RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-T11

Building a World-Class Proactive Integrated Security & Network Operations Center SNOC

Hanna Sicker CISM, CISSP
Security & Network Operations
SNOC Sr. Mgr.
StubHub/eBay
@snocgirl

Operations Leaders (Security & Network)

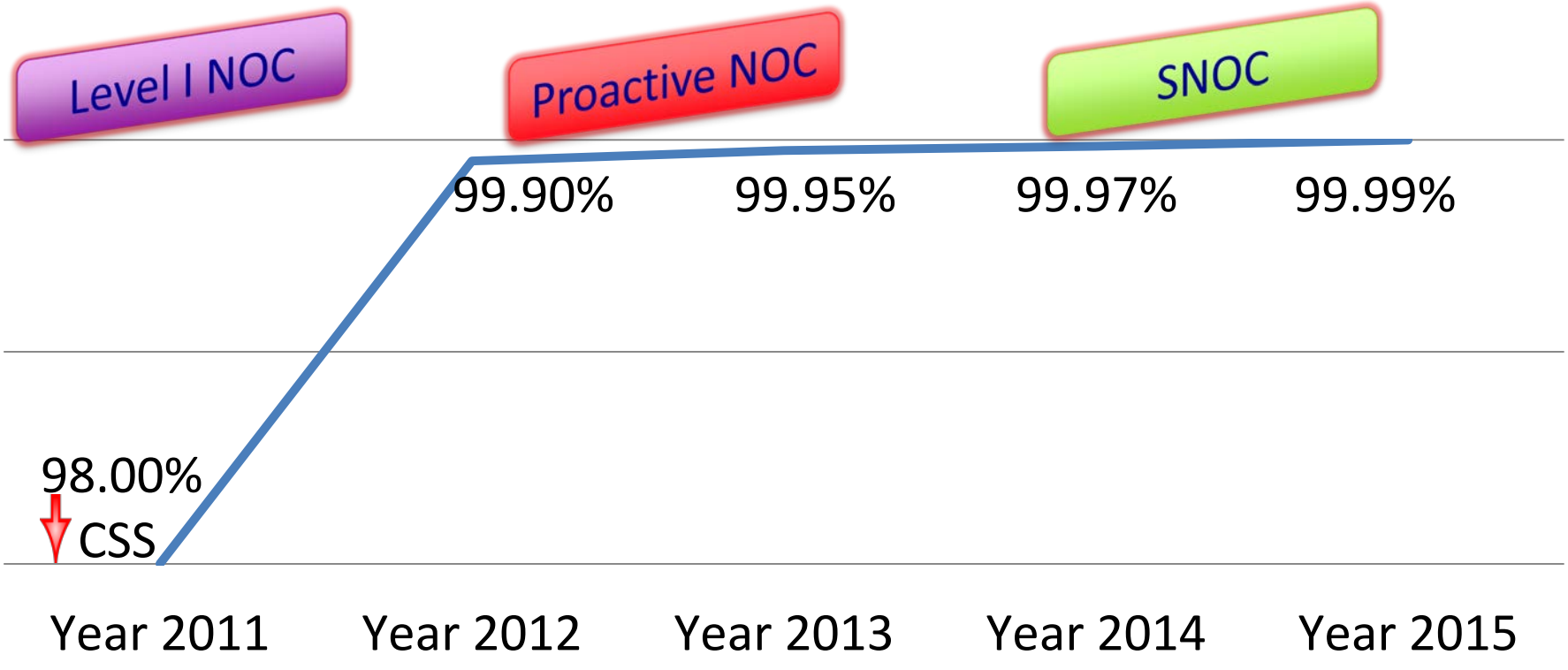
Service Unavailable…

Service Unavailable

The service is temporarily unavailable. Please try again later.

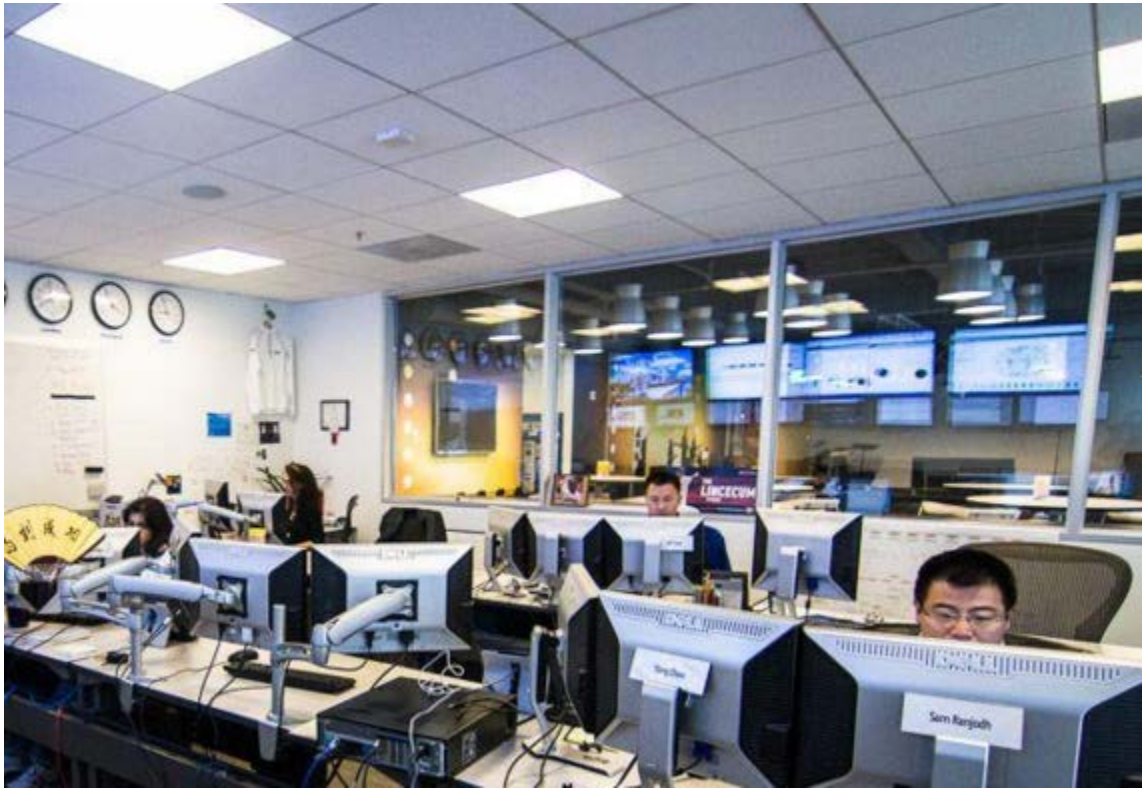
We Did it!

SNOC Impact on Uptime & CSS



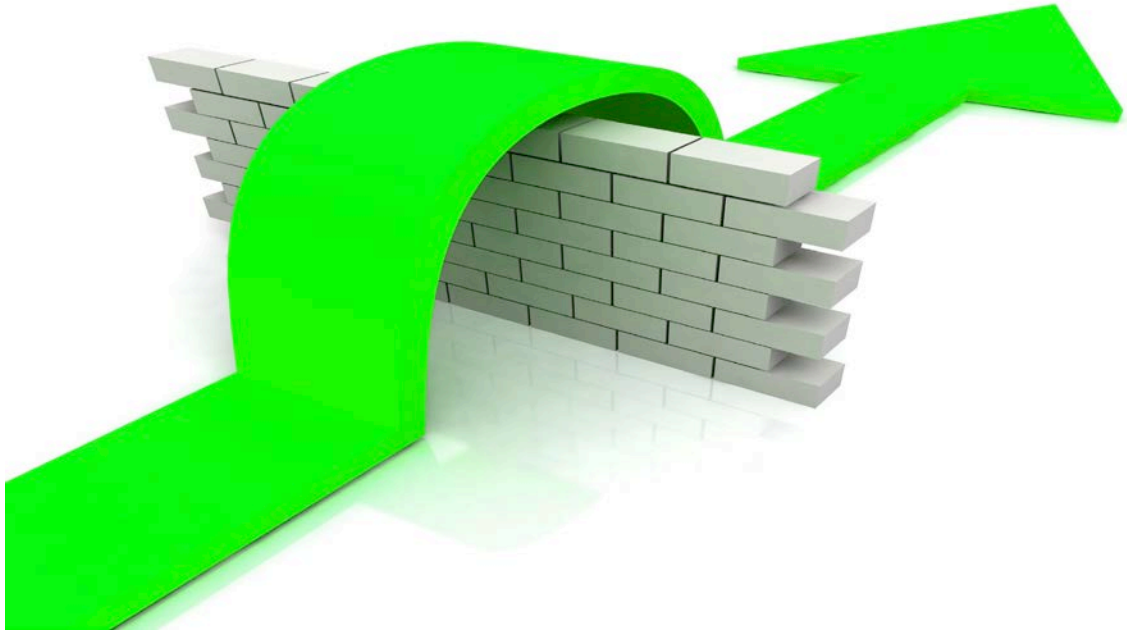
* CSS: Customer Satisfaction Score

How…

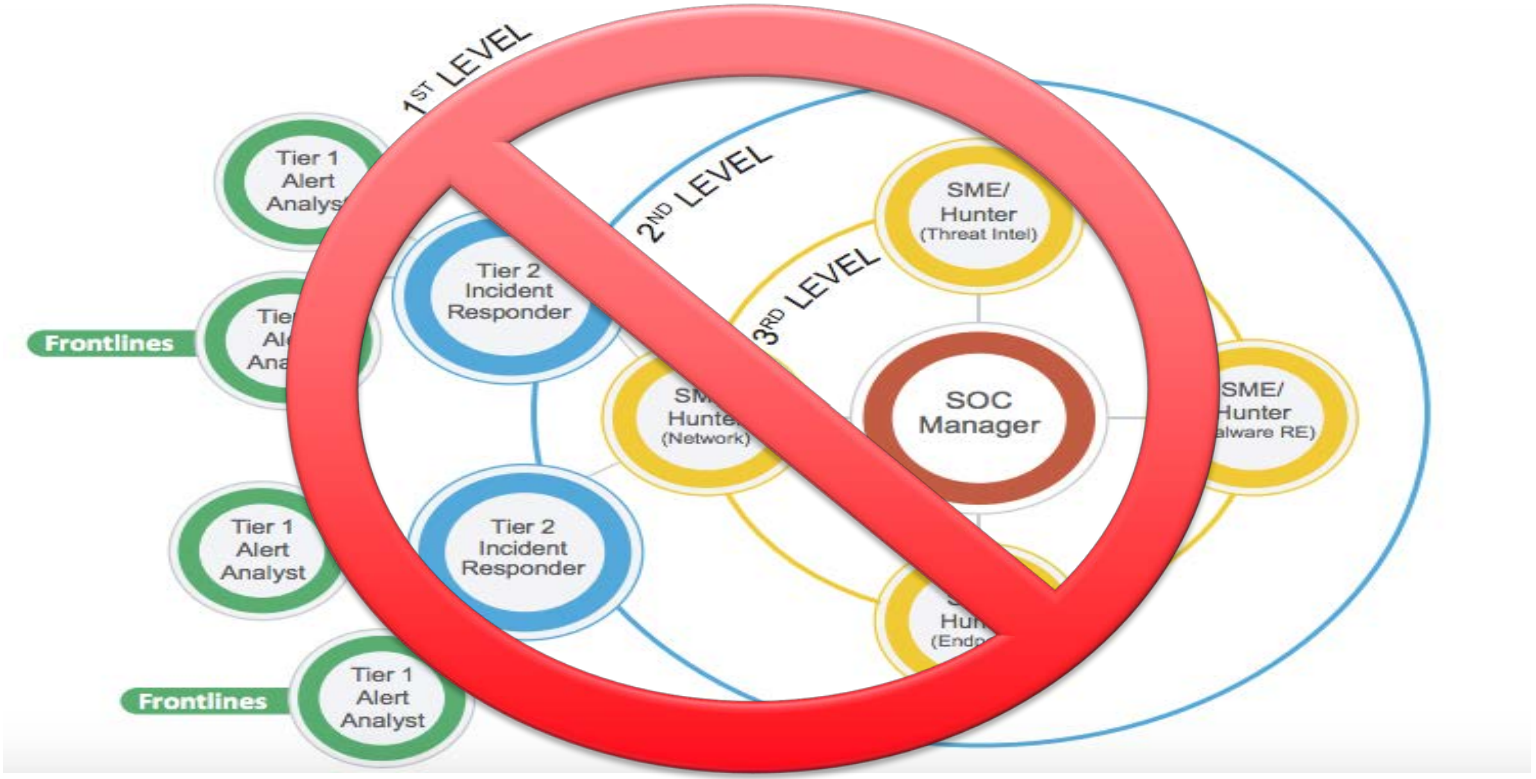


Typical NOC & SOC Challenges

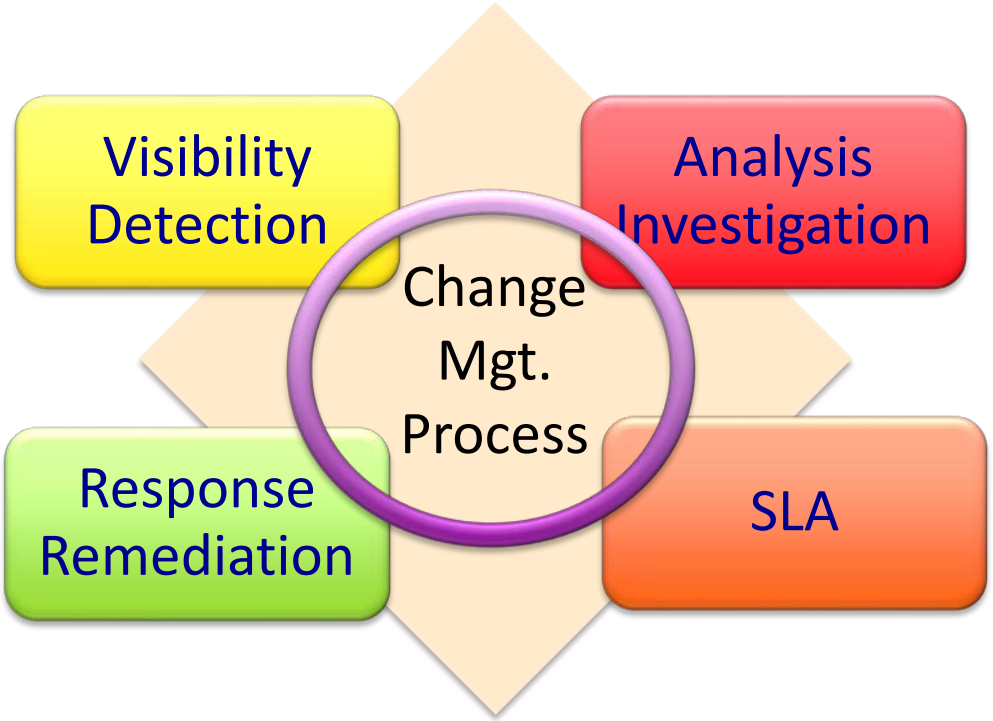
How We Overcame the Challenges



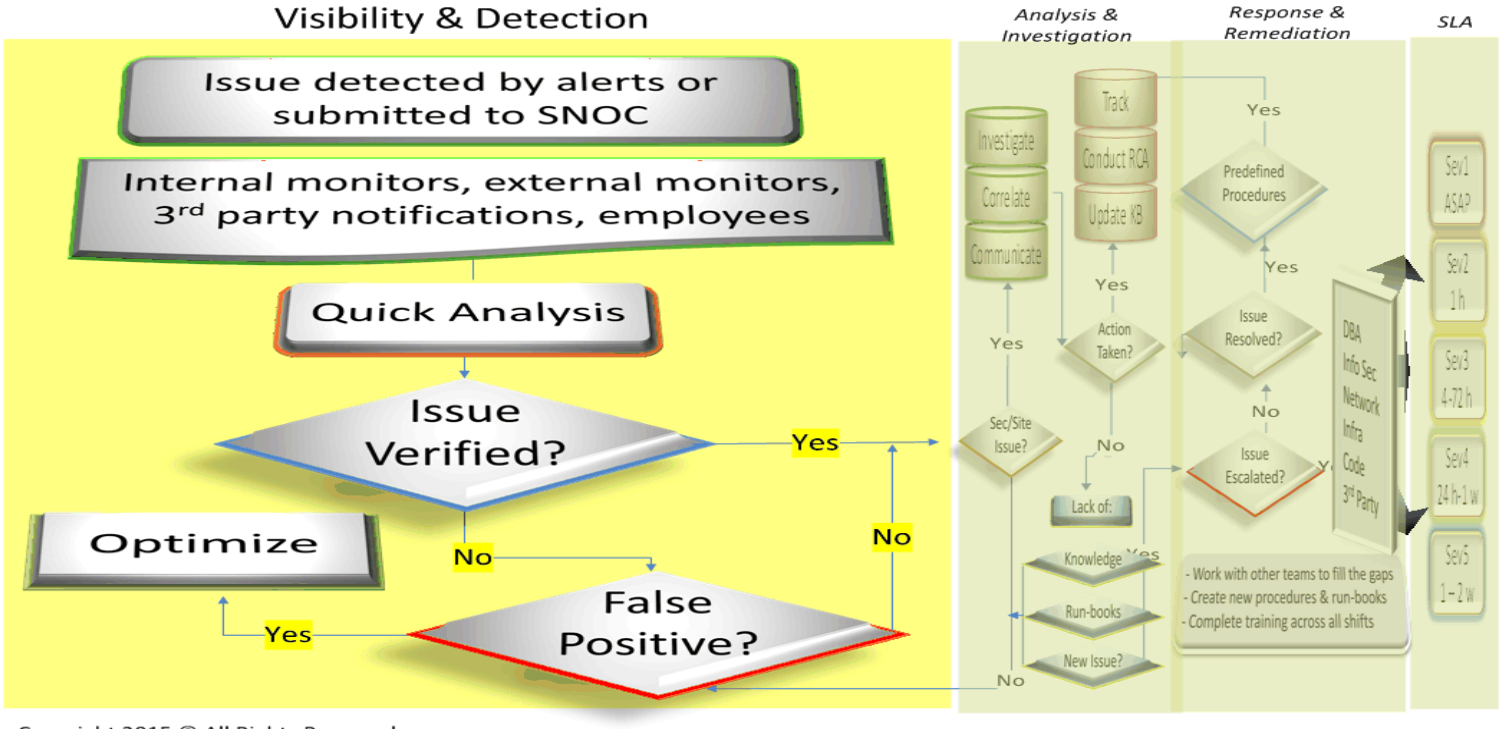
Break the Rules
Say “NO” to Traditional Tiered Model



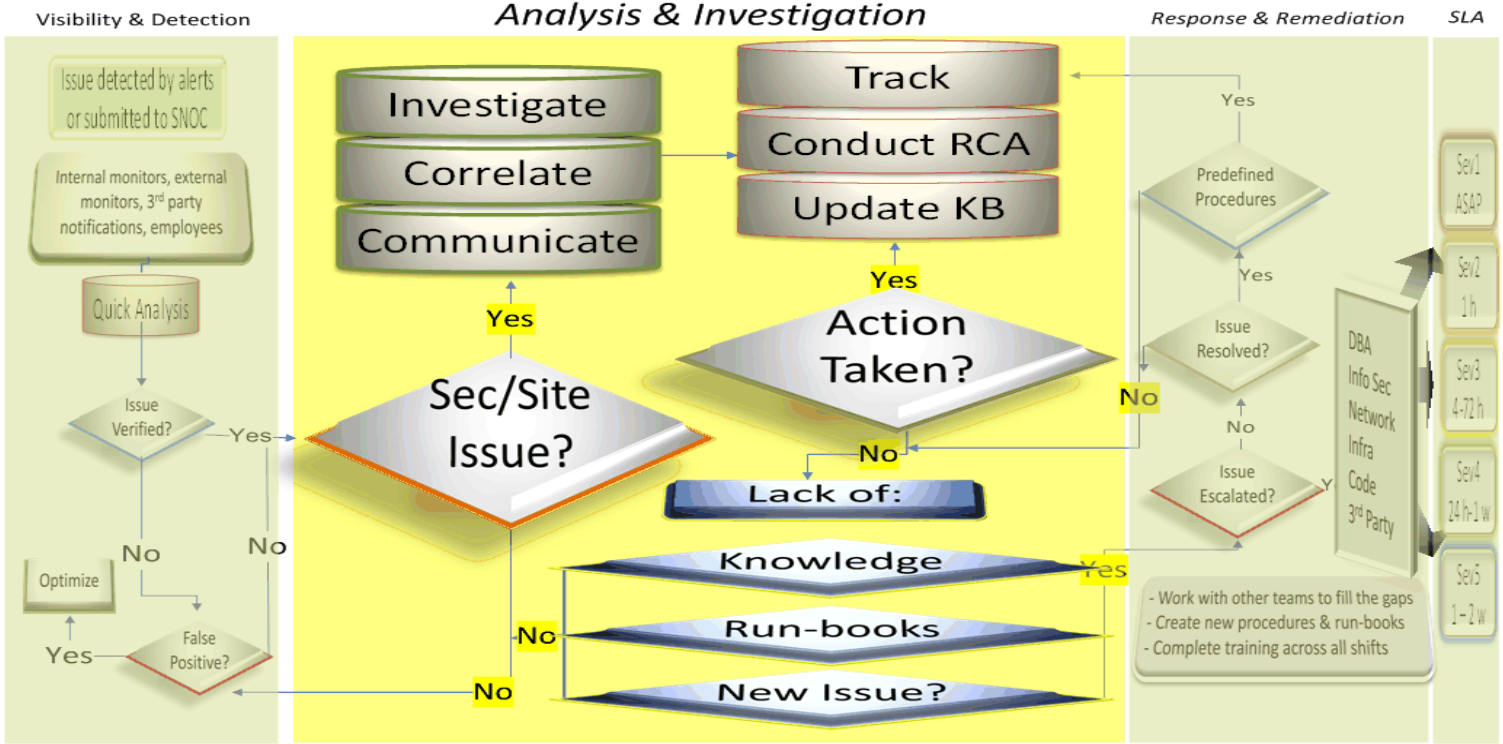
SNOC IRP (Incident Response Process)



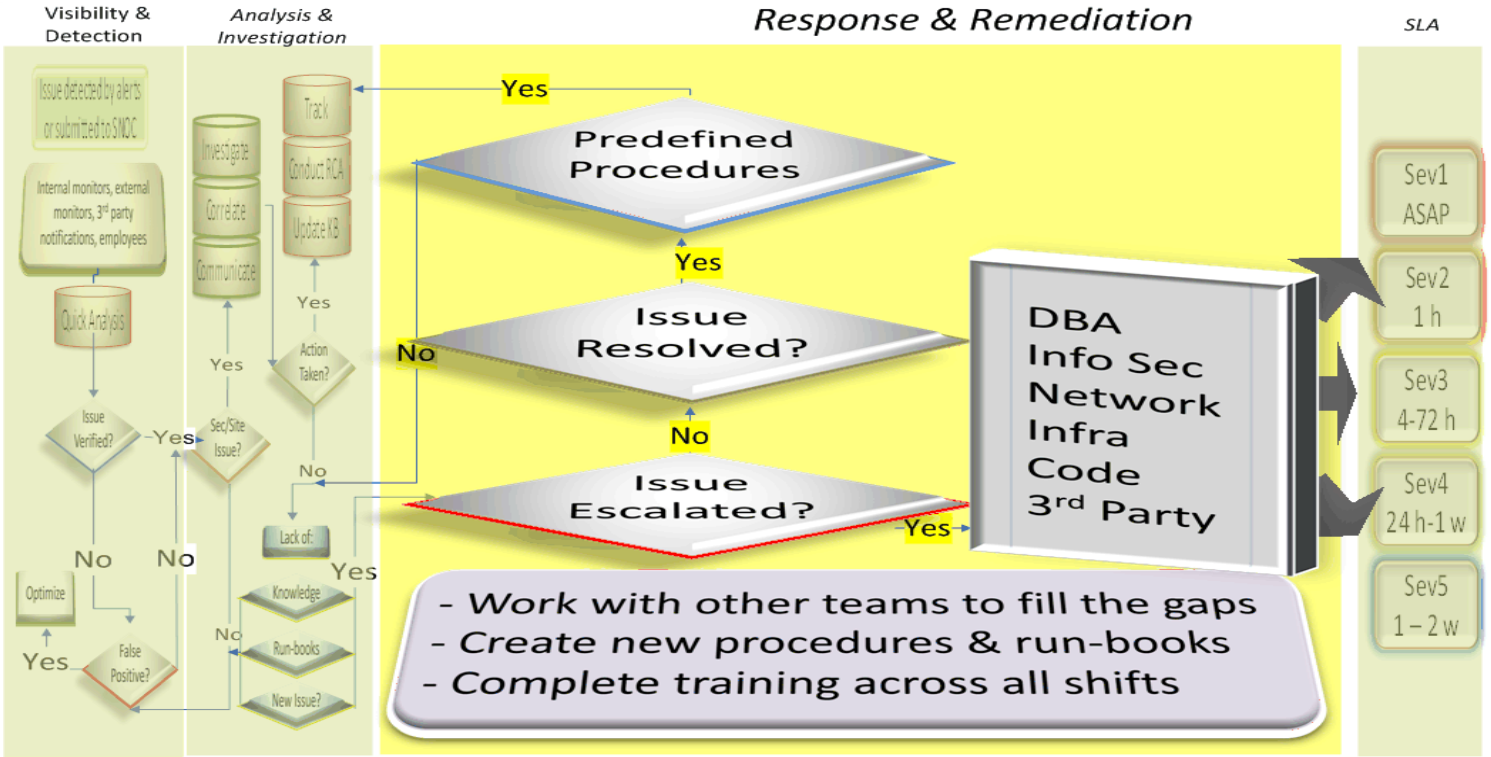
IRP – Step 1



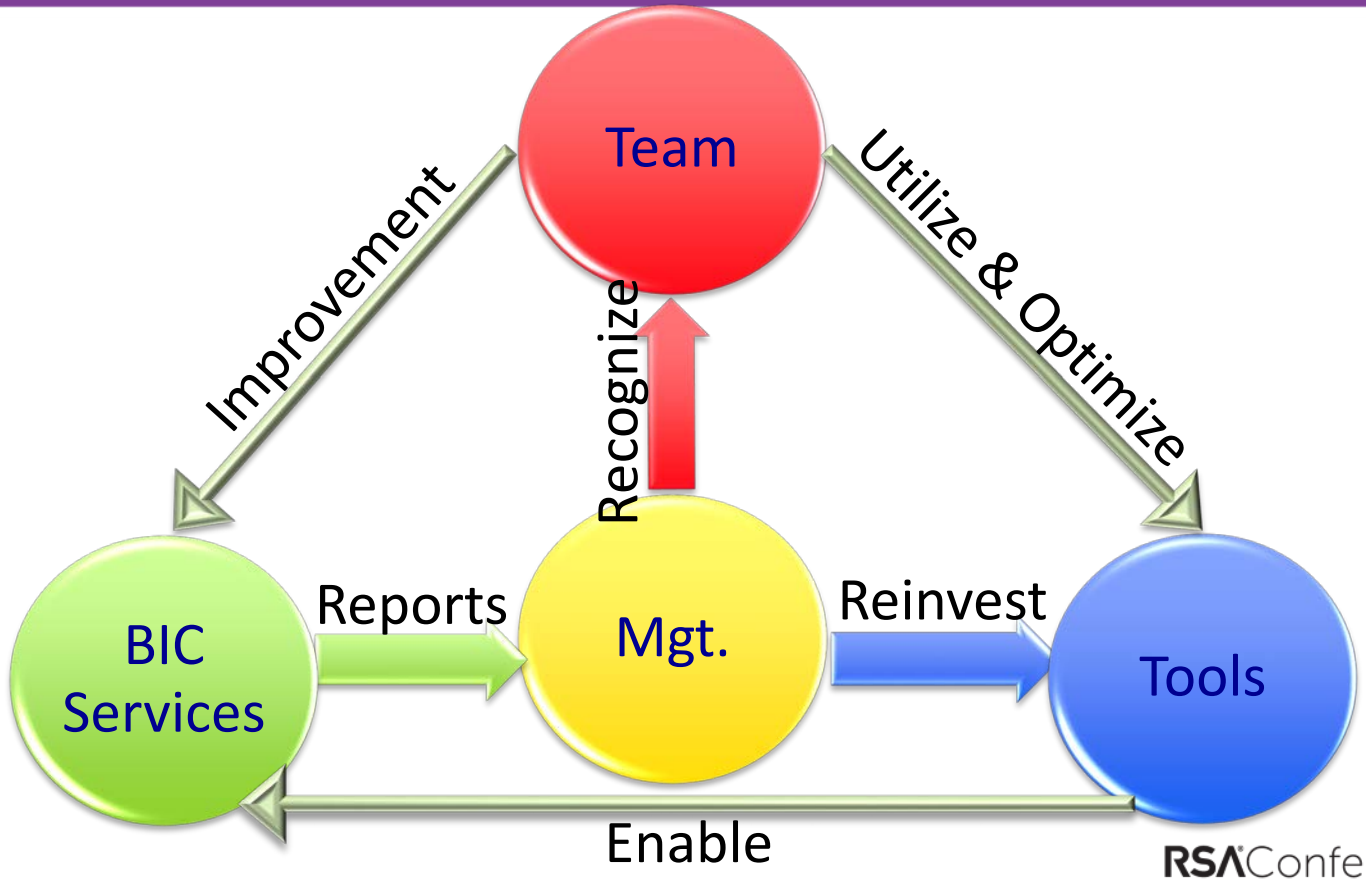
IRP – Step 2



IRP – Step 3



Proactive Integrated SNOC Framework



Building a Winning Team

Detailed SNOC Framework – Team

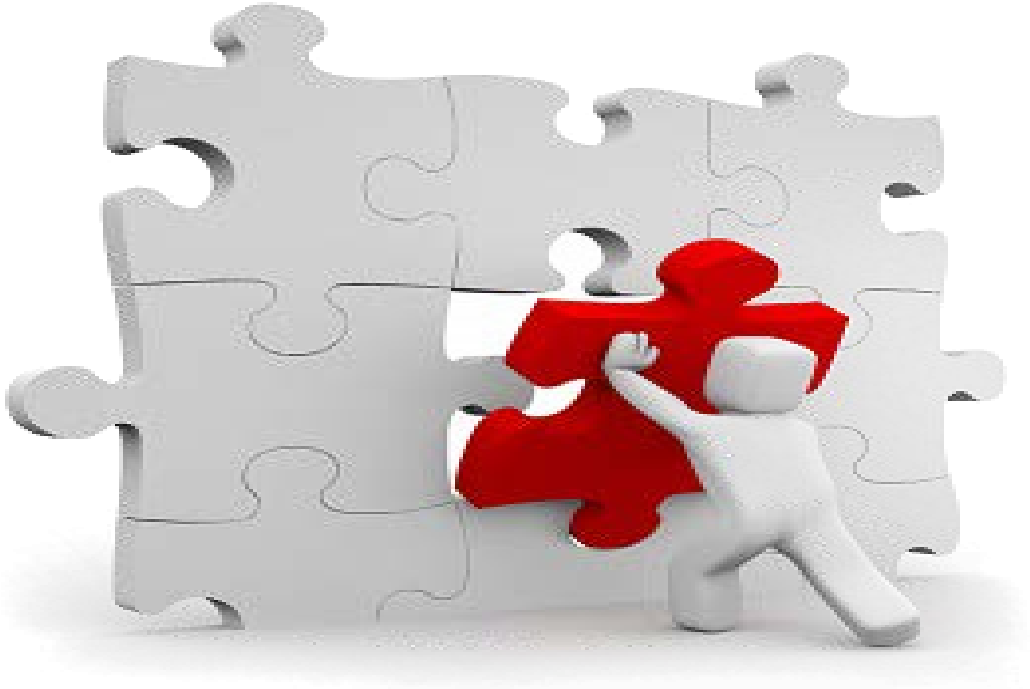
Stage 1	• Quick impact - utilize the existing structure
Stage 2	• Optimize & emphasize on quality
Stage 3	• Identify & hire talent
Stage 4	• Empower the team & remove the tiers
Stage 5	• Team development life cycle - TDLC

StubHub!

Stage 1 – Quick Impact (2 mo.)

Stage 2 – Optimize & Emphasize on Quality

Stage 3 – Identify & Hire Talent



Round out the team puzzle

Stage 4 – Empower the Team

Stage 5 - Team Development Life Cycle - TDLC

Detailed SNOC Framework – Tools

Stage 1	• Utilize
Stage 2	• Optimize
Stage 3	• Automate

Finding the Right Tools

SNOC Framework – BIC Services

Our Formula

BIC Services = Business Objectives =
Customer Satisfaction Score (CSS) + Revenue ($) + Team Defined Goals (*APS)
APS = Availability + Performance + Security

Quick results without initial Mgt support = Team + Existing Tools + Reports

SNOC Framework – Management

Our Formula

Increased demonstrated value = increased Mgt support (IMS)

IMS = Recognition + Reinvestment

Our Key to Success

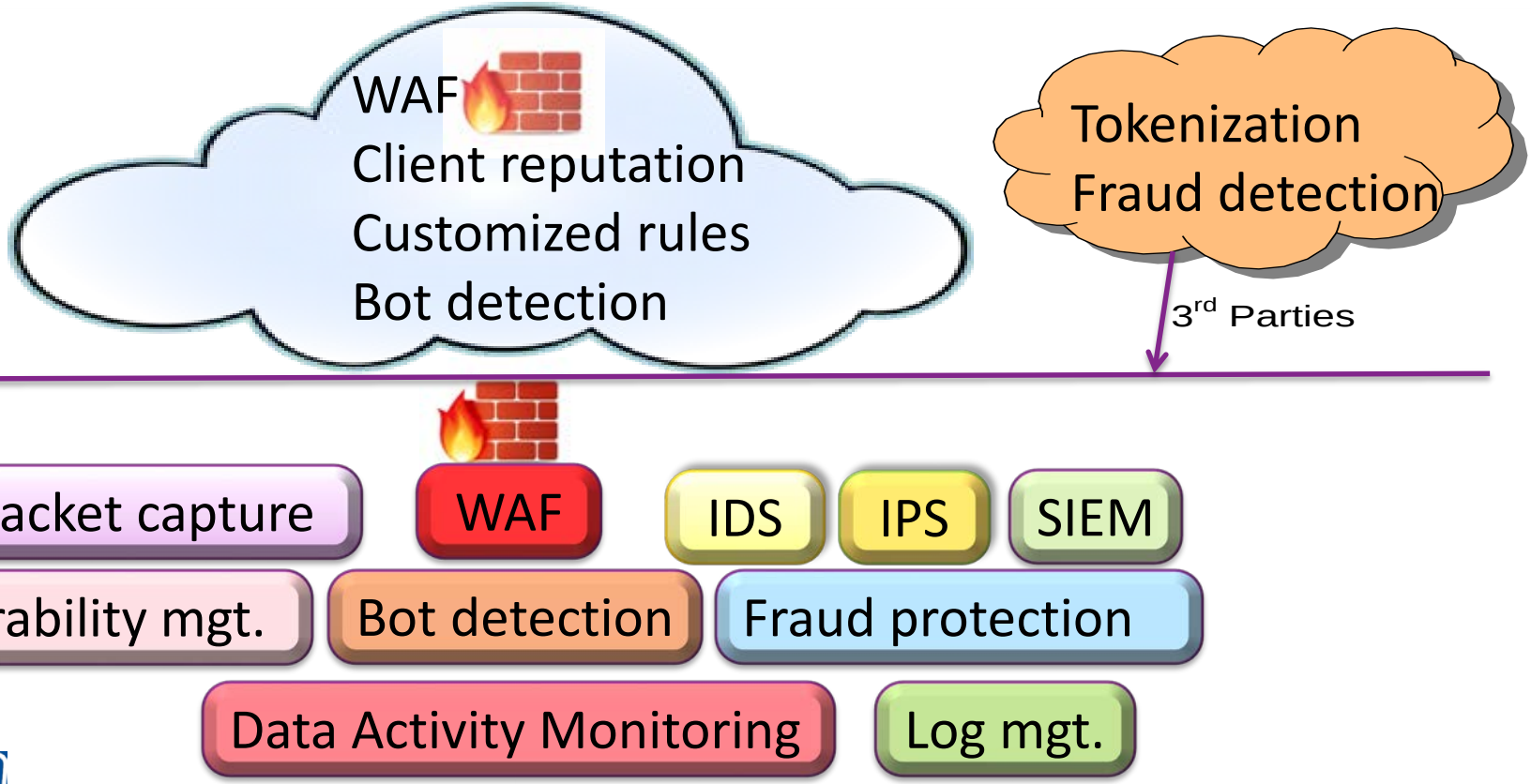
TEAM

&

Right Architecture

Team Characteristics

Right Architecture - Security Layers



Use Case – Reducing ATOs

SNOC Benefits & Future Challenges

Apply

- If you are in the process of building a SOC, and you have an existing NOC, utilize your existing NOC team and transition them to become SNOC.
- Recognize similar functions between NOC & SOC and combine them.
- Before obtaining Mgt. commitment, focus on your team as the core component to build successful SNOC.

Apply

- When you add new members, focus on character and culture fit. Try to round out the team puzzle.
- Do not pay for expertise; grow your own (entry level but highly motivated and trainable).
- Lead from the front
- Build alliances with other teams across all departments & learn from their key players.

Apply

- Understand your business goals, traffic and users.
- Filter your traffic at the edge and protect at all layers.
- Shield your data center - If your business does B2C then any cloud services who host businesses can be blocked. If your clients are within a specific geographic area, then block all other countries/areas that you do not do business with.
- To reduce ATOs & attacks, create WAF rules based on your traffic & customers' behavior.

StubHub!

Apply – Cont.

- Utilize & optimize your and other teams' existing tools.
- If no tools are available, then automate processes using scripts written by one of your own or another team's members.
- Tune out false positive alerts and train the team to tune and modify the thresholds.
- Check if the NOC has tools that are applicable for SOC usage. Example: If the NOC is using a network performance monitoring tools, check to see if the tools can perform full packet capture.

Let’s work together

My contact info:

Hanna Sicker
hsicker@stubhub.com
Twitter: @SNOCgirl

StubHub!