Entry-level Cyber Cyber Security Analyst Skill Development

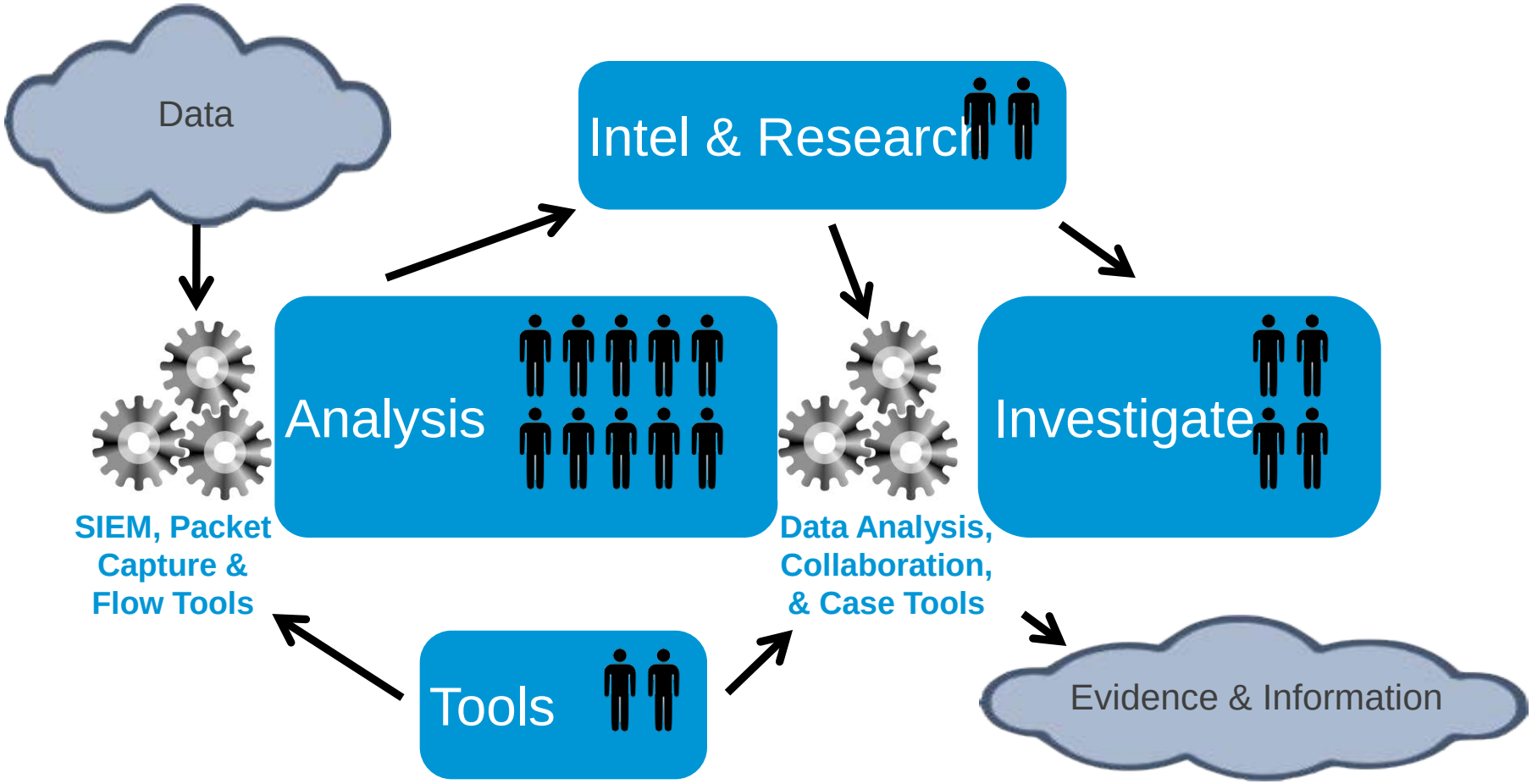
Brian Ford
Consulting Engineer, CISSP
bford@cisco.com

James Risler
Technology Education Specialist, CCIE# 15412
jarisler@cisco.com

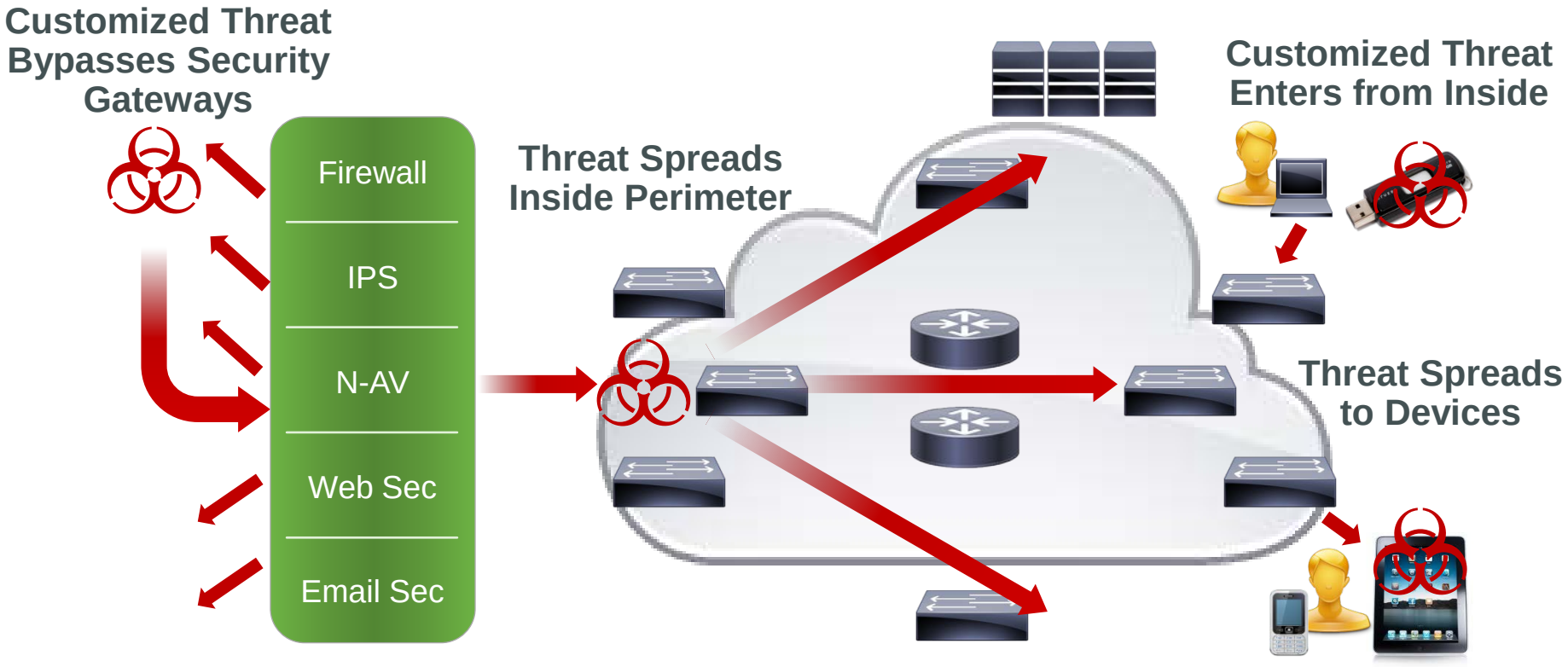
Overview

- Security Analyst Challenge
- Security Analyst skill Development
  - Competency areas
  - Facilitation of Knowledge
- Complex job of a Security Analyst
  - Tools used by Security Investigators
- Course development process
- Lab infrastructure
- Lessons Learned

IAT Roles & Relationships



Security Analyst Challenge



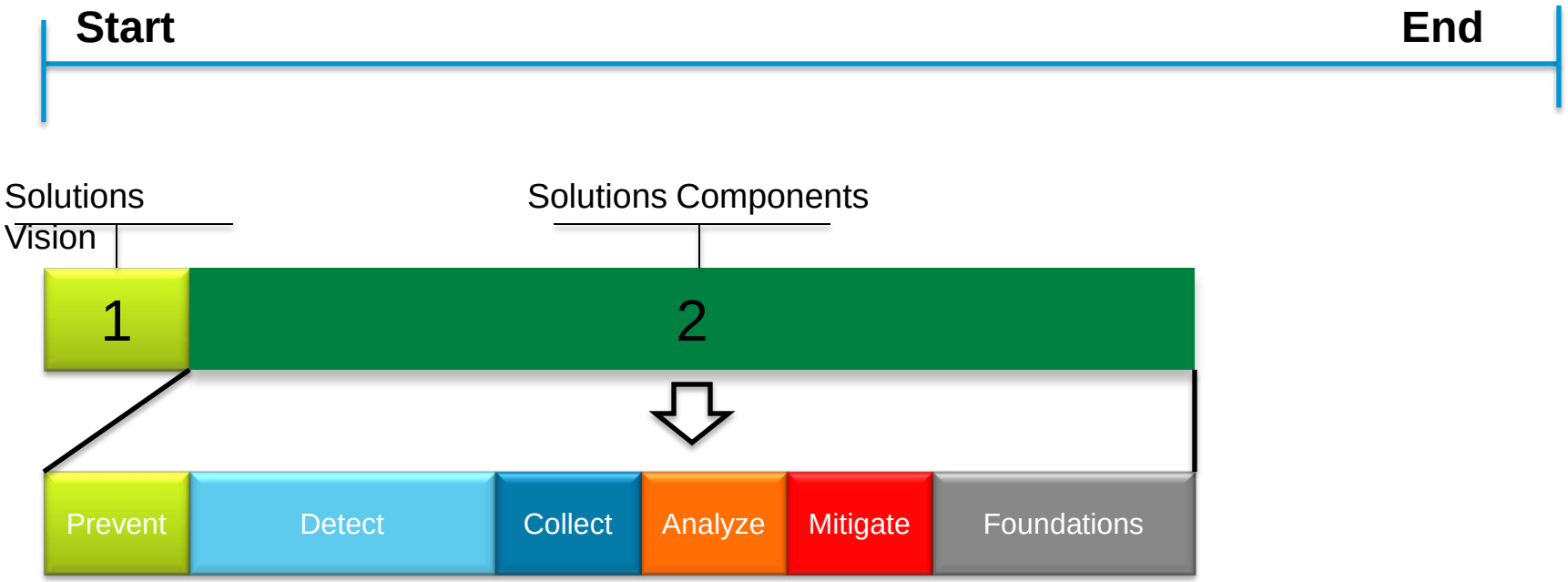
Perimeter security stops many threats but sophisticated Cyber threats evade existing security constructs

Fingerprints of threats are often found in network fabric

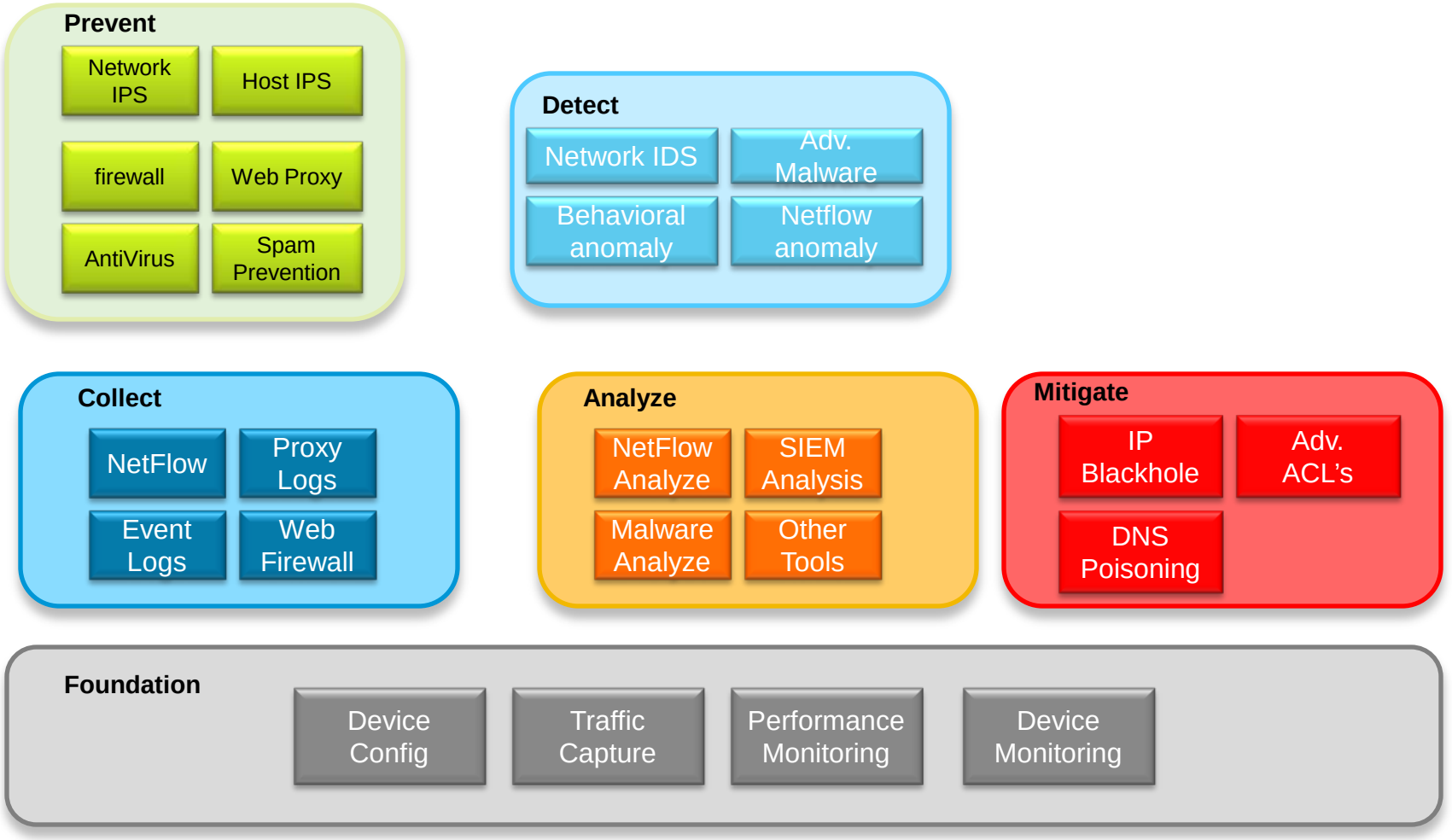
Security Analyst Skills

- What Skills to Develop?
  Major areas of competency
  - Understanding security policy
  - Data & Traffic Analysis
  - Identifying Security Events –> How & when to alarm
  - Incident Response
- Foundation/Background
  - Network infrastructure knowledge
  - Diverse device configuration ability
  - Security configuration knowledge
  - Data management & teamwork
- Challenge is Arming Security Investigators
  - Not tied to a product or solution
  - Complex knowledge – Not one specific process is correct or product solution
  - Diverse set of skills are needed

Security Investigation Process



Functional Model for Security Analyst

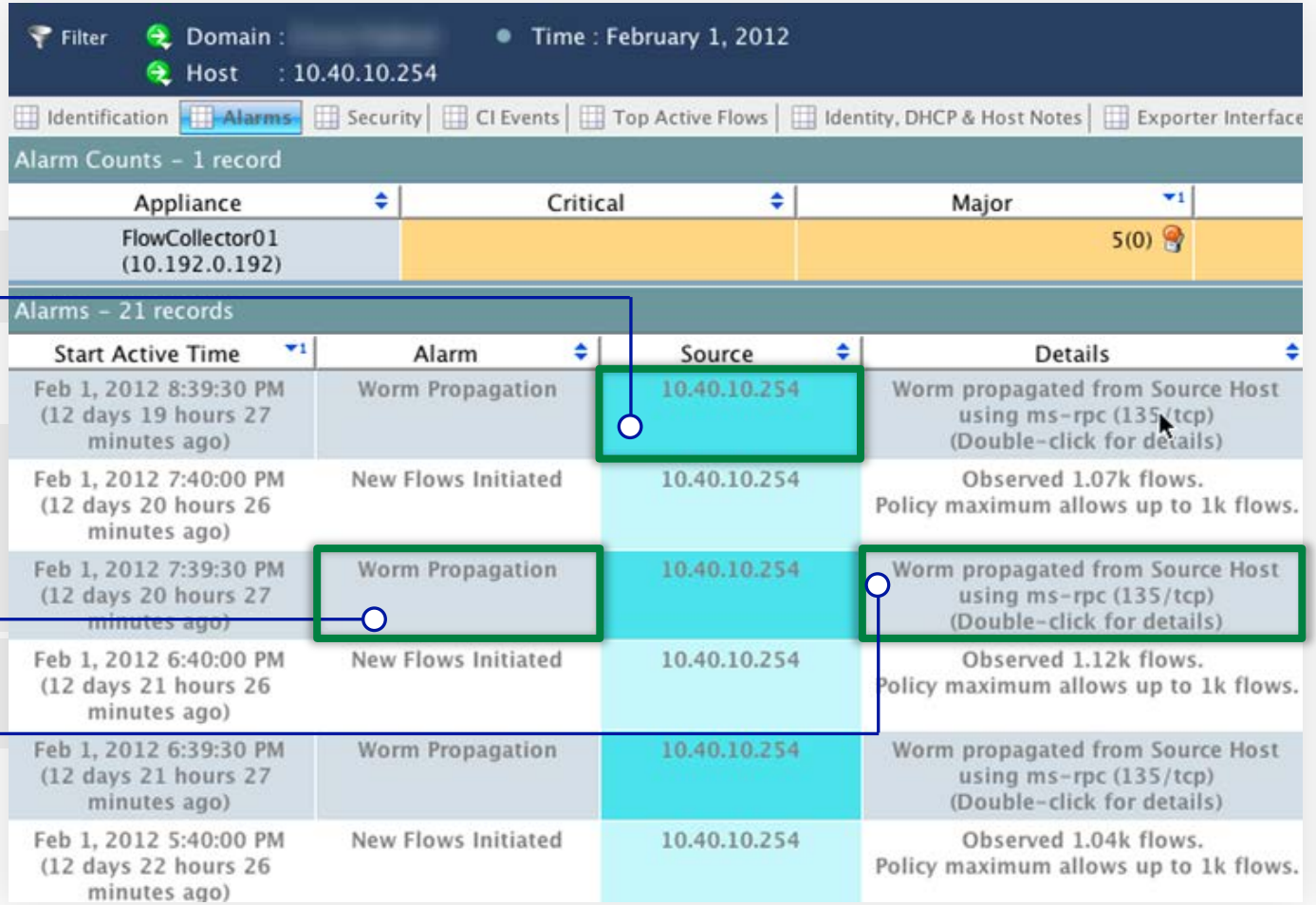


Example: SIEM tool identifying a Worm

IP Address

Alarm indicating this host touched another host which then began exhibiting the same suspicious behavior

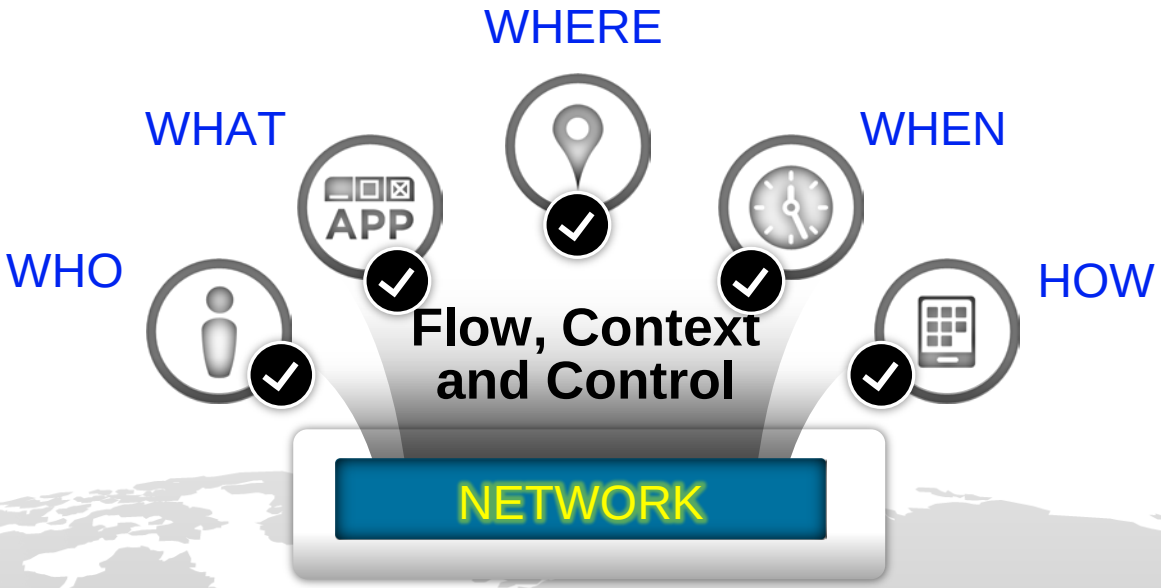
Suspicious activity that triggered the alarm



Goal – Train IAT & Security Analysts

- IAT – Information Assurance Technicians
  - Also known as Network & Security Analysts
  - Assess the state of the network based on established policies
  - Work in Network & Security Planning, Operations, Audit, and IRTs
- These are not entry level positions
  - Requires base knowledge of network and computer operations
  - Launching pad to many roles in IT
  - IT need in .mil, .gov, & .com environments
- The Challenge of being a Vendor & Practitioner
  - Cisco develops and sells routers, switches, & network equipment
  - Cisco has well established IT, NOC, SOC, PSIRT, & CSIRT

Complex Threat Puzzle



Use Netflow data to extend visibility to the Access Layer

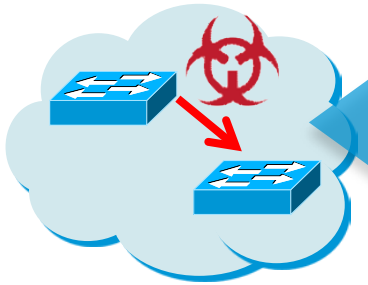
Unite Flow data with identity, reputation, application for context

Network switches as enforcement points for increased control

Example of a Complex Threat Visibility Concept

Leveraging Netflow to investigate a potential IT policy violation

Attack bypasses perimeter and traverses network



Netflow at the access layer provides greater granularity

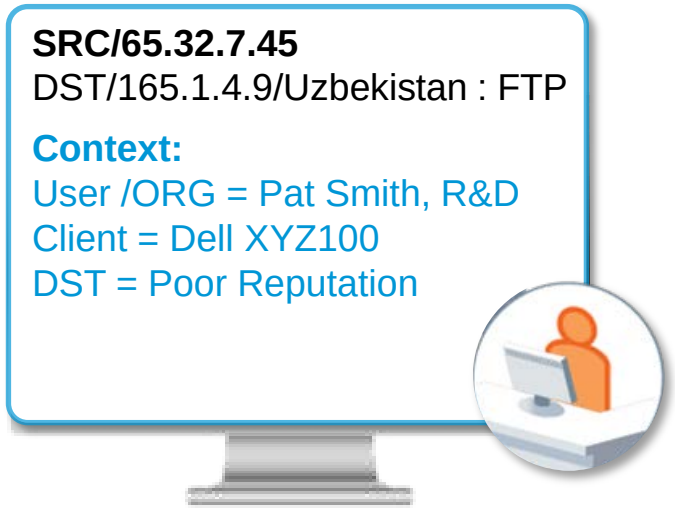
ACTIVE FLOWS: 23,892

SRC/65.32.7.45
DST/171.54.9.2/US : HTTP
DST/34.1.5.78/China : HTTPS
DST/165.1.4.9/Uzbekistan : FTP
DST/123.21.2.5/US : AIM
DST/91.25.1.1/US : FACEBOOK

Cisco Threat Context Grid – Automating Context Collection

SRC/65.32.7.45
DST/165.1.4.9/Uzbekistan : FTP

Context:
User /ORG = Pat Smith, R&D
Client = Dell XYZ100
DST = Poor Reputation



The need for visibility could/should drive information sharing!

Key Challenges: Complex Threat Visibility

- **Breached but How, Where and Who?**
  - Often very difficult to find
  - High value assets – major consequences
  - Network flow analysis is central to this process—throughout the network
- **Context is Critical**
  - No single system provides all data to decipher an attack
  - Related threats, identity, reputation, vulnerability, device type…
- **Disparate Data Sources, Manual Assembly**
  - Analysts collect and assemble contextual information from a variety of systems
  - Requires expensive analysts—round-the-clock coverage

What did Cisco Learn?

- Complex problem
- Sources of Data and Baseline
- Deep Packet Analysis needed
- Levels of Skill – Associate vs. Professional
- Log Analysis with correlation
- Where on the network to Monitor? (Key)
- Operational Process tied into Monitoring
- Incident classifying

What did Cisco Learn? – continued

- Investigating Security Incidents

  Structure, process, and tools

- Necessary tools

  Packet analysis, SIEM, Flow Analysis

  Collaboration & Teaming

  Mix of COTS & Open Source

- Mentoring during the Learning process
  - Using PCAP files with known complex threats
  - Netflow outputs tied to investigations
  - Historical threat signatures and packet payloads to develop individual capabilities

Conclusion

- Security Analyst competency areas - Key
- Skillset complexity (Where to Look)
- Course Development Process
- Labs – Build skills with a mix of COTS and open source tools
- Lessons Learned

Questions/Discussion?

Thank You