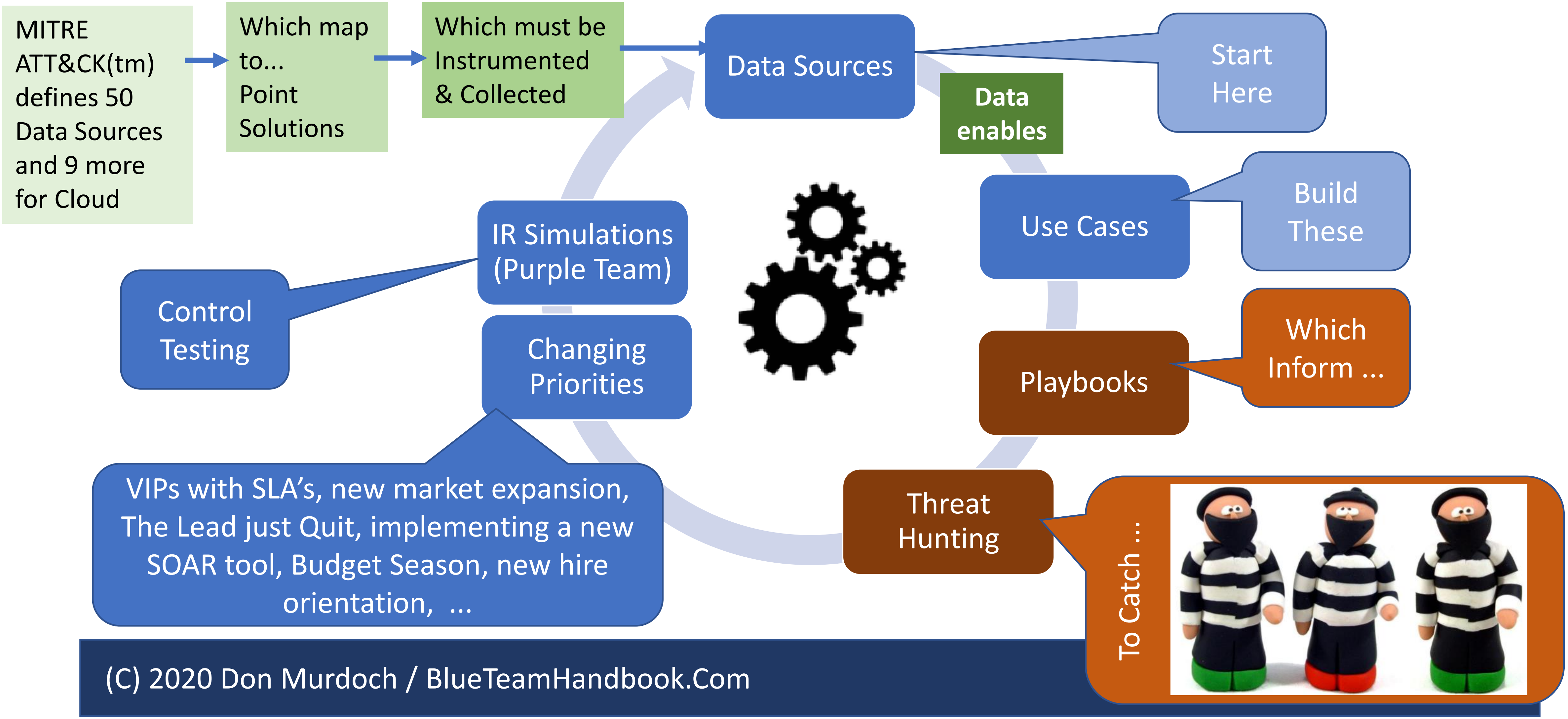
Building a Better Playbook
Don Murdoch, GSE

We often hear "Follow the playbook", but what makes playbook? This presentation will go over the components of a playbook, their creation and maintenance, how playbooks are used in IR Simulation and other governance programs, and a host of supporting tools that improve playbook usage like Confluence.

Agenda

- About $me
  - 20+ years in InfoSec, GSE, Author *Blue Team Handbook: INCRE & SOC/TH*
- Playbooks and the SOC Workstream Cycle
- The Investigation Challenge and its Impact on Playbook definition
- Sample Table of Contents
- Adversary Simulation, Purple Teaming, IR Simulation
- Playbook Metrics
- Confluence Examples

SOC Workstream Cyclone



MITRE ATT&CK(tm) defines 50 Data Sources and 9 more for Cloud

Which map to... Point Solutions

Which must be Instrumented & Collected

Data Sources

Start Here

Data enables

Use Cases

Build These

Playbooks

Which Inform ...

Threat Hunting

To Catch ...

IR Simulations (Purple Team)

Control Testing

Changing Priorities

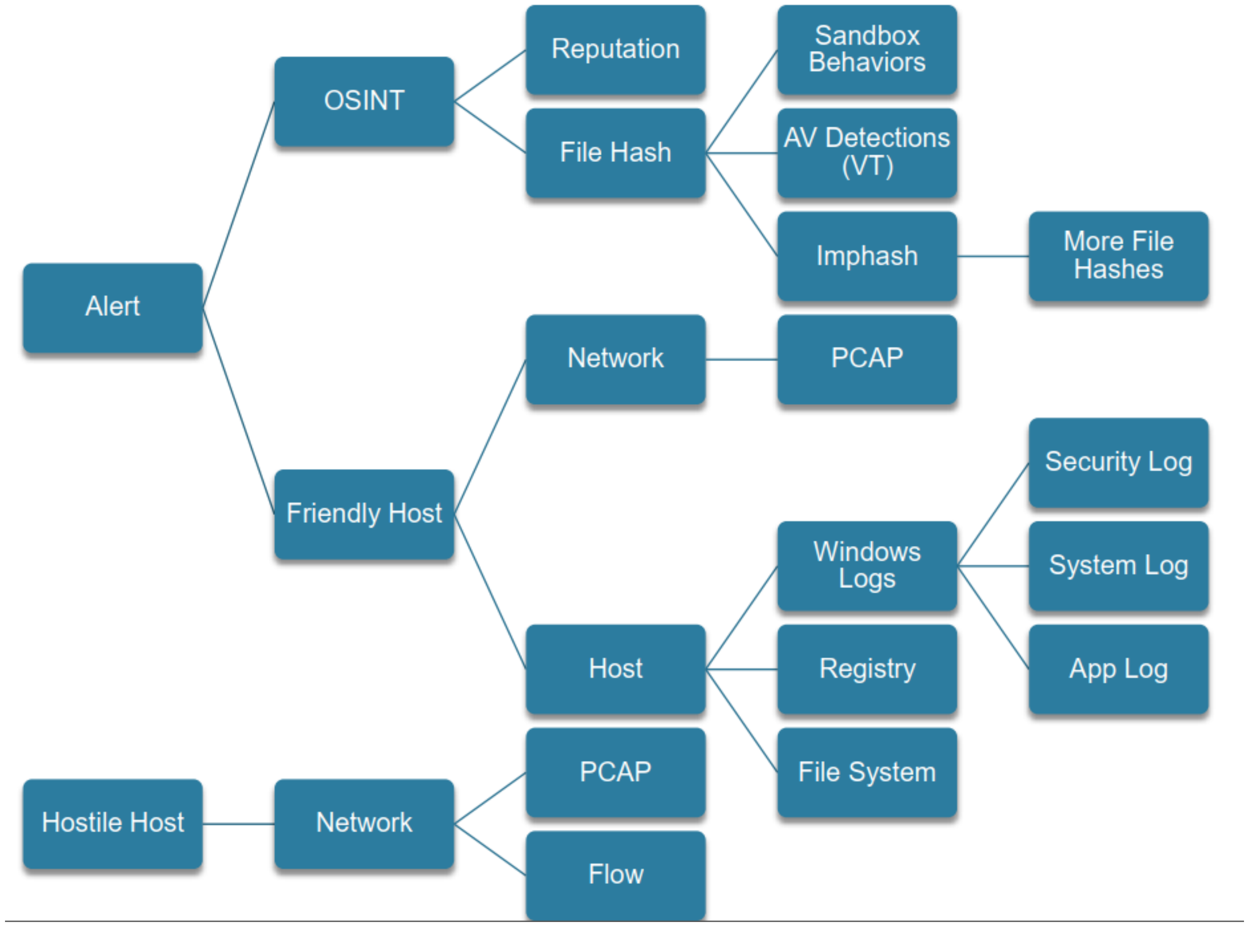
VIPs with SLA's, new market expansion, The Lead just Quit, implementing a new SOAR tool, Budget Season, new hire orientation, ...

Playbook Defined

- Part One:
  - Self-contained, fully documented, prescriptive procedures for finding and responding to undesired activity.
- Part Two:
  - A series of repeatable and predictable methods intended to elicit a specific response to an event or incident.
- Therefore:
  - A Playbook is predictable written guidance for the analyst to analyze events and alarms in order determine incident type, severity, and follow up treatment.

The Investigation Challenge by Chris Sanders

- Investigations are a series of decisions that begat other decisions.
- Is the Analyst on the right path?
- High context (PCAP) preferred 84% of time, but slows investigation and decision time down as much as 40%
- The more ‘steps’, the longer time to close
- Analysts prefer to investigate “unknown”
- Seeking to “Disprove” results in 58% improvement in close time



Ref: https://www.slideshare.net/chrissanders88/soc2016-the-investigation-labyrinth

Playbook Sample Table of Contents

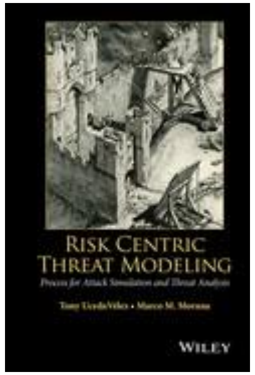
- Title Box (Confluence Page Props!)
  - Title:
  - Description:
  - Author:
  - Date:
  - Last Revised (& By)
- Discussion:
  - Objective Statement
  - Triggering Condition(s)
  - Fidelity
  - Analysis Steps
  - Key Data
  - Escalation / Notification
  - Output
  - Standardized Messaging (cuz gramma and spellink countz)
- Solution Support
  - Event Source
  - Data Query
  - Breadcrumbs
  - Report(s), Dashboard(s), Alert(s)
- SOAR Support
  - Testable conditions and messaging
  - Retrieve supplemental indicators
- Validation Process
  - Condition Trigger
  - Last Tested

PB ToC Notes

- The **objective statement** is intended to provide background information and good reasoning for why the play exists.
  - Not for a Security Engineer
  - For an IT knowledgeable person what to look for on the network
  - Answer the “What and the Why”
- Analysis section advises the analyst on how to investigate the alert and act on the results.
  - Be as prescriptive and insightful as possible
- Data Query/Code
  - Esp for query driven systems like Splunk, Kibana, NetWitness, ...

Where Do You Start?

- What are we trying to protect?
  - Privileged users, trade secret, client/internal data, business process, brand, l..
- What are the threats?
  - Threat Modeling – a strategic process aimed at considering possible attack scenarios and vulnerabilities within a proposed or existing application environment for the purpose of clearly identifying risk and impact levels.
- How do we detect them?
  - OS, Application, Network, and point solution instrumentation
- How do we respond?

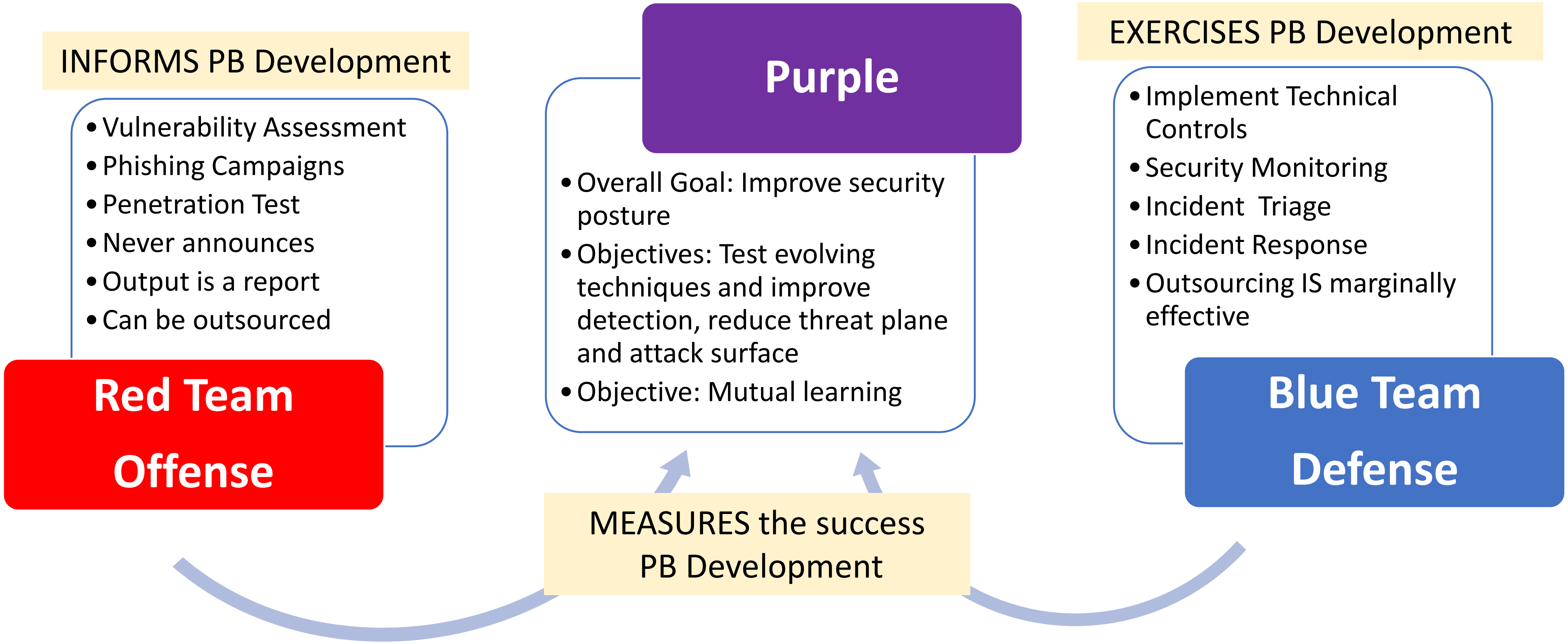


PB’s and IR (Adversary) Simulation

- **Adversary emulation** and **purple teaming** are fundamentally different activities.
  - In adversary emulation, a red team member conducts an assessment using only the techniques and tool types used by a specific adversary.
  - This differs from the more generic "threat emulation" red team where assessors use any tool or technique available to them.
- In **purple teaming**, the red team works hand in hand with the blue team to validate that their actions are detected.
  - If a particular action is not detected by the blue team, red team should repeat the action after the blue team adjusts instrumentation. Then lather, rinse, repeat

From Jake Williams, GSE

Where does the Playbook Apply?



INFORMS PB Development

- Vulnerability Assessment
- Phishing Campaigns
- Penetration Test
- Never announces
- Output is a report
- Can be outsourced

Red Team

Offense

Purple

- Overall Goal: Improve security posture
- Objectives: Test evolving techniques and improve detection, reduce threat plane and attack surface
- Objective: Mutual learning

EXERCISES PB Development

- Implement Technical Controls
- Security Monitoring
- Incident Triage
- Incident Response
- Outsourcing IS marginally effective

Blue Team

Defense

MEASURES the success
PB Development

Angst and Answers

- Technical accuracy
- Query issues
- Coverage issues
- Doc/Process quality issues
- What field again?
- Accuracy

- Peer review, dynamic refinement
- Peer review + cut/copy/paste
- Unit testing with outliers
- Ensure **fp** indicators discussed
- Include source data discussion
- Code based testing

PB Lifecycle: Design and CMS Process

Design

- Understand the Security Issue
- Review Data source & capability
- Map out detection capability

Develop

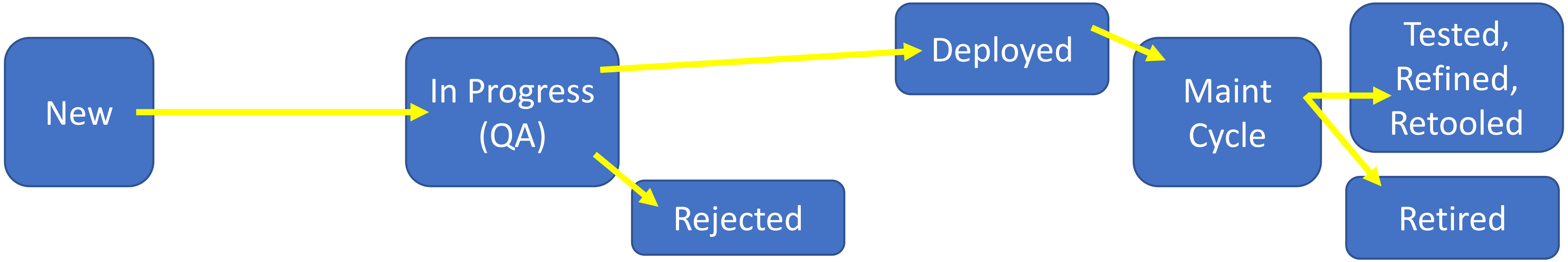
- Populate the template
- Develop a unit test
- Peer Review
- Formal QA
- Script the test harness
- "Subject Comms"

Run

- Train Team
- Link to PB from Security Platform
- Refine as needed
- Add link to SIEM Alert

Maintain

- Periodic Review (12-18 mo)
- Effectiveness?
- Retire?
- Validate?



Playbook Testing

- Each “period” – review a balanced set of prioritized playbooks
  - Define a subset exercise and peer review input/output/process
  - Remainders can be reviewed
- Key decisions to make
  - Keep: PB is good as it stands and the unit test functions
  - Update: PB is relevant, but needs a process/procedure/tech update
  - Retire: No longer relevant, technology no longer in use, business change
- Process
  - Test procedures by triggering the alert and work the steps through your process, update as necessary, and record results
  - Where possible, commit a test harness/script to Git
  - PB’s without a validation process require extra scrutiny

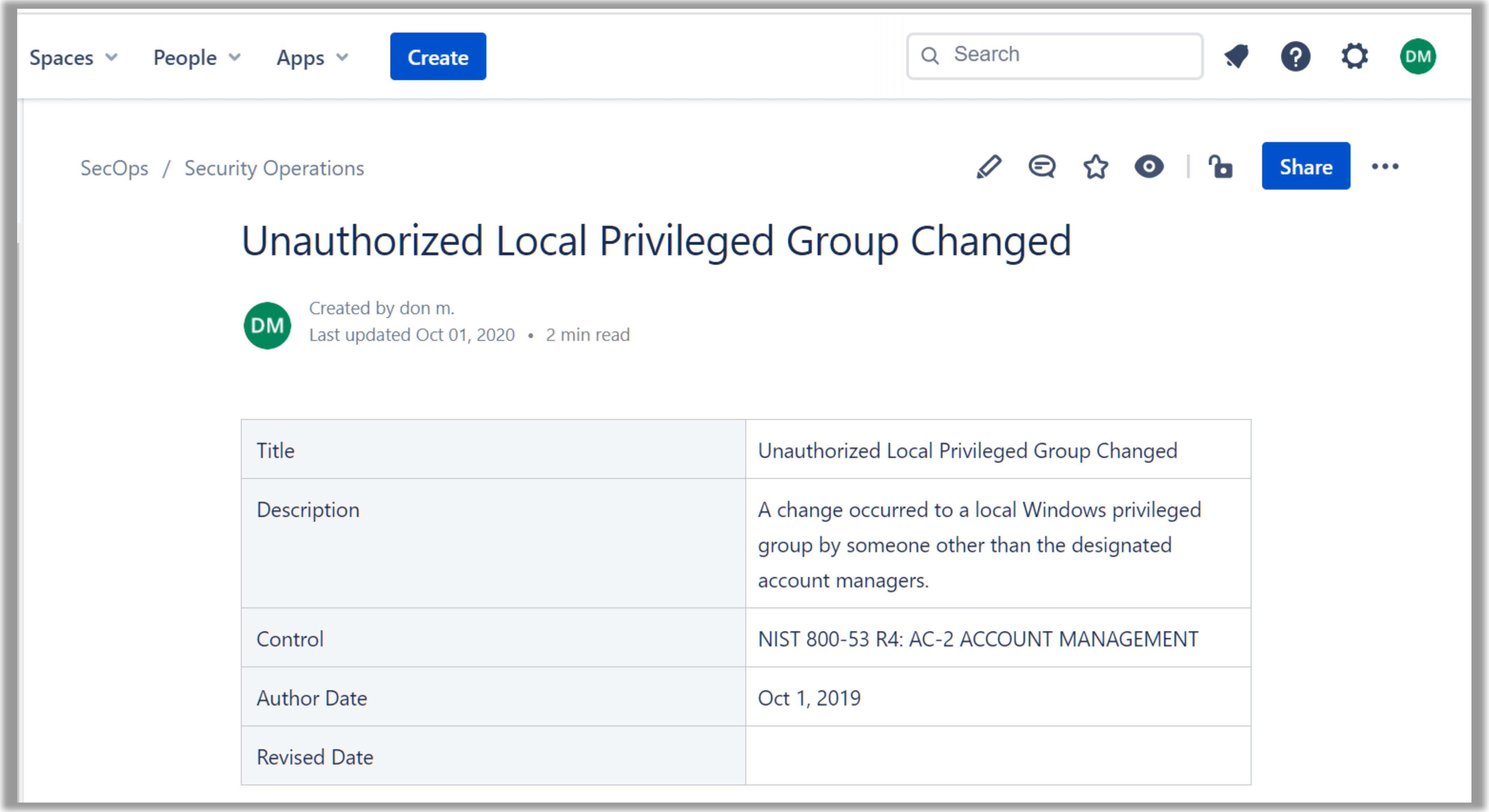
Metrics (Yes, We Love These …)

Measurement	Meaning	Examples/Notes
Security Program Coverage	Of the items in the ITGC/SP that can yield an alert, how many have Playbooks?	NIST 800-53 R4 = 159 controls. Most SIEM's cover 80 -98 w/ default content. Of this 56%, how many of them are functionally defined with a PB?
Data Sources with Playbooks	Percentage of data sources that have a general playbook	If your enterprise has 153 reporting systems, and 104 are supported by PB's, score is 68%
	How many of your alarms are supported by a playbook	If you have 453 alarms and 306 of them have a PB reference, score is 68%
Validation Testing	How many PB's are tested annually? Alarms?	If you have 80 PB's, and each are tested sometime within a 12 month period, 100%.
Never Used	How many alarms that cross index to a PB are *never run?*	Objective is to find PB's that either a) don't work or b) incorrectly configured
PB Quality	How many PB's require updates	Count how many PB's are refined/improved *before* the review cycle

ITGC/SP: Information Technology General Controls / Security Program

Confluence

- Add a sample template
  - Create Base Template
  - Add new docs based on the template
  - Add the “playbook” label
  - Create report based on page properties for type ‘playbook’
- A review process

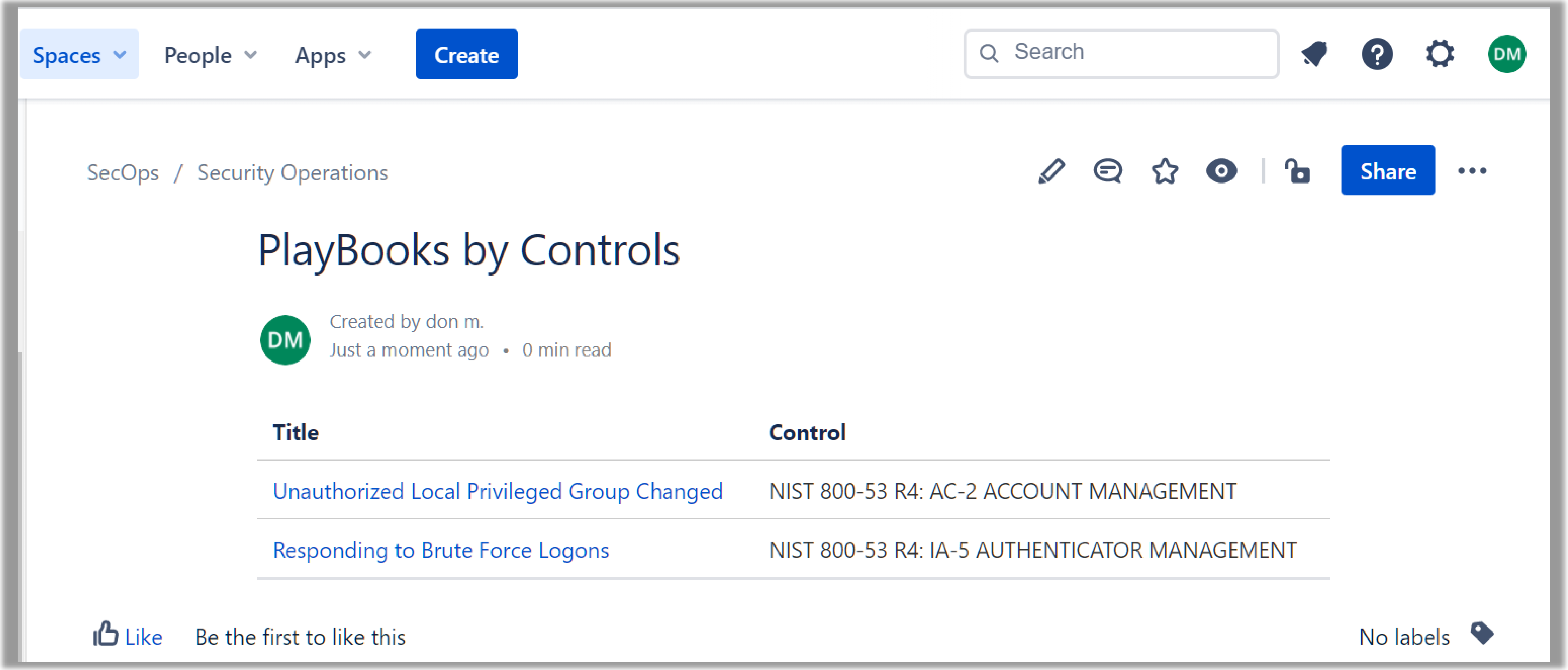


SecOps / Security Operations

Unauthorized Local Privileged Group Changed

Created by don m.
Last updated Oct 01, 2020 • 2 min read

Title	Unauthorized Local Privileged Group Changed
Description	A change occurred to a local Windows privileged group by someone other than the designated account managers.
Control	NIST 800-53 R4: AC-2 ACCOUNT MANAGEMENT
Author Date	Oct 1, 2019
Revised Date	



SecOps / Security Operations

PlayBooks by Controls

Created by don m.
Just a moment ago • 0 min read

Title	Control
Unauthorized Local Privileged Group Changed	NIST 800-53 R4: AC-2 ACCOUNT MANAGEMENT
Responding to Brute Force Logons	NIST 800-53 R4: IA-5 AUTHENTICATOR MANAGEMENT

Like Be the first to like this

No labels