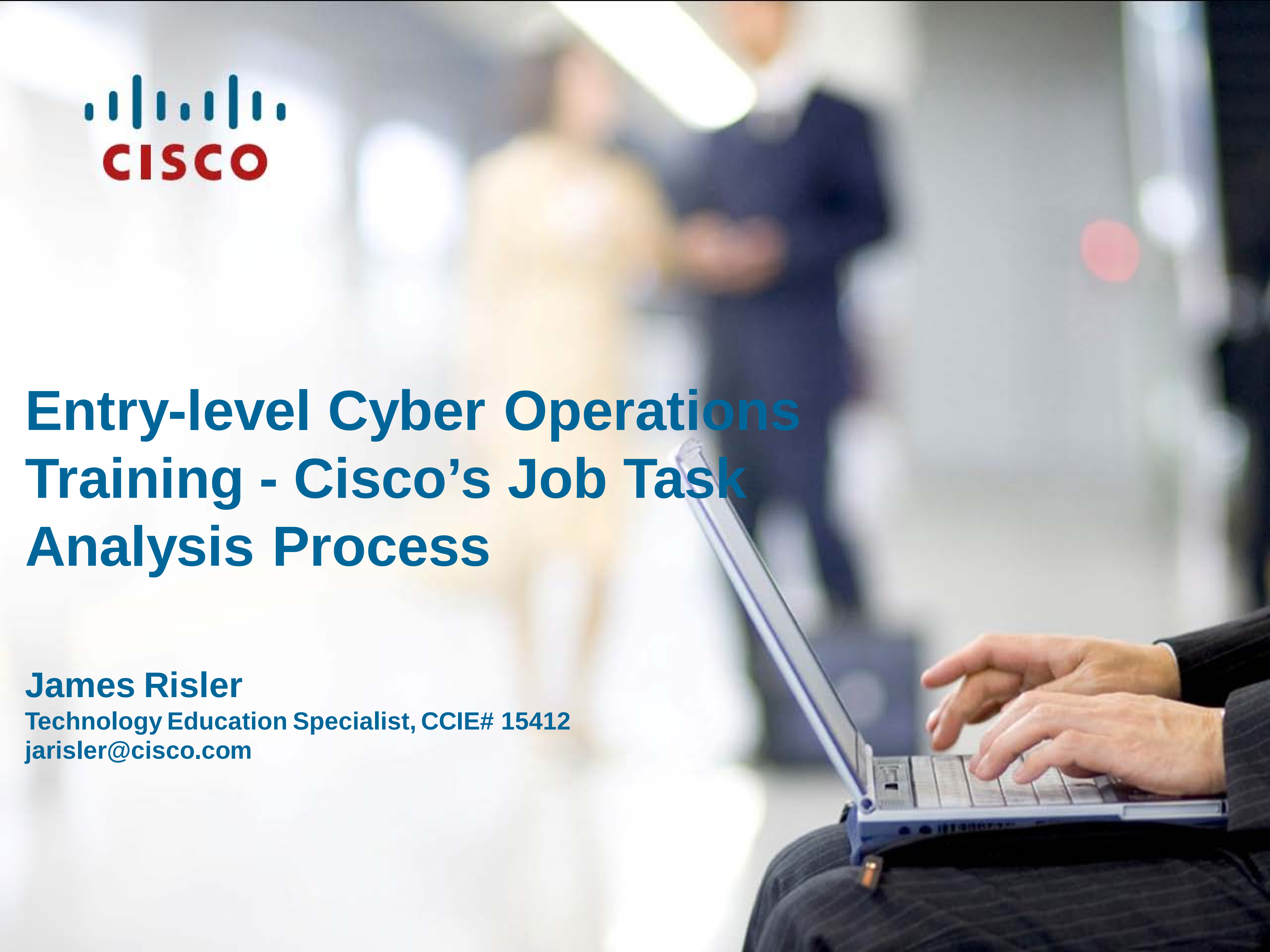


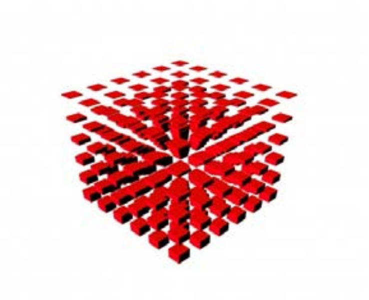
# Entry-level Cyber Operations Training - Cisco’s Job Task Analysis Process

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

# Knowledge Transfer

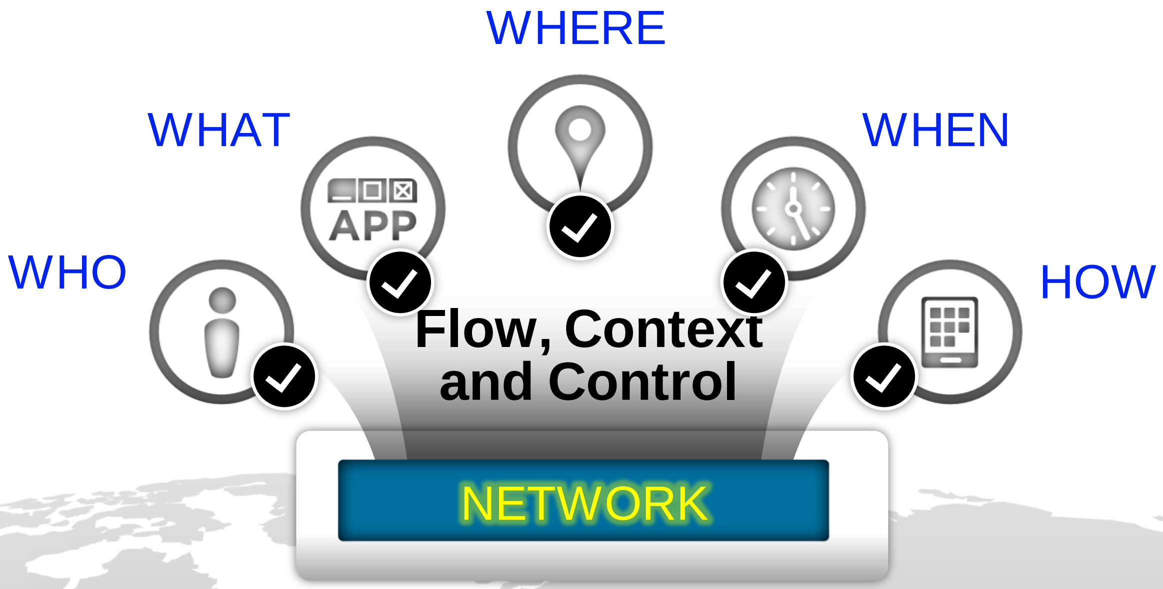
- Taking Cisco product & solution knowledge and transferring that to our customers
  - Staff know how products work
  - Staff have developed and tested solutions and produced replicable architectures
- Challenge is transferring **process** knowledge
  - Not tied to a product or solution
  - Complex knowledge – Not one specific process is correct
  - Diverse set of skills are needed
- What Skills to Develop?
  - Diverse skill set with emphasis on investigation & forensics
  - Many prerequisites
  - How do SMEs train new staff

# Goal – Train IAT & Security Analysts

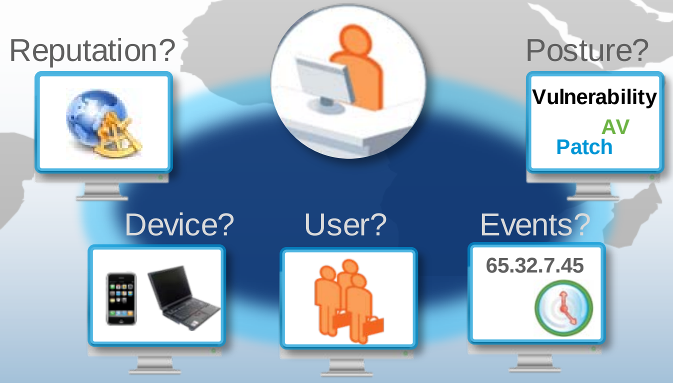


- IAT – Information Assurance Technicians
  - Also known as Network & Security Analysts
  - Assess the state of the network based on established policies
  - Work in Network & Security Planning, Operations, Audit, and IRTs
- These are not entry level positions
  - Requires base knowledge of network and 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



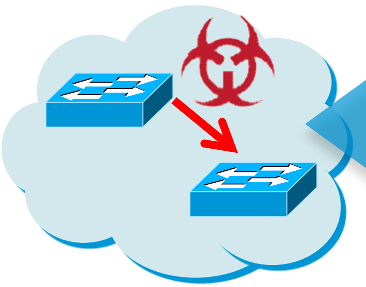
Unite Flow data with identity, reputation, application for context

Network switches as enforcement points for increased control

# Example of a Complex Threat Visibility Concept

## Leveraging Netflow to investigate a potential IT policy violation investigation

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

# Why does Cisco do a Job Task Analysis (JTA)?

## *Subject Matter Experts – Job Role Analysis*

- Domain of Expertise (technical area)
- Skill and tasks needed for a specific technical area
- Task inventory and rating of importance, difficulty and frequency
- Outcome is blueprint of technical domains which are ranked
- Curriculum planning
- High Level Design Document
- Lab requirements (topology, tools, design)
- Content Development and validation

SECURITY:

Firewall

IPS

VPN

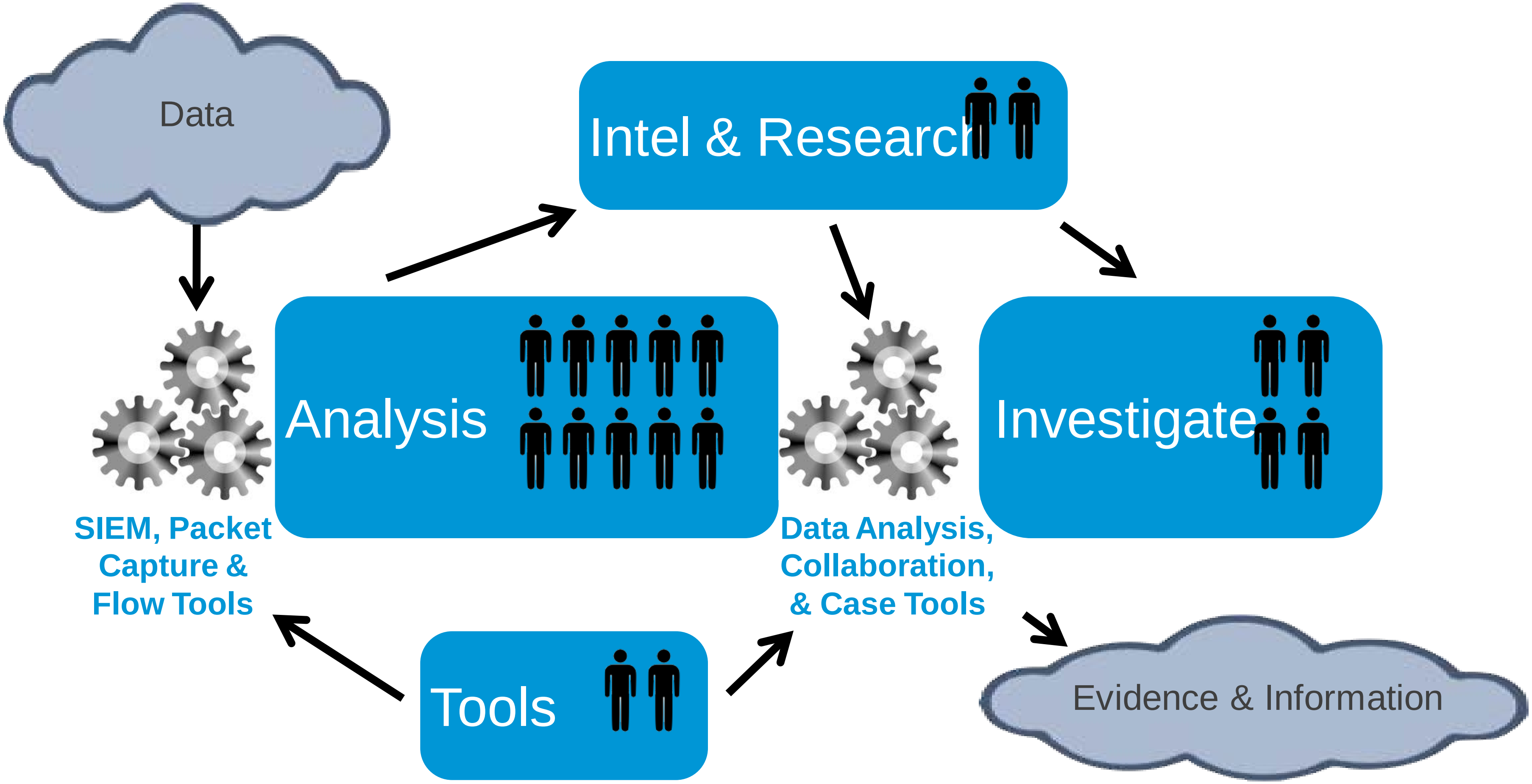
ScanSafe

# Cisco’s IAT Subject Matter Experts (SME)

## Security Intelligence Operations (SIO)

- Information Technology
- Cisco’s Product Security Incident Response Team (PSIRT)
  - Manages, investigates and public reporting of security vulnerabilities
  - Incident response and forensic analysis
  - Focused on Cisco products
- Applied Intelligence Group
  - Research, document, and test potential security mitigations
  - IPS Signatures
  - Publish research and bulletins correlating IT security risks and events
- Remote Operations Support (ROS) Team
  - Incident response and investigation
  - Network management

# IAT Roles & Relationships



Data

Intel & Research

Analysis

Investigate

SIEM, Packet Capture & Flow Tools

Data Analysis, Collaboration, & Case Tools

Tools

Evidence & Information

# 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

  Netflow analysis, packet capture

  Wireshark

- 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

CYBER SECURITY
SUPERHERO SERIES 2012
Join the fight against cyber crime!
Cisco | Networking Academy
Mind Wide Open
cisco

# Conclusion

- Process Knowledge transfer is critical
- Skillset diversity and complexity
- Mentoring key component
- Labs – Build skills with PCAP and Netflow information
- Iterative Approach

# Questions/Discussion?

Thank You

cisco