
# Introduction to Defending the Enterprise using Automated Security Operations

Tomasz Bania

October 2018

# Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.



splunk> .conf18

# 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 in Government, Education, and Enterprise
- Background in Government Network Securities and Management

# Automation: What is it?

# What is Security Automation and Orchestration (SAO)?

- SAO is the integration of disparate security platforms to complete workloads using limited human interaction

splunk> .conf18

# Why is Automation Important?

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

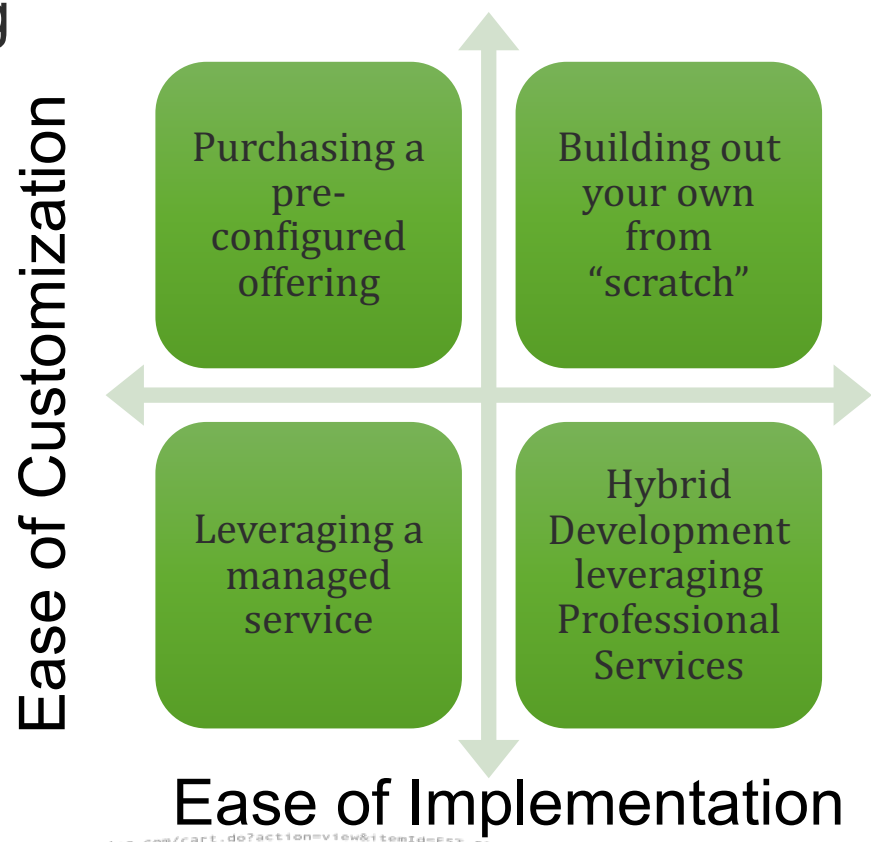
# Is Automation Easy?

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

# Automation: Where do I Start?

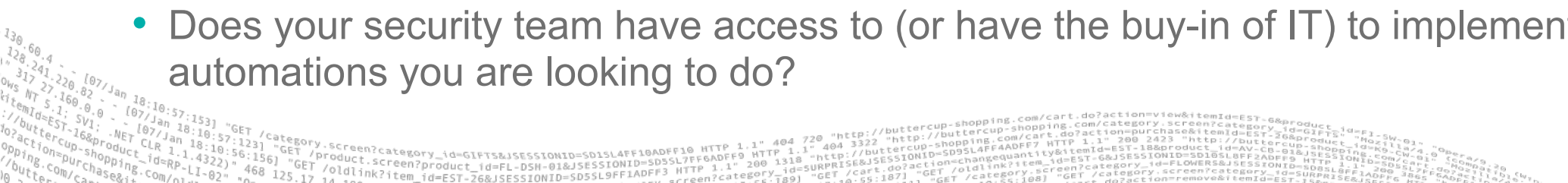
# The Four Paths to Automated Security Operations

- Building out your own from “scratch”
- Hybrid Development leveraging Professional Services
- Purchasing a pre-configured offering
- Leveraging a managed service



# How Do I choose the Right Path?

- Cost Considerations
  - Resources
    - *Financial*
    - *Personnel*
- Organizational Knowledge
  - Does your organization have people that 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?



splunk> .conf18

# 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 the workflow repeatable?
    - Is there an API or script?
    - Is it Time-Consuming?

# Tactical VS Strategic Automation

- Tactical Automation
  - Individual Tasks or Workflows
- Strategic Automation
  - Combination of multiple automated workflows

splunk> .conf18

# How Can I Measure my Organizations Automation Effectiveness?

- Level One - No Automation
- Level Two - Limited Tactical Automation/No Strategic
- Level Three -  Significant Tactical/Limited Strategic
- Level Four - Full Tactical/Partial Strategic
- Level Five - Full Tactical and Strategic Automation

# 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 Orchestration and Management
  - Manual or Automated Input
    - *Examples:*
      - *Temporary Network Access*
      - *Temporary Firewall Opening for Controlled Environments*
  - Orchestrated Implementation
  - Effective Reporting

# Resources

- SANS 2018 SOC Report
- Gartner SOAR Innovation Insight 2017

splunk> .conf18

# Thank You

**Don't forget to rate this session in the .conf18 mobile app**