18T00:00:00</incident:Restoration_Achieved>
                <incident:Incident_Reported precision="second">2012-12-10T00:00:00</incident:Incident_Reported>
            </incident:Time>
            <incident:Description>Intrusion into enterprise network</incident:Description>
            <incident:Reporter>
                <stixCommon:Description>The person who reported it</stixCommon:Description>
                <stixCommon:Identity id='example:Identity-cd64aaa6-b1c0-4025-8ea1-14ff5a19e5fb">
                    <stixCommon:Name>Sample Investigations, LLC</stixCommon:Name>
                </stixCommon:Identity>
                <stixCommon:Time>
                    <cyboxCommon:Produced_Time>2014-03-11T00:00:00</cyboxCommon:Produced_Time>
                </stixCommon:Time>
            </incident:Reporter>
            <incident:Victim id="example:Identity-dd8637b7-51b4-48f0-9e3c-a2b23b3a2dd7">
                <stixCommon:Name>Cyber Tech Dynamics</stixCommon:Name>
            </incident:Victim>
            <incident:Impact_Assessment>
                <incident:Effects>
                    <incident:Effect xsi:type="stixVocabs:IncidentEffectVocab-1.0">Financial Loss</incident:Effect>
                </incident:Effects>
```



© 2017 ServiceNow All Rights Reserved

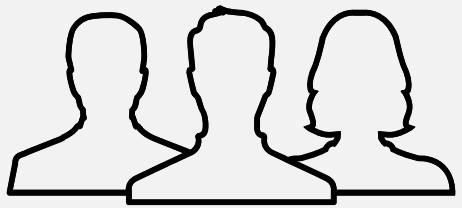
DEMO

© 2017 ServiceNow All Rights Reserved

Key Takeaways

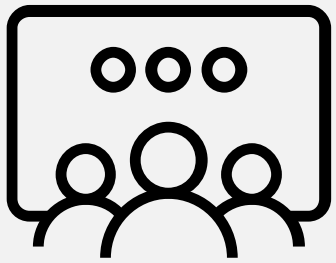
1

You are not alone!



2

Community improves awareness



3

Bad guys are sharing, why aren't you?



© 2017 ServiceNow All Rights Reserved

Q & A

RICH REYBOK
Sr. Director, Security Products R&D
ServiceNow

SCOTT LEWIS
Sr. Product Manager
ServiceNow

© 2017 ServiceNow All Rights Reserved

Thank You

RICH REYBOK
Sr. Director, Security Products R&D
ServiceNow

SCOTT LEWIS
Sr. Product Manager
ServiceNow

#Know17

© 2017 ServiceNow All Rights Reserved