Overcoming Security Automation Roadblocks

Overcoming Myths, Determining Best Practices

About the Presenter

John Moran

- Sr. Product Manager, DFLabs
- IR Consultant
- Law Enforcement

DFLABS
CYBER INCIDENTS UNDER CONTROL

Automation Myths Obscure Reality

DFLABS
CYBER INCIDENTS UNDER CONTROL

Myth: Automation means fewer jobs

DFLABS
CYBER INCIDENTS UNDER CONTROL

Automation should supplement, not replace

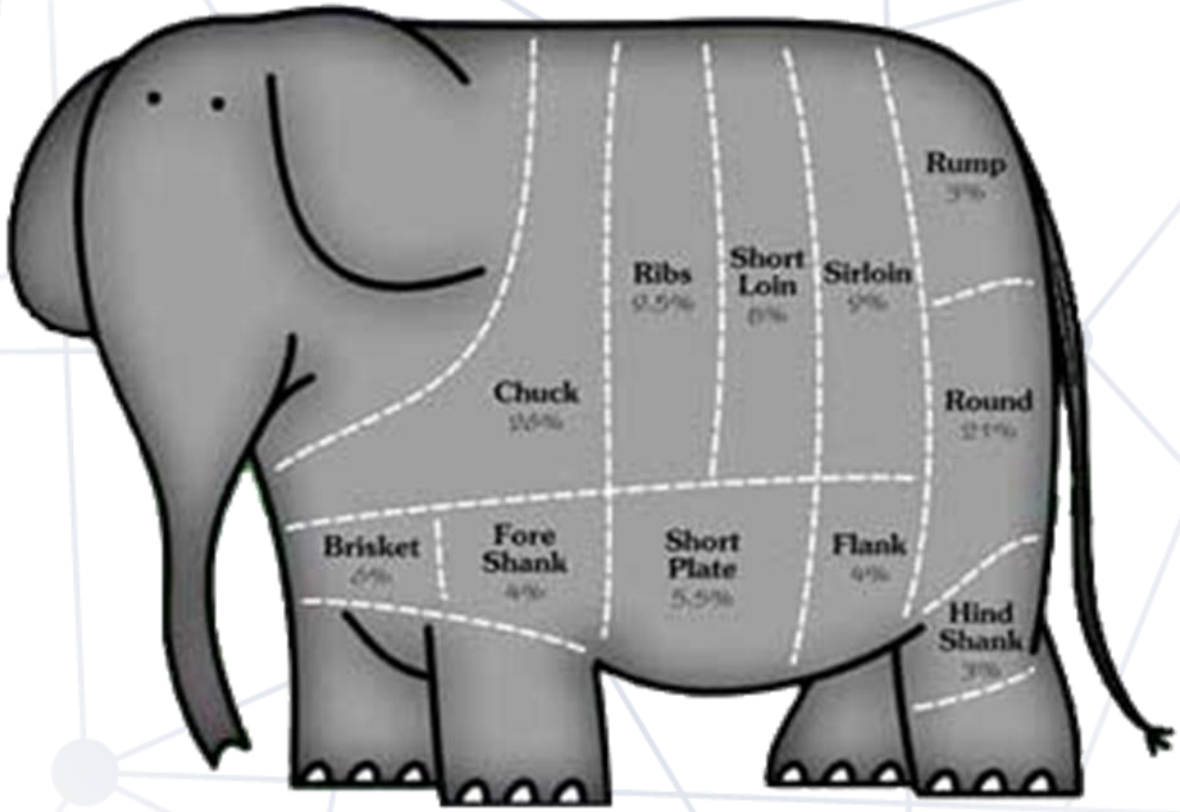
- Analysts are being inundated with alerts
- Too much time spent on mundane, repeatable tasks
- Automation should supplement, not replace
- Allow analysts to focus on tasks which require human intervention

DFLABS
CYBER INCIDENTS UNDER CONTROL

Myth: Security it too complex to automate

DFLABS
CYBER INCIDENTS UNDER CONTROL

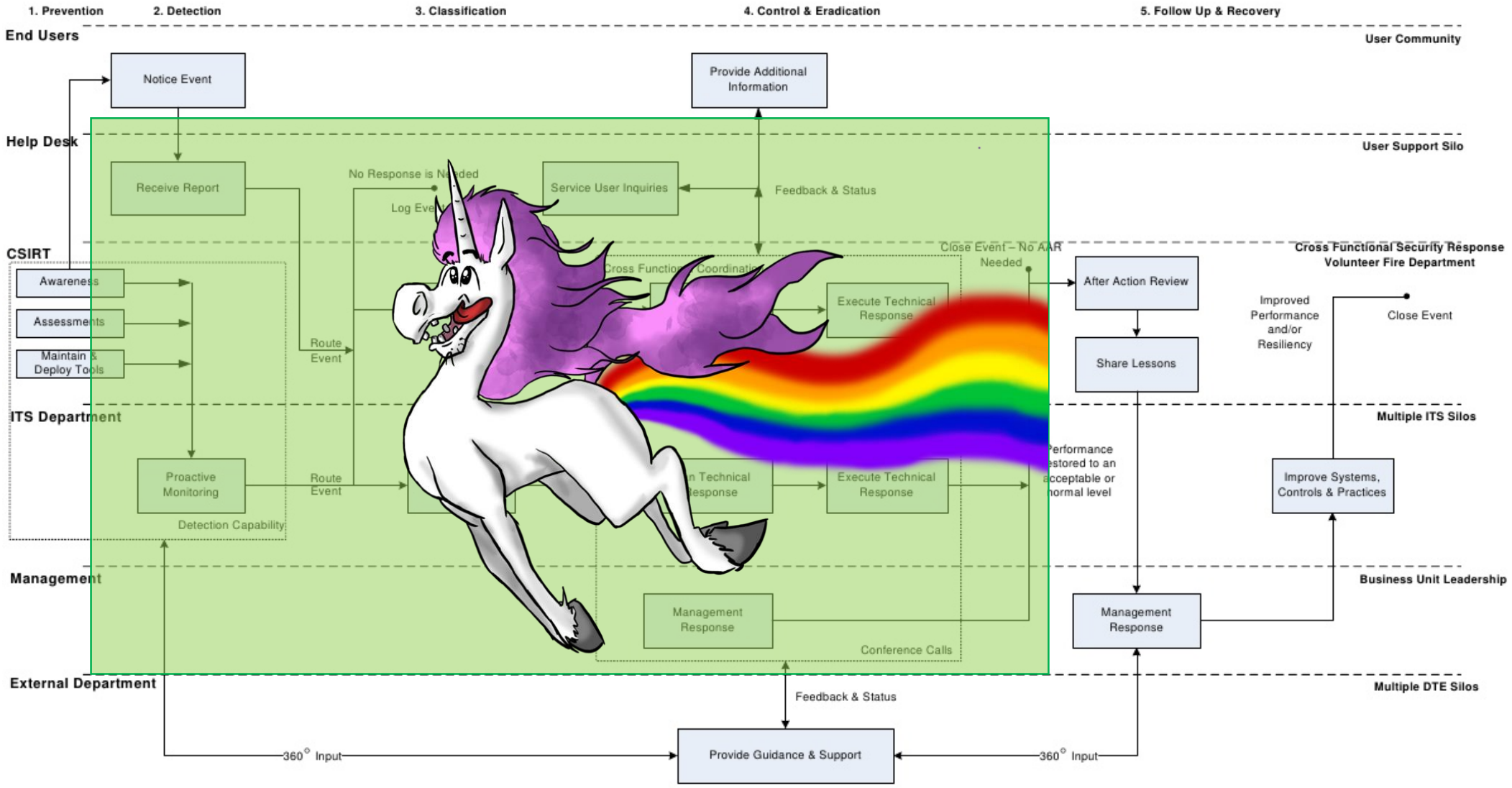
Start with small, manageable bites



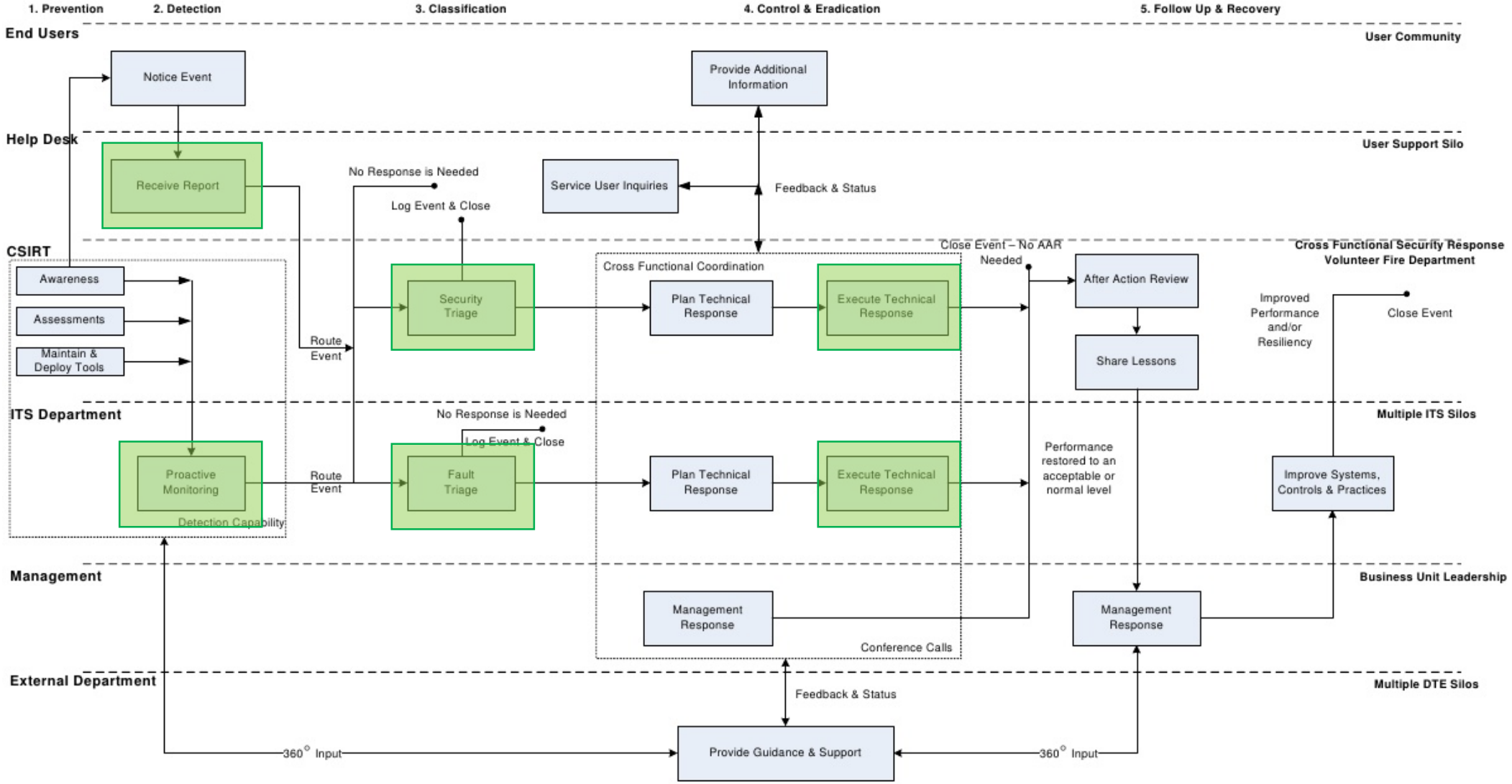
DFLABS
CYBER INCIDENTS UNDER CONTROL

Myth: Automation is dangerous

DFLABS
CYBER INCIDENTS UNDER CONTROL



DFLABS
CYBER INCIDENTS UNDER CONTROL



DFLABS
CYBER INCIDENTS UNDER CONTROL

Best Practices = Best Results

DFLABS
CYBER INCIDENTS UNDER CONTROL

Why Automate?

- Have measurable goals in mind:
  - Automate the repetitive, mundane tasks
  - Decrease time to respond to an incident
  - Act as a force multiplier for security teams
  - Respond in a documented, repeatable manner
  - Reduce risk

DFLABS
CYBER INCIDENTS UNDER CONTROL

Identifying Processes to Automate

- Review all security processes and tools
  - Which tools can be easily automated?
  - Which processes are consistent and predictable?
  - Which processes are repetitive?
  - Which processes require little human intervention?
  - Which processes are taking too much time?

DFLABS
CYBER INCIDENTS UNDER CONTROL

Getting Started

- Small, easy to automate processes
- Well documented, well understood processes
- Quickly and easily show value
- Build out from there…

DFLABS
CYBER INCIDENTS UNDER CONTROL

Human are not the Enemy!

- The goal is *NOT* to remove humans from the process
- Automation and analysts should complement each other
- Include human interaction at critical junctions or decisions

DFLABS
CYBER INCIDENTS UNDER CONTROL

Common Use Cases

DFLABS
CYBER INCIDENTS UNDER CONTROL

Phishing Email

- ✓Query threat data for:
  - Embedded links
  - Sender email
  - IPs in header
- ✓Scan email attachments
- ✓Scan embedded URLs
- ✓Check for other instances
- ✓Quarantine email
- ✓Notify users

DFLABS
CYBER INCIDENTS UNDER CONTROL

Proxy Alert - URL

- ✓Query threat data
- ✓Get domain info
- ✓Get A records
- ✓Geolocate IPs
- ✓WHOIS queries
- ✓Access URL via Sandbox
- ✓Query Proxy or SIEM logs
- ✓Block domain

DFLABS
CYBER INCIDENTS UNDER CONTROL

IDS Alert

- ✓Query threat data
- ✓Geolocate IPs
- ✓Reverse DNS
- ✓WHOIS queries
- ✓Traceroute
- ✓Query Proxy or SIEM logs
- ✓Simulate network traffic
- ✓Block IP

DFLABS
CYBER INCIDENTS UNDER CONTROL

Questions?

DFLABS
CYBER INCIDENTS UNDER CONTROL

Thanks!

DFLABS
CYBER INCIDENTS UNDER CONTROL

John Moran
Senior Product Manager, DFLabs
john.moran@dflabs.com