From Band Practice to SOC Symphony

Michael Lyons
IBM Resilient Offering Manager
What is SOAR?


- The next generation of Incident Response dramatically accelerates and sharpens response by combining case management, orchestration, artificial and human intelligence and automation in a single platform.
- Resilient uniquely delivers significant capability on all three pillars of the Gartner Security Operations, Automation, and Response (SOAR) stack.

SOAR = SOA + SIR + TIP
What is Orchestration & Automation?

What is Orchestration?
Evolving Orchestration

Orchestration Act I

- Develop standard processes
- Bring together information
- Bring together people
- All in one location
- Manual actions for escalation and remediation
Evolving Orchestration

Orchestration Act II
- Expand actions to the full suite of security technologies
- Automate actions where ever possible
- Integrating playbooks into all investigations
Evolving Orchestration

Orchestration Today
- How have we evolved?
- Are we in Act III?
- Have we achieved world domination yet?
- What is driving the growth?
Orchestration Today

Where are we?

• An Evolution of Act II
• More sophisticated use cases
• Extending the reach of the SOC

Evolution has come with 3 keys innovation:

• Dynamic Playbooks
• Extending the SOCs reach with Trust
• Last Mile IT Automation
Dynamic Playbooks
Playbooks today

Task
Integration
Script
Playbooks today
Playbooks today
Playbooks today
Dynamic Playbook
Dynamic Playbooks enable:
- Adaptive response
- Triage intelligently
- Sense complex attacks
Extending beyond the SOC with Trust
The SOC involves more places

- HR
- IT/OT
- Legal / Privacy
- Fraud

SOC
The SOC involves more places

How can we effectively build out processes to these external organizations?
The SOC involves more places

By using a foundation of Trust. But how?
Creating a foundation of Trust

The Big Scary Black Box of Automation

Commands

Desired Results
Creating a foundation of Trust

The Big Scary Black Box of Automation

Commands
Creating a foundation of Trust

How can we validate the actions are correct?
Creating a foundation of Trust

The Big Scary Black Box of Automation

Validation

Commands
Creating a foundation of Trust

The Big Scary Black Box of Automation

Validation

Commands
Creating a foundation of Trust

How can we explain what happened?
Creating a foundation of Trust

The Big Scary Black Box of Automation

Commands → Validation

Explainability

Trust
Extending beyond the SOC with Trust
Last Mile IT Automation
Last Mile IT Automation - Yesterday

Large Ticket volume and no way to track them all
Large Ticket volume and no way to track them all
Last Mile IT Automation - Today

SOC

SOAR Platform

IT

ITSM / Ticketing

Trust

SIEM

Telemetry

IBM Security
Last Mile IT Automation - Today

- SOC
- SOAR Platform
- Trust
- IT
  - ITSM / Ticketing
- SIEM
- Telemetry

IBM Security
Conduct a Symphony
Questions?!?!
Conducting a Symphony
An Integrated Response to a Malware Attack

QRAadar: Log & event collection, correlation, and analytics.

Resilient: Incident management and orchestrated response.

Ansible: Provisioning, config mgmt, and application deployment tool.

Distributed Servers: Find & Remove
Demo