knowledge17

http://clabs.link/lab132018

WORK at LIGHTSPEED

Enterprise Security Response
Creating Automated Workflows for Security Playbooks

Sean Barrett
Advisory Solution Consultant
ServiceNow

Robert Held
Security Operation Advisory Solution Architect
ServiceNow

Jerry Hu
Advisory Solution Consultant
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Speaker Introduction



Name: Sean Barrett

Title: Advisory Solution Consultant

Function: Sales

Company: ServiceNow

Experience: 7 years working on the ServiceNow platform, all areas

Expertise: Security Operations, Governance, Risk & Compliance, Facilities, Customer Service, ITSM

Achievements: My beautiful family (wife, son, & daughter)…and my 2 dogs

Current Projects: My beautiful family (wife, son, & daughter)…and my 2 dogs

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Robert Held

Title: Security Operation Sr. Solution Architect

Function: Sales

Company: ServiceNow

Experience: 20+ years of Sys Admin, Software Dev, and Security

Expertise: Security Incident/Vulnerability Response, Threat Intel

Achievements: Numerous customer workshops, POVs, and Field Enablement

Current Projects: Knowledge 17, Field Enablement for Jakarta release

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Jerry Hu

Title: Advisory Solution Consultant

Function: Sales

Company: ServiceNow

Experience: 1.5 Years with ServiceNow, 20+ years of IT Software

Expertise: IT Operation/Automation, Security Operations

Achievements: Worked for great companies with great customers

Current Projects: Service automation for retail store

© 2017 ServiceNow All Rights Reserved

Agenda

- Overview of ServiceNow Security Operation Solution
- Lab Session
  - Lab 1 Access and Configuration of Lab Environment
  - Lab 2 Understanding the Workflow Interface
  - Lab 3 Walk Thru Security Workflow Examples
  - Lab 4 Configure Email Parser
  - Lab 5 Build Security Operation Workflow
  - Lab 6 Test and Demo What We Built

© 2017 ServiceNow All Rights Reserved

Objectives and What You Will Learn

Objectives

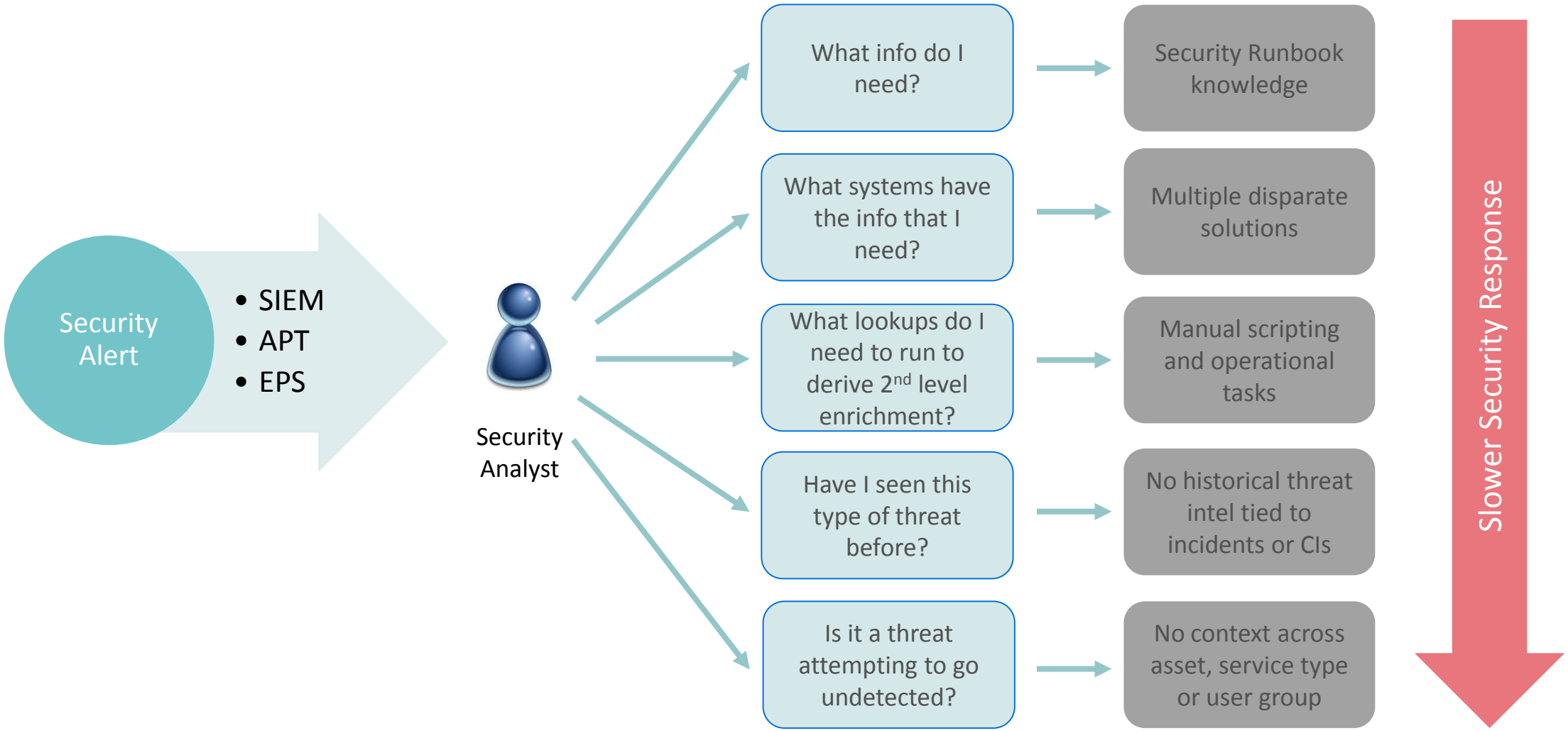
- You will get hands-on workflow creation experience with security use cases, which can turn your manual-based security operation playbooks into automated processes and therefore greatly expedite security incident and vulnerability responses.

What you will learn

- Understanding of Values from ServiceNow Security Operations Solution
- Understanding of ServiceNow Platform Orchestration Capabilities
- Understanding of ServiceNow Security Operation Workflow Key Use Cases
- Hands-on Experience with Security Operation Workflow Creation

© 2017 ServiceNow All Rights Reserved

Typical Security Response Challenges



© 2017 ServiceNow All Rights Reserved

Impact on Operations and Response Times

1. Lost time during alert prioritization and assignment

2. Lost time during manual data enrichment and gathering processes

3. Lost time in hand-offs across teams and round-trips

© 2017 ServiceNow All Rights Reserved

ServiceNow: Enterprise Security/ IT Response Platform Benefits



Resource Efficiency

Time to Identify

Time to Respond

Risk

© 2017 ServiceNow All Rights Reserved

Lab Session

#Know17 | http://clabs.link/lab132018

© 2017 ServiceNow All Rights Reserved

Thank You

Lab Sponsored by Amazon Web Services



Sean Barrett
Advisory Solution Consultant
ServiceNow

Robert Held
Security Operation Advisory Solution Architect
ServiceNow

Jerry Hu
Advisory Solution Consultant
ServiceNow

#Know17 | http://clabs.link/lab132018

© 2017 ServiceNow All Rights Reserved