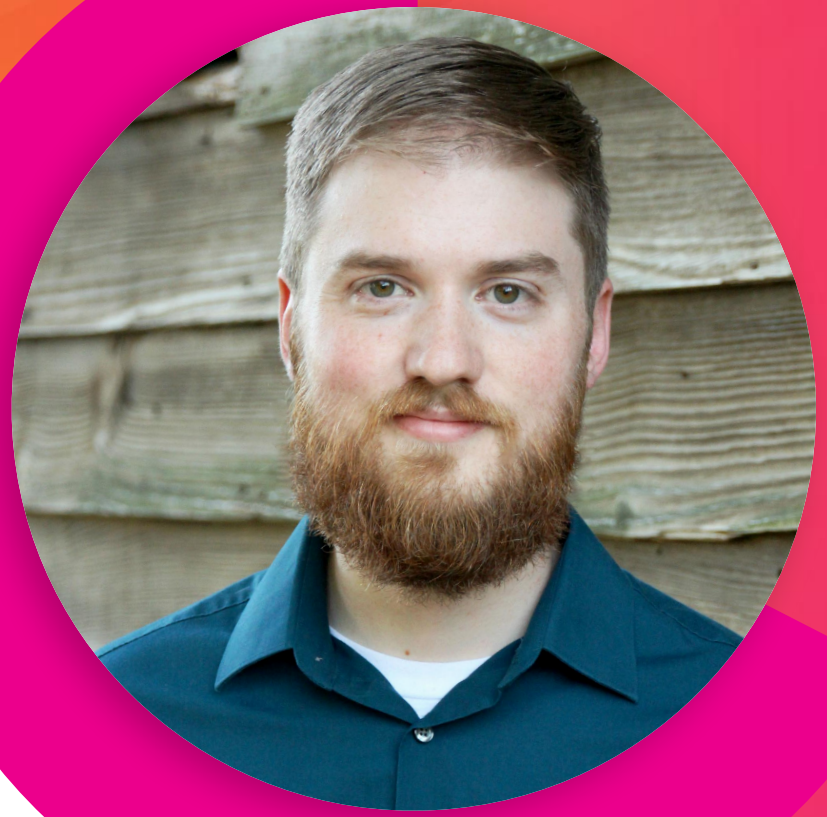
Building Automated Decisions for Incident Response with Phantom

by Mark Cooke, General Electric

October 2019 | Version 2.0



Building Automated Decisions for Incident Response with Phantom

Mark Cooke
Staff Incident Responder | General Electric

splunk> .conf19

General Electric

Imagination at Work

+300K

+300K

1

24/7

50

3

Goals for Automation

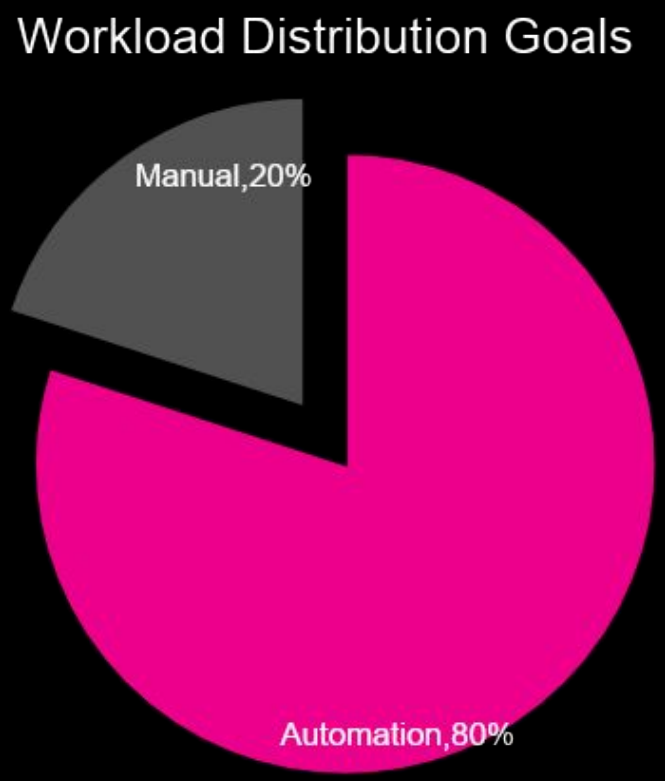
Team Goals & Outcomes

.conf19

splunk>

Goals for Automation

Team Goals & Outcomes



- Broader coverage
- Maintainable workload

- Focused analysts
- Proactive response team

Foundation for Automation

Design, Phases, Examples, Results

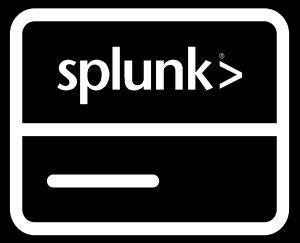
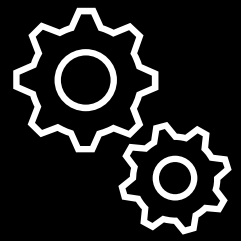
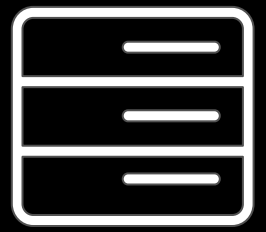
.conf19

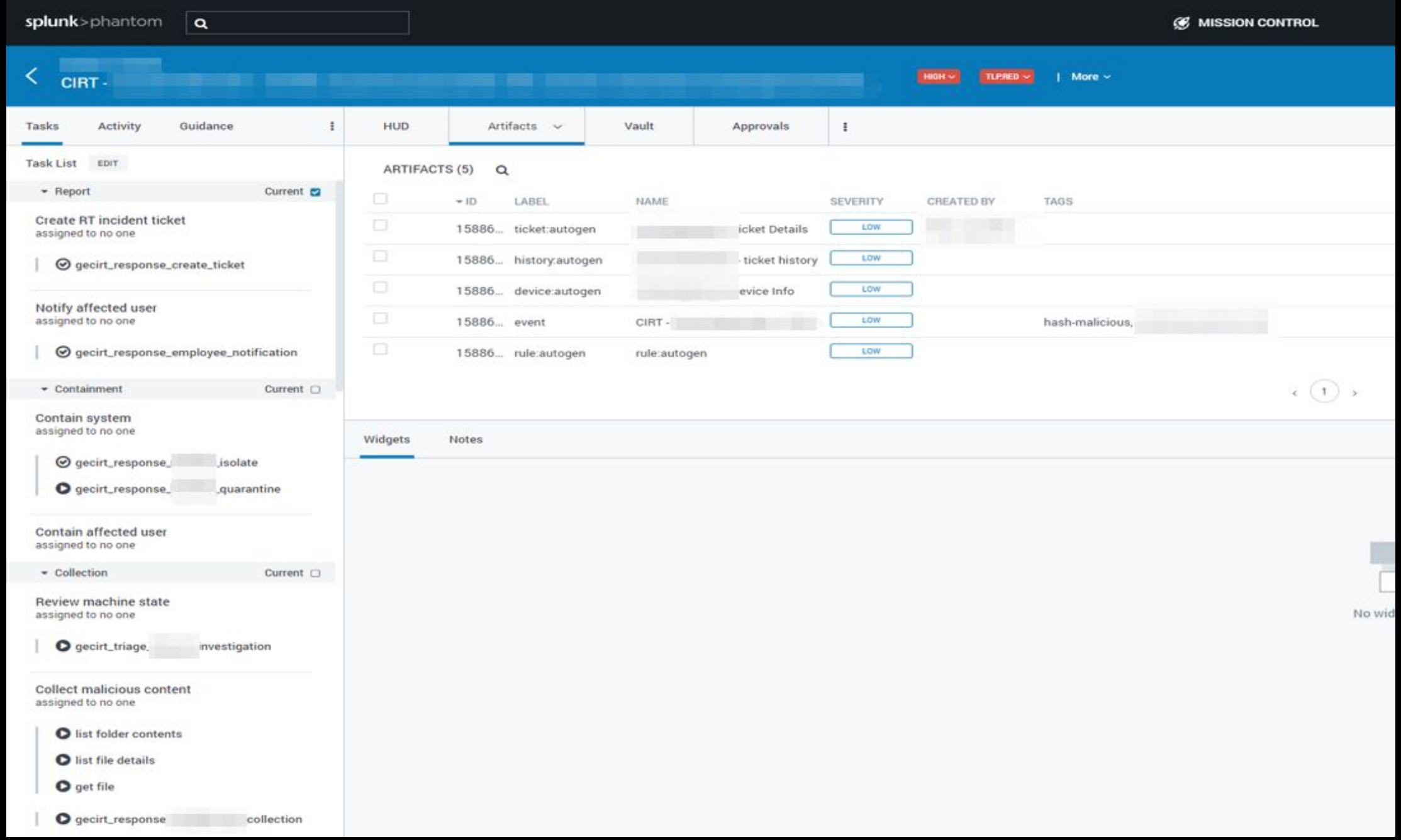
splunk>

Foundation for Automation

Automation Design & Phases

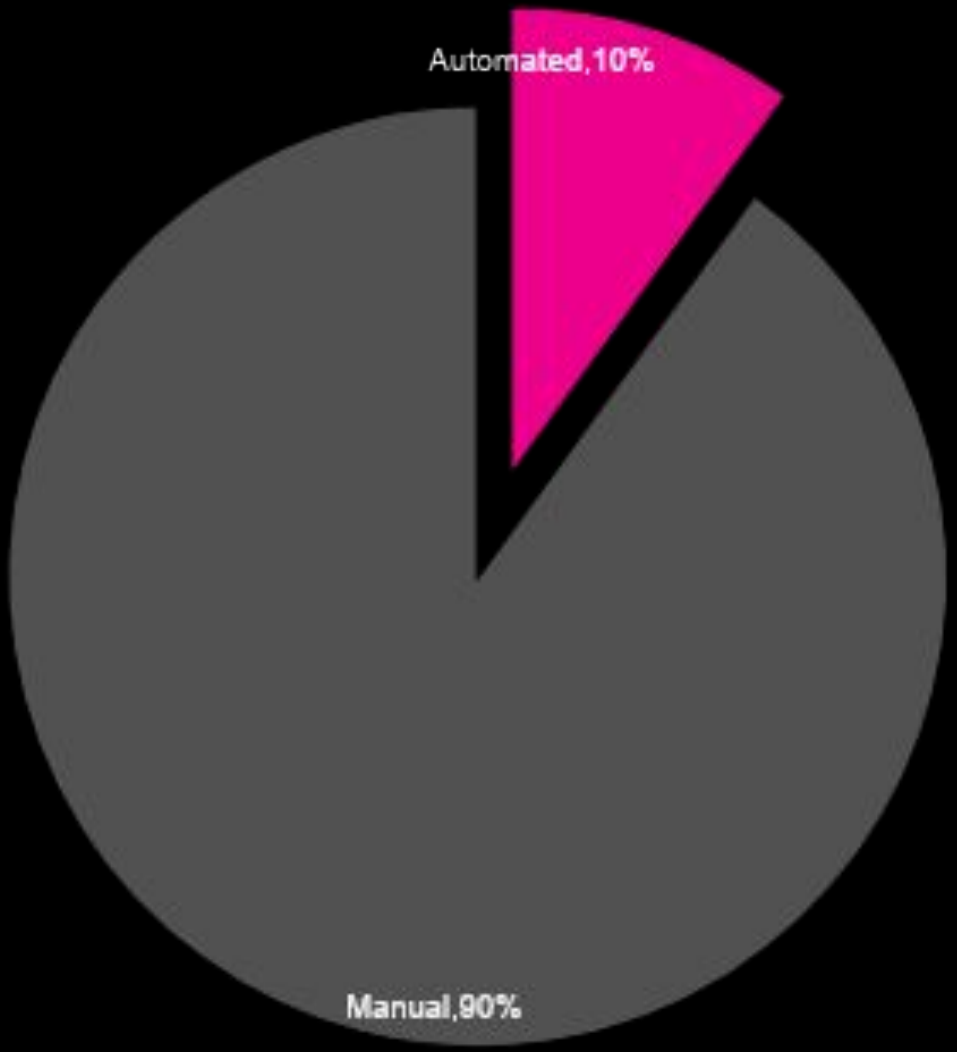
Phantom

Ingestion	Enrichment	Triage	Response
			
• Detection • Forward	• Enrichment	• Triage • Analysis	• Reaction


splunk>phantom
MISSION CONTROL
CIRT -
HIGH
TLP:RED
More
Tasks
Activity
Guidance
HUD
Artifacts
Vault
Approvals
Task List
EDIT
Report
Current
Create RT incident ticket
assigned to no one
gecirt_response_create_ticket
Notify affected user
assigned to no one
gecirt_response_employee_notification
Containment
Current
Contain system
assigned to no one
gecirt_response_ isolate
gecirt_response_ quarantine
Contain affected user
assigned to no one
Collection
Current
Review machine state
assigned to no one
gecirt_triage_ investigation
Collect malicious content
assigned to no one
list folder contents
list file details
get file
gecirt_response collection
ARTIFACTS (5)
ID
LABEL
NAME
SEVERITY
CREATED BY
TAGS
15886... ticket:autogen icket Details LOW
15886... history:autogen - ticket history LOW
15886... device:autogen evice Info LOW
15886... event CIRT - LOW hash-malicious,
15886... rule:autogen rule:autogen LOW
Widgets
Notes
No wid

Foundation for Automation

Workload Distribution – After a Year



Building Automated Decisions

Requirements, Collecting Data, Decision Components, Processing Decisions, & Integration

.conf19

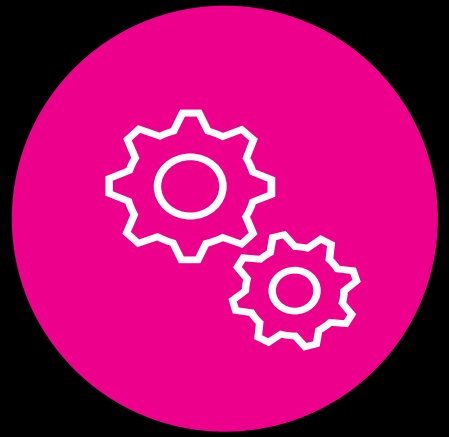
splunk>

Need for Automated Decisions

Requirements

Capture Data

Team Collaboration

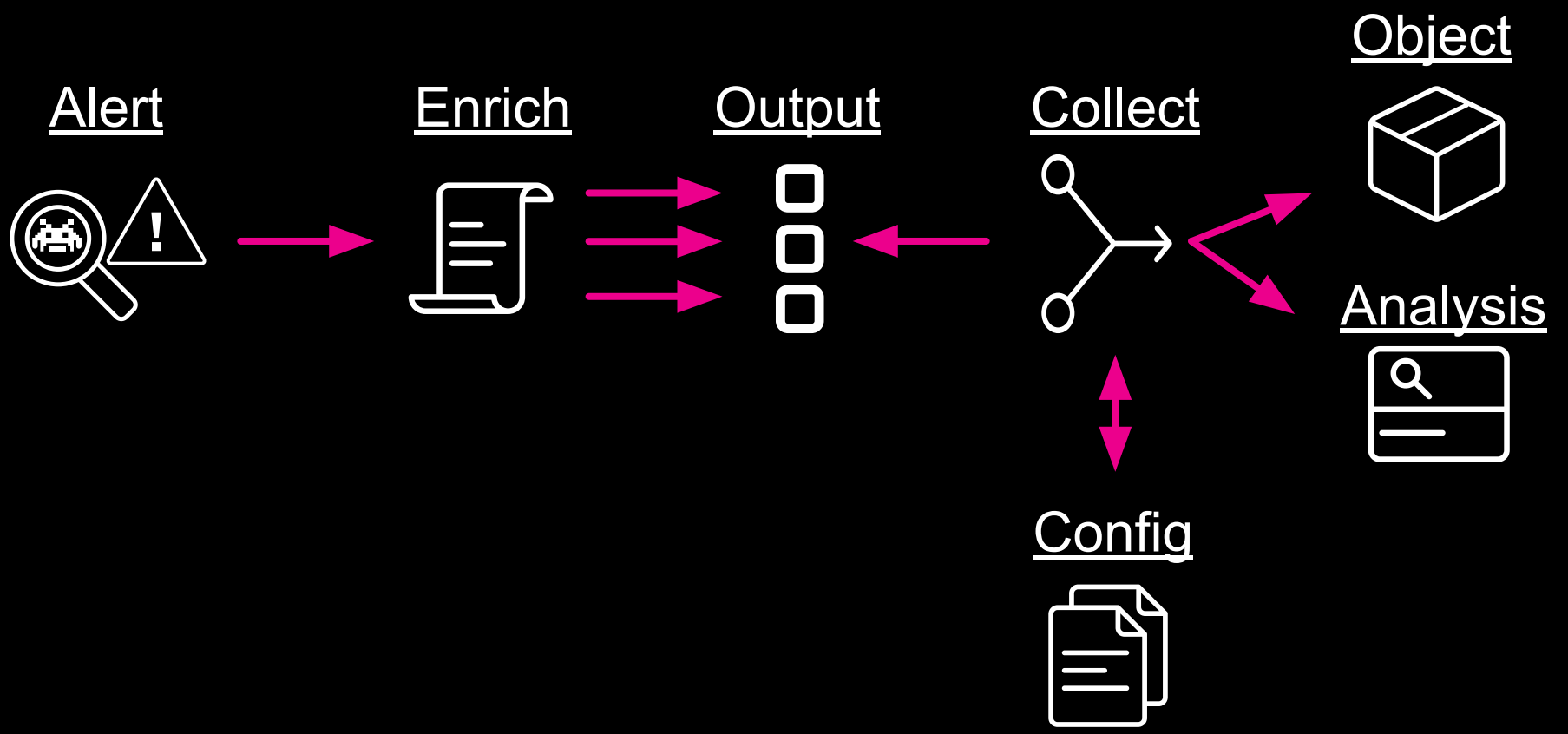


Separate Logic

Common Syntax

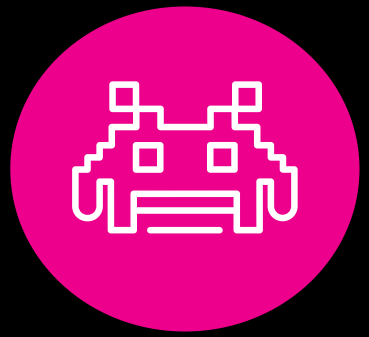
Building Automated Decisions

Collecting Data - Phantom



Building Automated Decisions

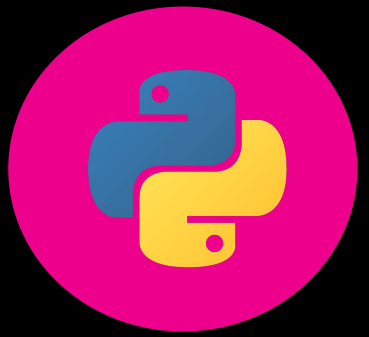
Decisions Components - Capturing Conditions



- Malware analysis

- Pattern matching

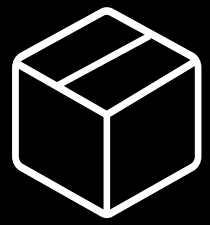
- Analyst friendly



- Python integrated

Building Automated Decisions

Decision Components



1

```
{
   "alertName": "confExample",
   "hostname" : "exampleHost",
    …
}
```

2

```
rule confExample
{
   condition:
    alertName = "confExample"
}
```

3

```
rule confExample
{
   condition:
    "confExample" = "confExample"
}
```

Building Automated Decisions

Decision Components - Reactions

```
rule confExample
{
    meta:
    author =  "mcooke"
    created = "2019-10-21"
    expires = "2020-10-20"
    category = "response"
    playbook = "contain_host_playbook"
    parameter = "automation"
    condition:
     alertName = "conf19"
}
```

Metadata

Reaction

Conditions

Container Data Variable

Response Categories

- Contain
- Prioritize
- Suppress
- Notify
- Escalate

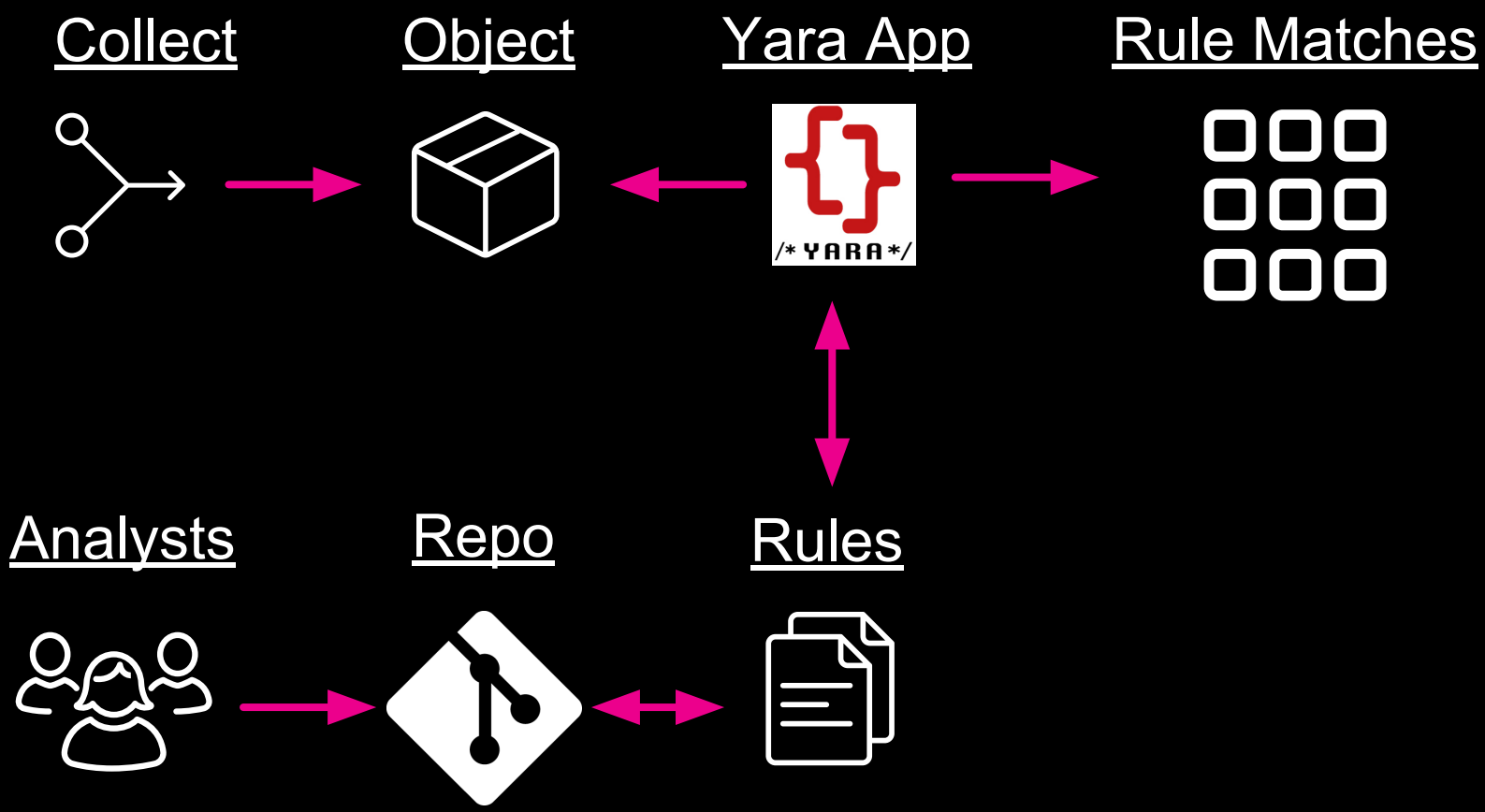
Building Automated Decisions


```
"status": "success",
"parameter": {
    "external_variables": "{\"alertName\": \"conf19\"}",
    "data": "dummy_data",
},
"message": "1 matches",
"data": [{
        "matches": [{
                "meta": {
                    "author": "mcooke"
                    "created": "2019-10-21",
                    "expires": "2020-10-20"
                    "type": "contain",
                    "response": "contain_host_playbook"
                    "reason": "I needed an example for .conf!",
                    "parameter": "automation"
                },
                "namespace": "/path/yara_rules/confExample.yar",
                "strings": [],
                "rule": "confExample",
                "tags": []
            }
        ],
        "errors": [{
    }
],
"summary": {
    "rules": ["confExample"],
    "matches": 1
}
```


splunk> .conf19

Building Automated Decisions

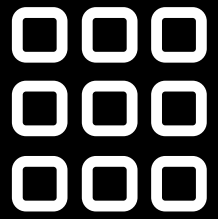
Processing - Matches



Building Automated Decisions

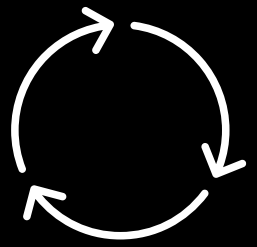
Processing - Actions

Rule Matches



- Extract metadata

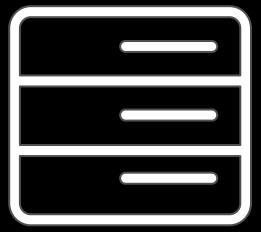
Process



- Dedupe
- Prioritize
- Control flow

React

Alert Queue

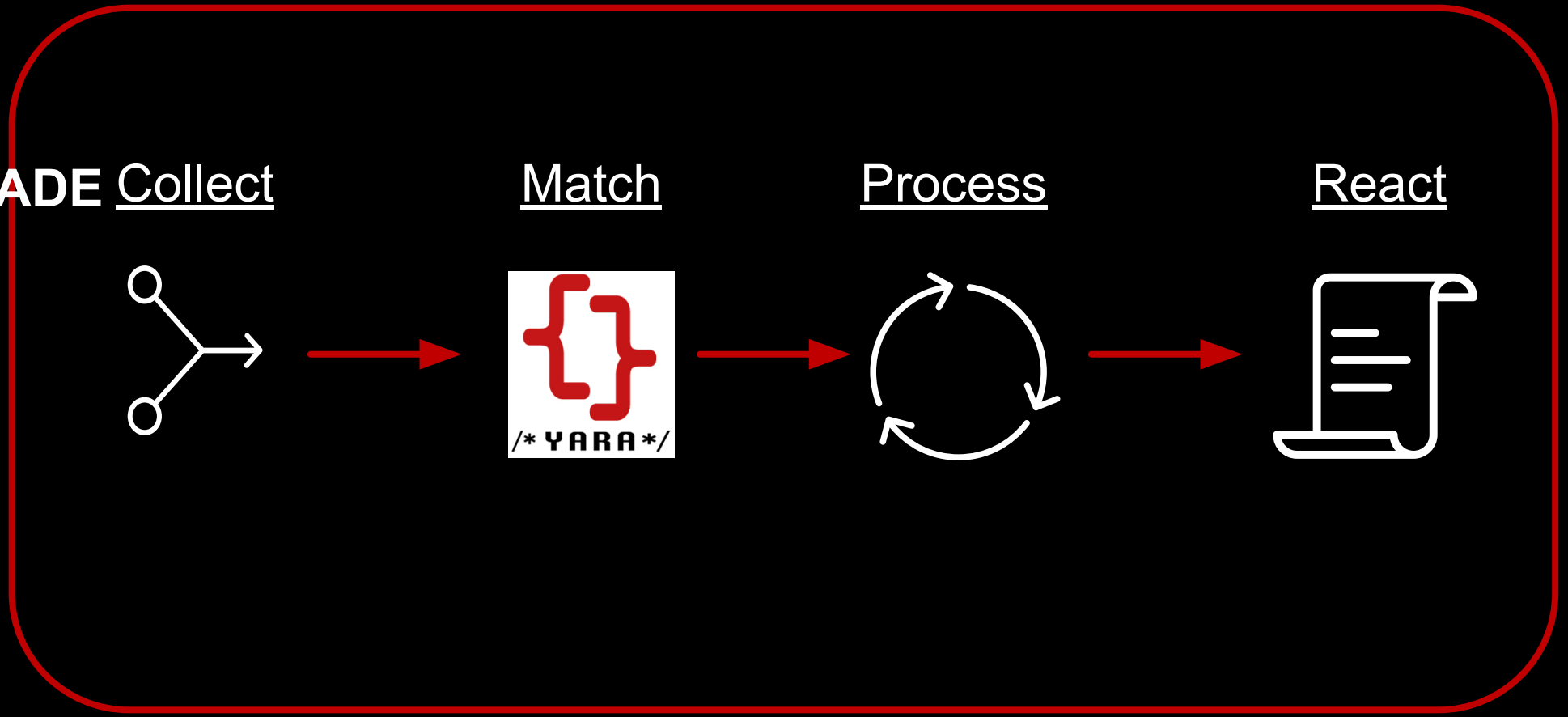


- Display
- Inform

Building Automated Decisions

Integration – Overall Decision Phase

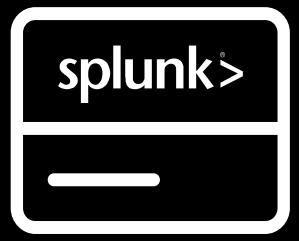
PHantom **A**utomated **D**ecision **E**ngine



Building Automated Decisions

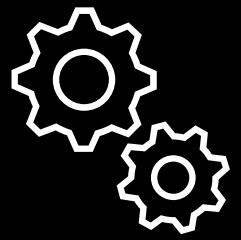
Integration – Overall Automation Phases

Ingestion



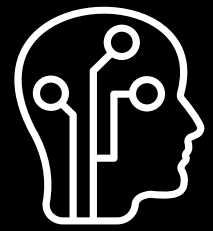
- Detection
- Forward

Enrichment



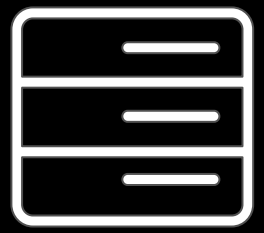
- Enrichment

Decision



- Filter
- React
- Control

Triage



- Triage
- Analysis

Response

- Reaction

Use Cases for Automated Decisions

Suppression, Prioritization, & Others

.conf19

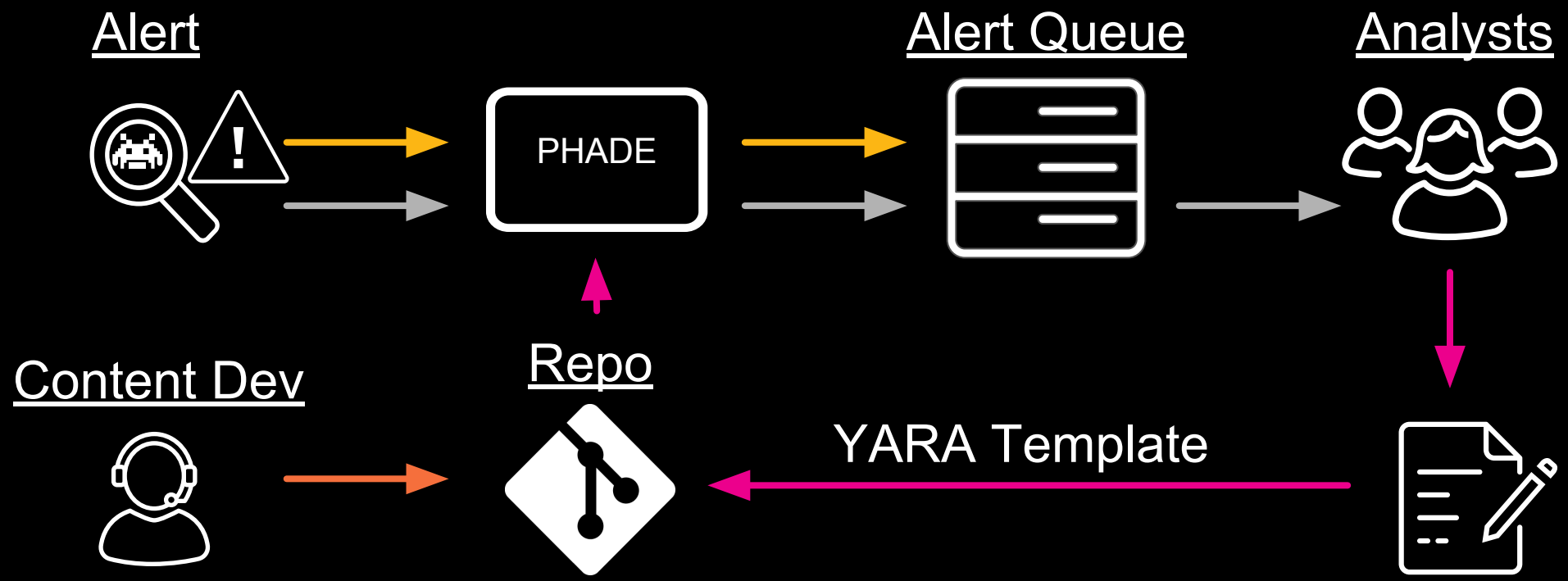
splunk>

Use Cases for Automated Decisions

Alert Suppression - Process

Goals

- React to false positive alerts
- Filter rules on enriched data
- Filter conditions across multiple rules

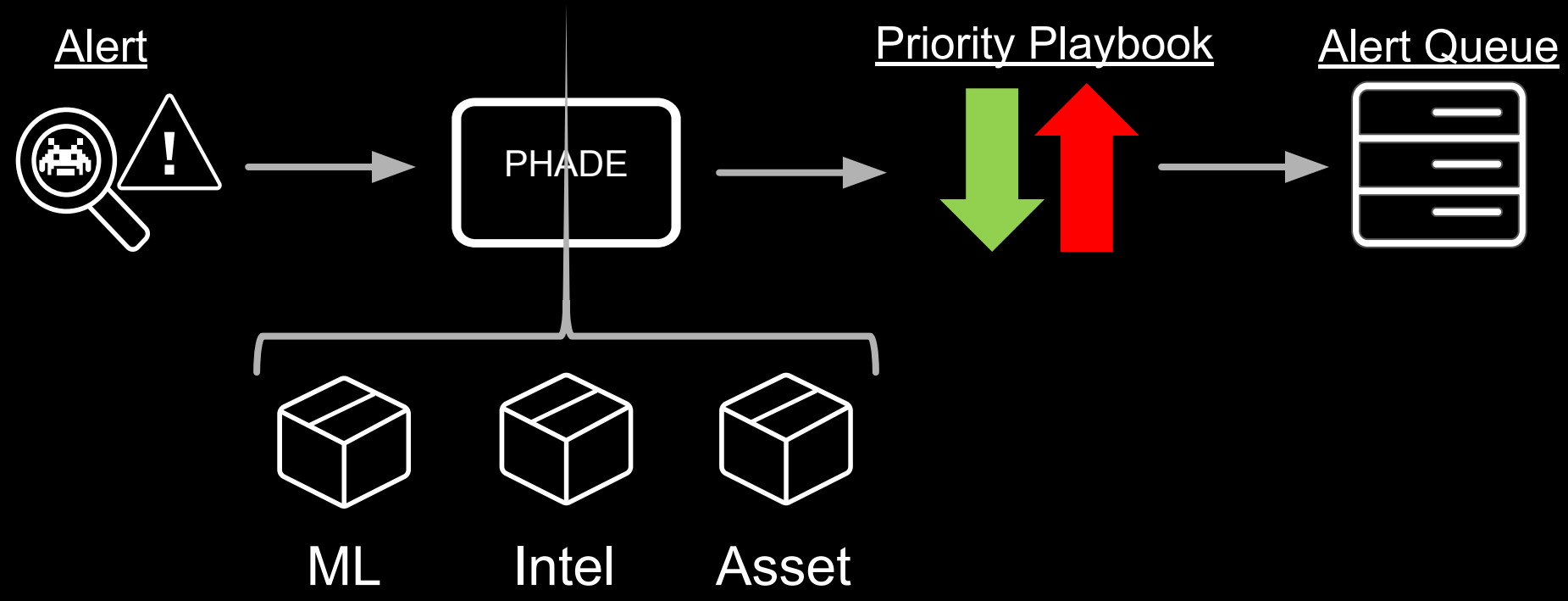


Use Cases for Automated Decisions

Alert Prioritization

Goals

- Dynamic alert priorities
- Change priority based on context



Results of Automated Decisions

Automation by the Numbers

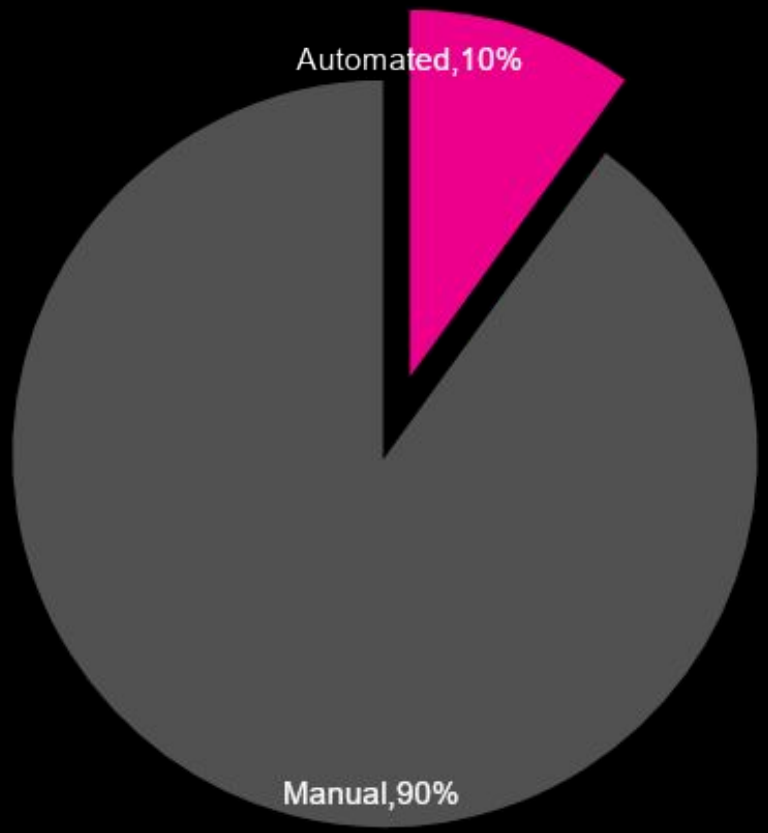
.conf19

splunk>

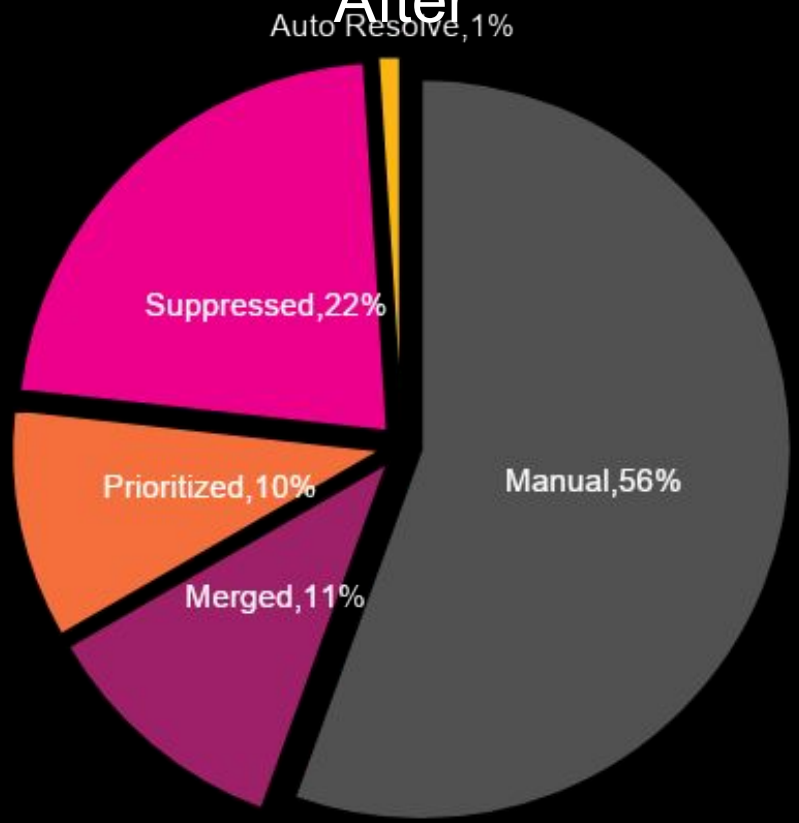
Automation Results

Automation by the Numbers

Before



After



Key Takeaways

Lessons learned

.conf19

splunk>

Key Takeaways

Lessons Learned

- Have a goal & measure it
- Think about collecting data
  - Machine vs Analyst
  - Code vs Analysis
- Separate decision logic from code
  - Contributors
  - Flexibility
- Start with simple decisions
  - Many iterations
  - Continue improving

splunk>

Thank You!