

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: STR-F02

Introduction to Defending the Enterprise using Automated Security Operations

RSA 2019 | Version 1.0

Tomasz Bania
Dolby
@baniasec



#RSAC

Tomasz Bania

Cyber Defense Manager,
Information Security, Dolby

- Formerly Cyber Defense Center Lead at HP
- 8 Years in IT
- 6 Years in Cyber Security
- Worked within Government, Education, and Enterprise

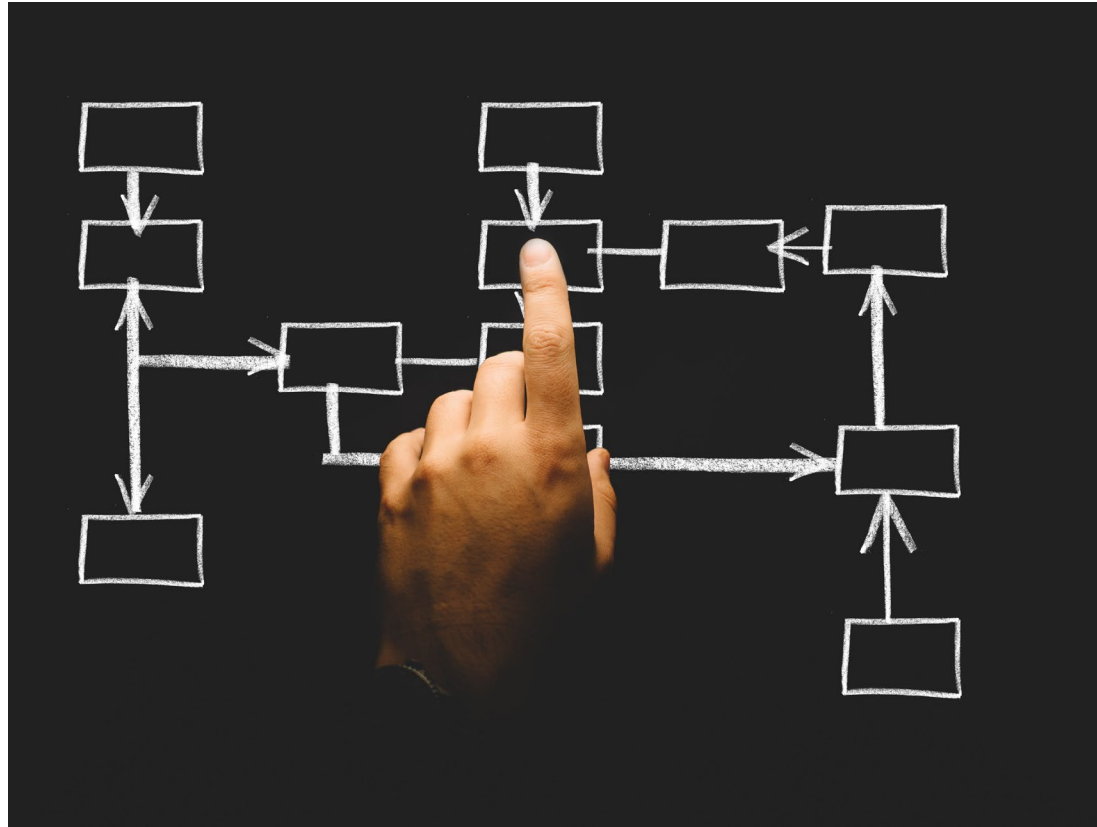


Automation: What is it?



What is Security Orchestration, Automation and Response(SOAR)?

- SOAR is the integration of disparate security platforms to complete workloads leveraging various levels of human interaction.



Why is Automation Important?

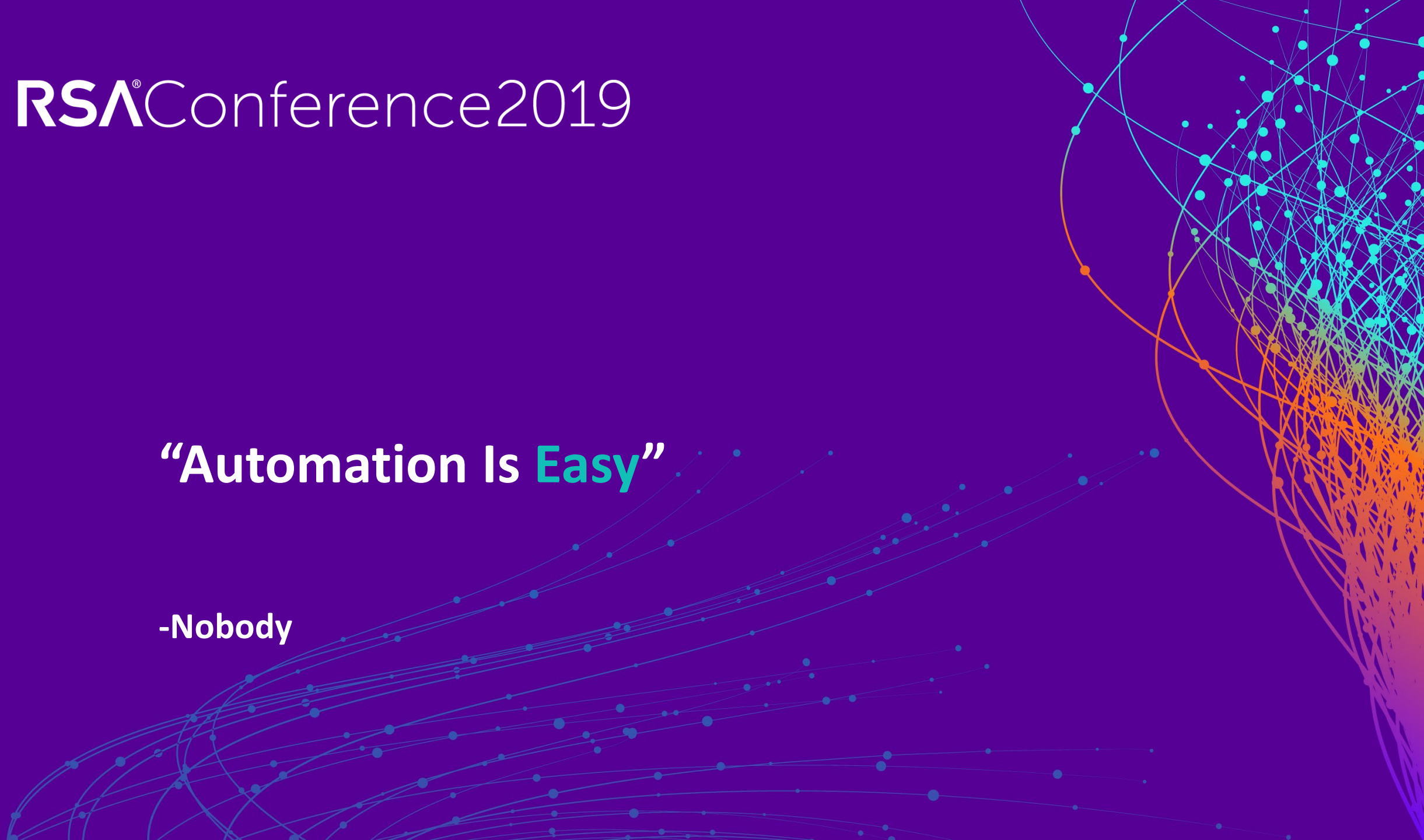
- 62% of Organizations report Security Challenges related to the Lack of skilled staff (SANS 2018 SOC Report)
 - Addressing the skills gap with automation allows organizations to improve their security posture by improving the efficiency of resources already present



RSA®Conference2019

“Automation Is Easy”

-Nobody



What are security teams saying about automation?

- 50% of Organizations Report Challenges related to Lack of automation and orchestration (Second only to the hiring of skilled staff) (SANS 2018 SOC Report)
- Only 18% of organizations feel they have implemented an effective Security Automation Strategy (SANS 2018 SOC Report)

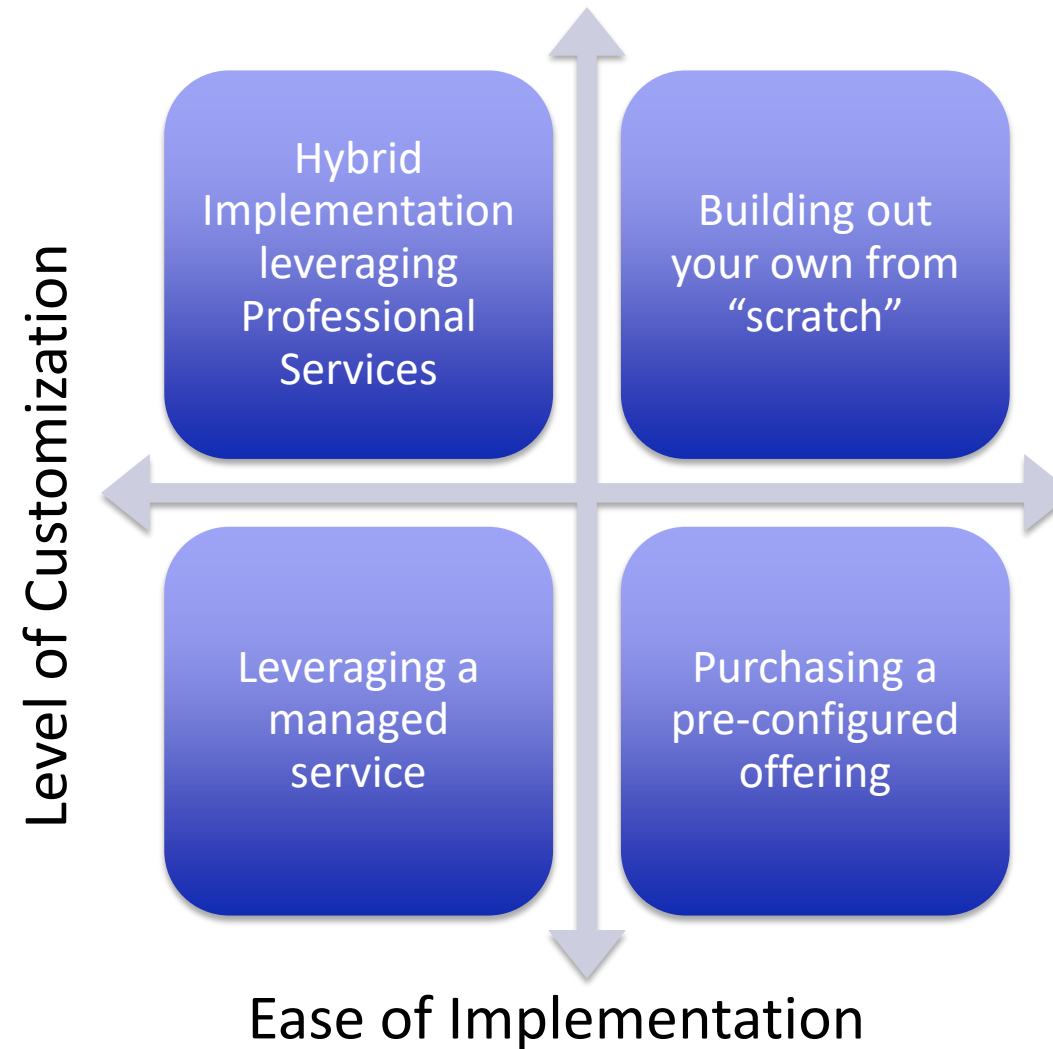


RSAConference2019

Automation: Where do I Start?



The Four Paths to Automated Security Operations



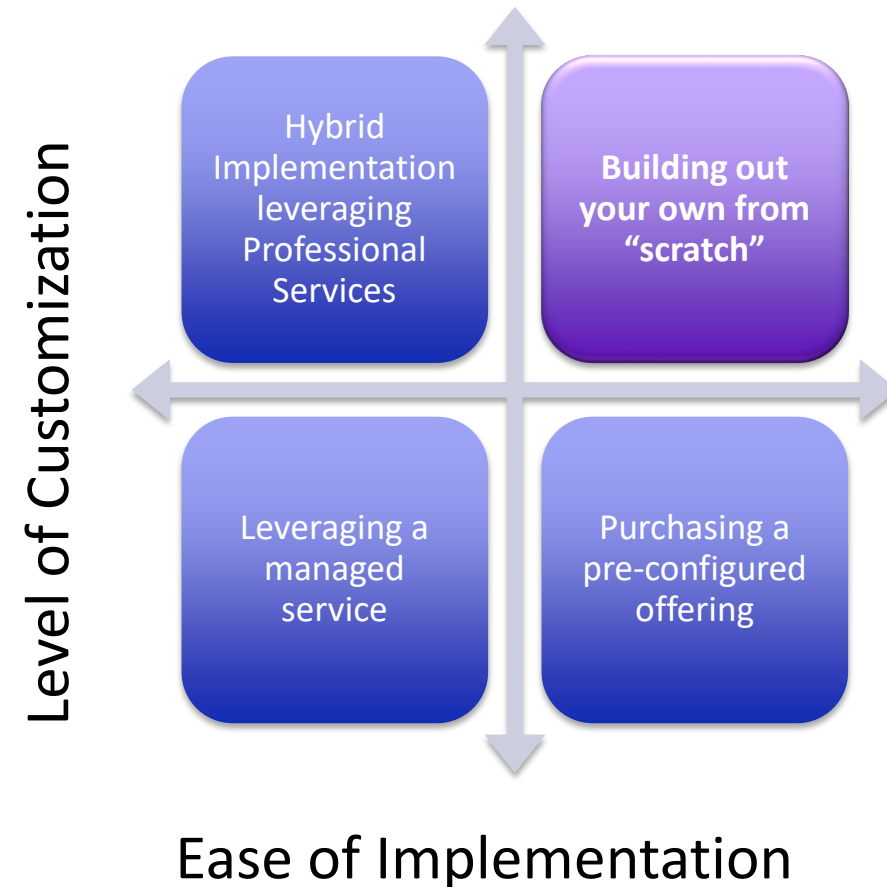
Building Out Your Own From “Scratch”

► Pros:

- Full Customization
- No Functional or External Limitations

► Cons:

- High Cost to Effectively Implement (Time/Resources)
- Must Self-Correct for any updates and changes to any external platforms
- Significant Ongoing Maintenance



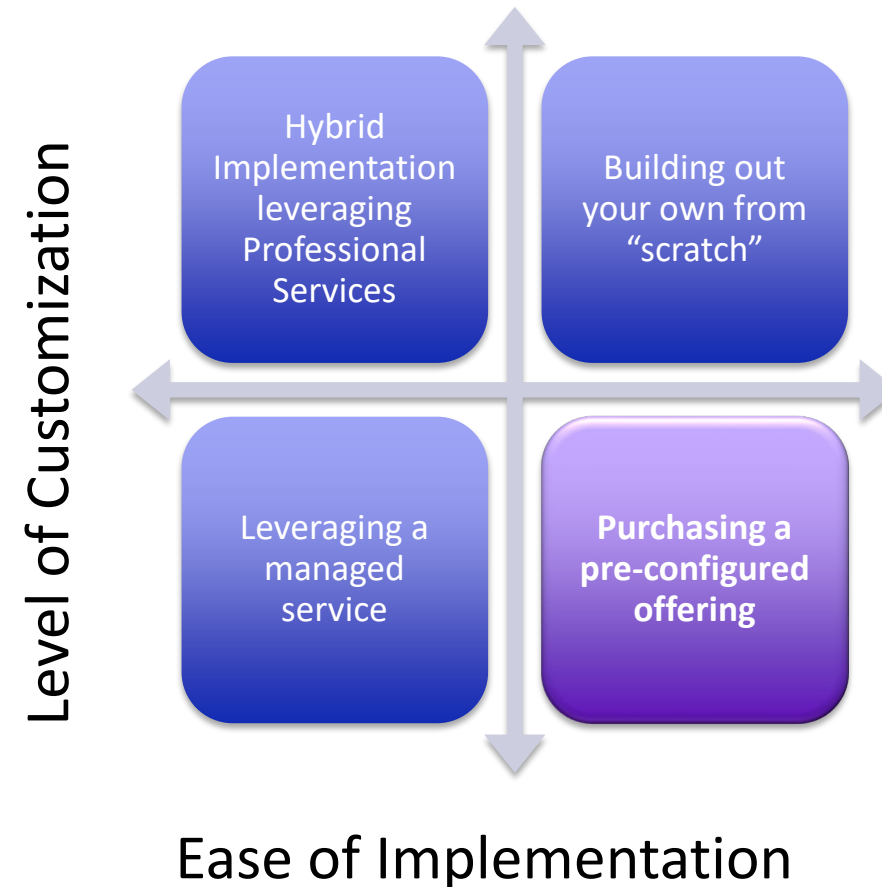
Purchasing a Pre-Configured Offering

► Pros:

- Provides a great base to build on
- Frees up time to implement automations and integrate tools

► Cons:

- Functionality Partially Dependent on Vendor



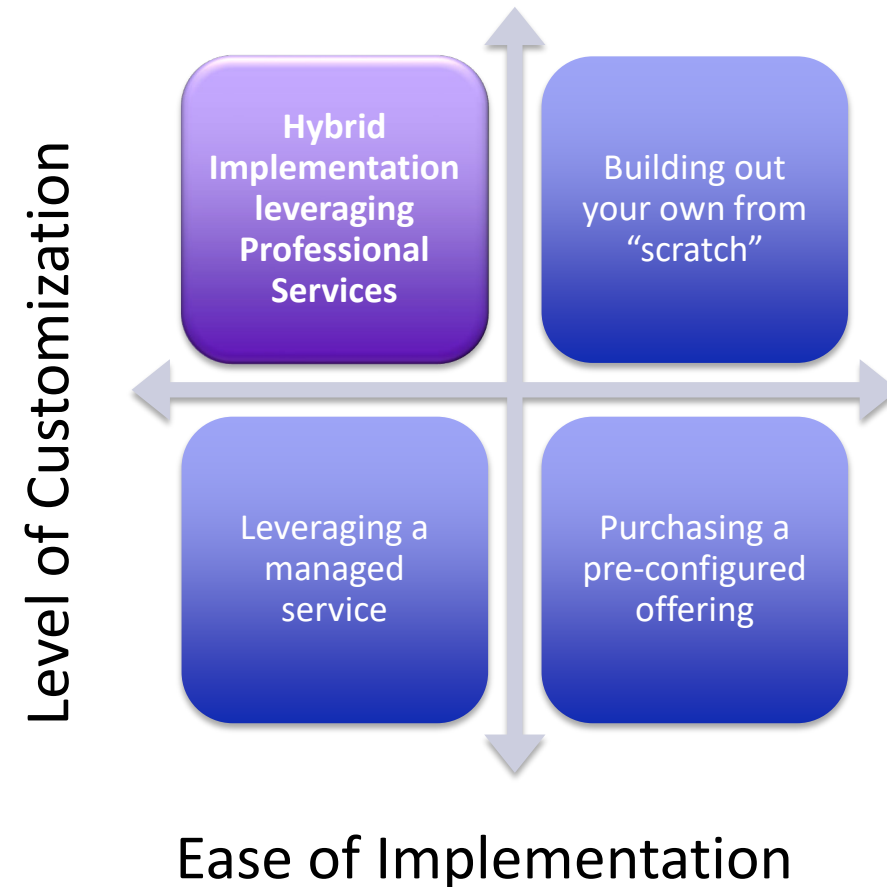
Hybrid Development Leveraging Professional Services

► Pros:

- Flexibility to Implement Custom Configurations with ease
- Gain Insight and Validation from Third Party

► Cons:

- External Development Resource is potentially shared and may limit speed of implementation



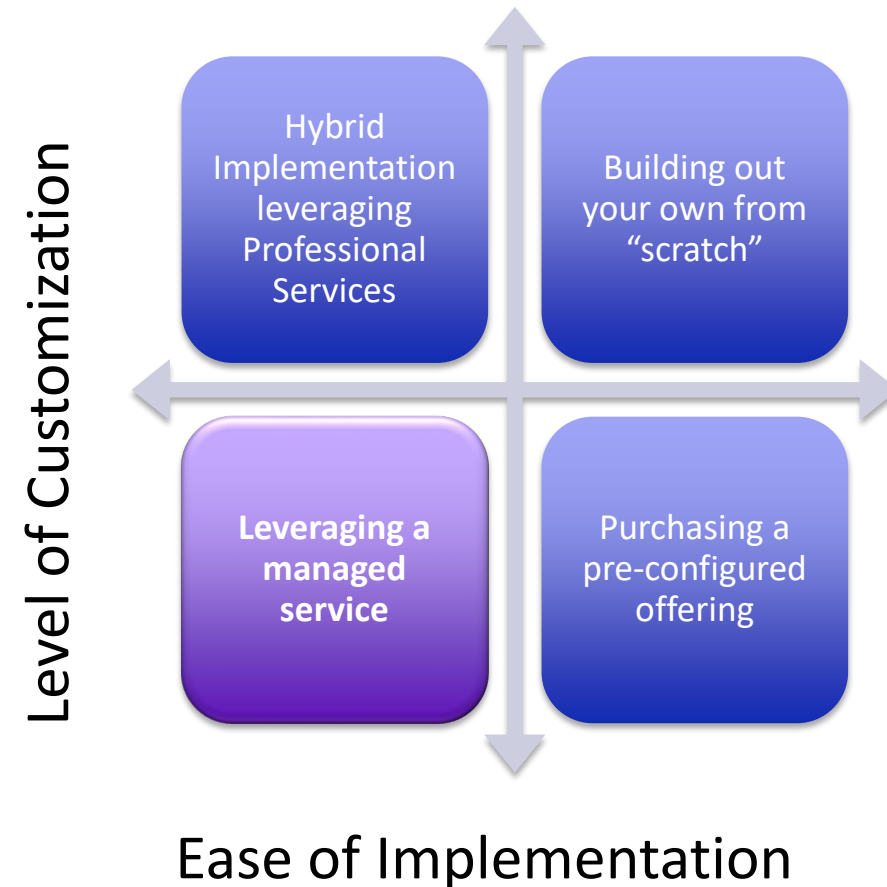
Leveraging a Managed Service

► Pros:

- Near-Instant Return On Investment (Post-Implementation)

► Cons:

- Can be Very Costly
- Potentially Limited Scope of Service
- Vendor Lock-In



How Do I choose the right path?

- Cost Considerations
 - Resources
 - *Financial*
 - *Personnel*
- Organizational Knowledge
 - “Does your organization have people who truly ‘know’ what to do?”
 - *Extensive operational experience*
 - *Comprehensive existing workflows/playbooks*
- Enterprise Resources
 - “Is there any resistance to automating certain actions (such as blocking IP’s or domains automatically)?”
 - “Does your security team have access to (or have the buy-in of IT) to implement the automations you are looking to do?”
 - “Do your platforms support the pace of automation planned?”

I've settled on a path, now what?

- With all paths:
 - Ensuring there is an understanding regarding the following:
 - *Expected Deliverables*
 - *SLA's/SLO's*
 - *Continuous Improvement Plan*
- If leveraging a managed service or purchasing a preconfigured offering:
 - Balancing Expectations Vs. Realities
 - *You are not the only client...*
 - *...however, you can leverage the collective knowledge gained by others*
- If Building Your own or Leveraging External Contractors
 - Defining your automation goals and benchmarks
 - Determining what is in-scope and out-of-scope
 - *Do I implement an automated block or do I automate a notification to an engineer for validation?*

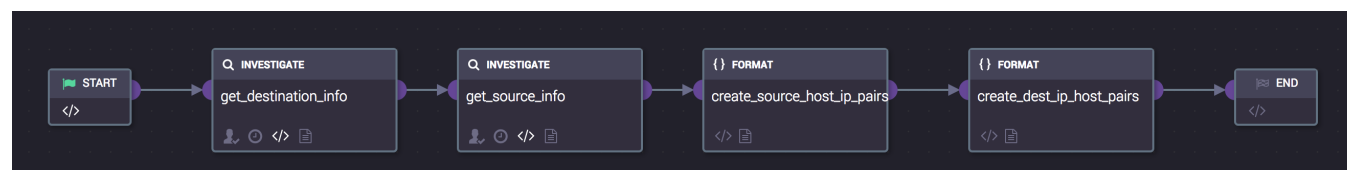
Where Not to begin your Automation Journey

- Buy a product/solution without an implementation plan
 - Avoid buying “shelfware”
 - Review existing documented processes
 - Validate organizational knowledge of existing platforms
 - Define # of FTE available for automation management
- Trying to automate everything on day one
 - Prioritize your automations using the following criteria:
 - Is there buy-in for the workflow?
 - Is the workflow repeatable?
 - Is there an API or script?
 - Is it Time-Consuming?

Tactical Orchestration vs Strategic Automation

- Tactical Orchestration
 - Individual Tasks or Workflows
 - Implementation of Security Exceptions

- Strategic Automation
 - Combination of Orchestrations to complete a Full Security Response
 - End To End Incident Response Playbook



How can I measure my organizations Automation Effectiveness?



• Level One

- Manual Processing



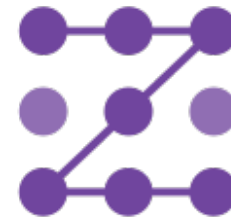
• Level Two

- Limited Orchestration
- No Automation



• Level Three

- Significant Orchestration
- Some Automation



• Level Four

- Full Orchestration
- Significant Automation



• Level Five

- End to End SOAR Implementation

How To Calculate ROI

- Document the steps to your workflow
- Determine the time needed to manually complete every step
- Use a normalized salary to calculate cost/minute (keep note that no downtime is factored into the calculation)
- Document the time needed to complete the action using automation
- Compare the time and cost between manual and automated processing

Automation Return on Investment

- April-December 2017
 - Addressing the Basics
 - 50-100 Automated Events/Day
 - \$75k ROI
 - 5 Active Playbooks
- End of 2018
 - Enhancing the Lineup
 - 1,000 Automated Events/Day
 - \$500k ROI
 - 17 Active Playbooks
- End of 2019
 - Closing the Loop
 - ~25,000 Automated Events/Day
 - \$10M ROI
 - 25 Active Playbooks

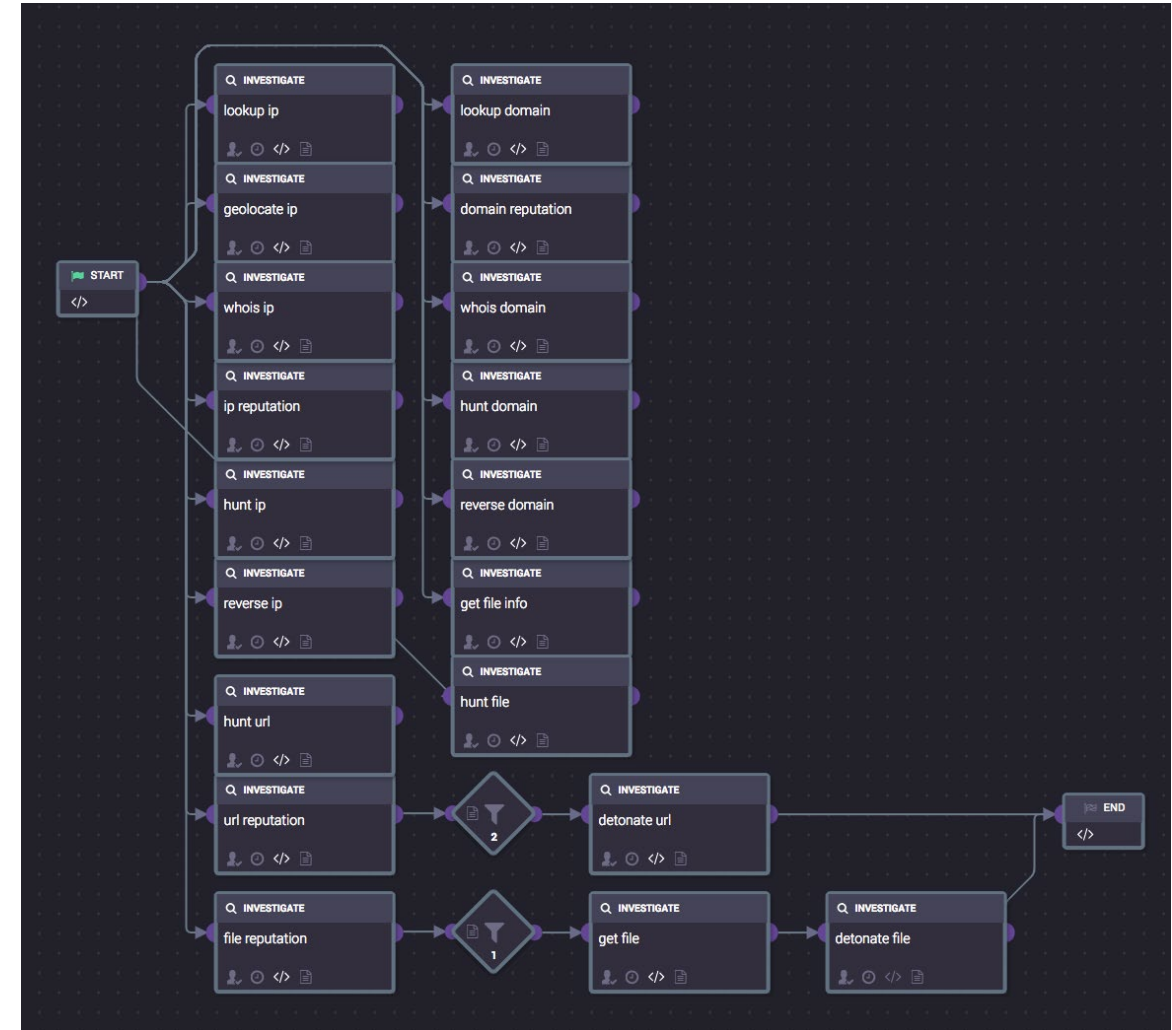
RSAConference2019

Automation: What Can I Do?



What are some things I can automate?

- Basic Automated Phishing Analysis
 - Gathering Submissions
 - Conducting Analysis
 - Implementing desired actions based on findings
- Automated Alert Analysis and Remediation
 - Forwarding alerts to automation platforms
 - Conducting an Investigation
 - Establishing a remediation plan
- Temporary Security Exception Management
 - Manual or Automated Input
 - *Examples:*
 - *Temporary Network Access*
 - *Temporary Escalated Permissions*
 - Orchestrated Implementation
 - Effective Reporting



How can I get this done in my organization?

- Next 30 Days
 - Identify opportunities for automation within your organization
 - Verify buy-in from potentially involved or impacted groups
- Before Next Budget Cycle
 - Develop an implementation plan suitable to your operation
 - Validate your capex/opex costs to limit possible delays
- During The Implementation
 - Ensure that resources are available to complete the process
 - Document contingency plans should an automation stop functioning

Key Takeaways

- Ensure that your financial and organizational resources are sufficient to move forward with a chosen path.
- Establish a Security Automation strategy before acquiring and/or implementing a solution.
- Maintain implementation guidelines and continuous improvement benchmarks that are clear and appropriate.

RSA®Conference2019

Thank You



Resources

- SANS 2018 SOC Report
- Gartner SOAR Innovation Insight 2017

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID:



#RSAC

“Apply” Slide

- Bullet point here (see slides 5 – 8 for instructions)
- Bullet point here
- Bullet point here

RSA[®]Conference2019

