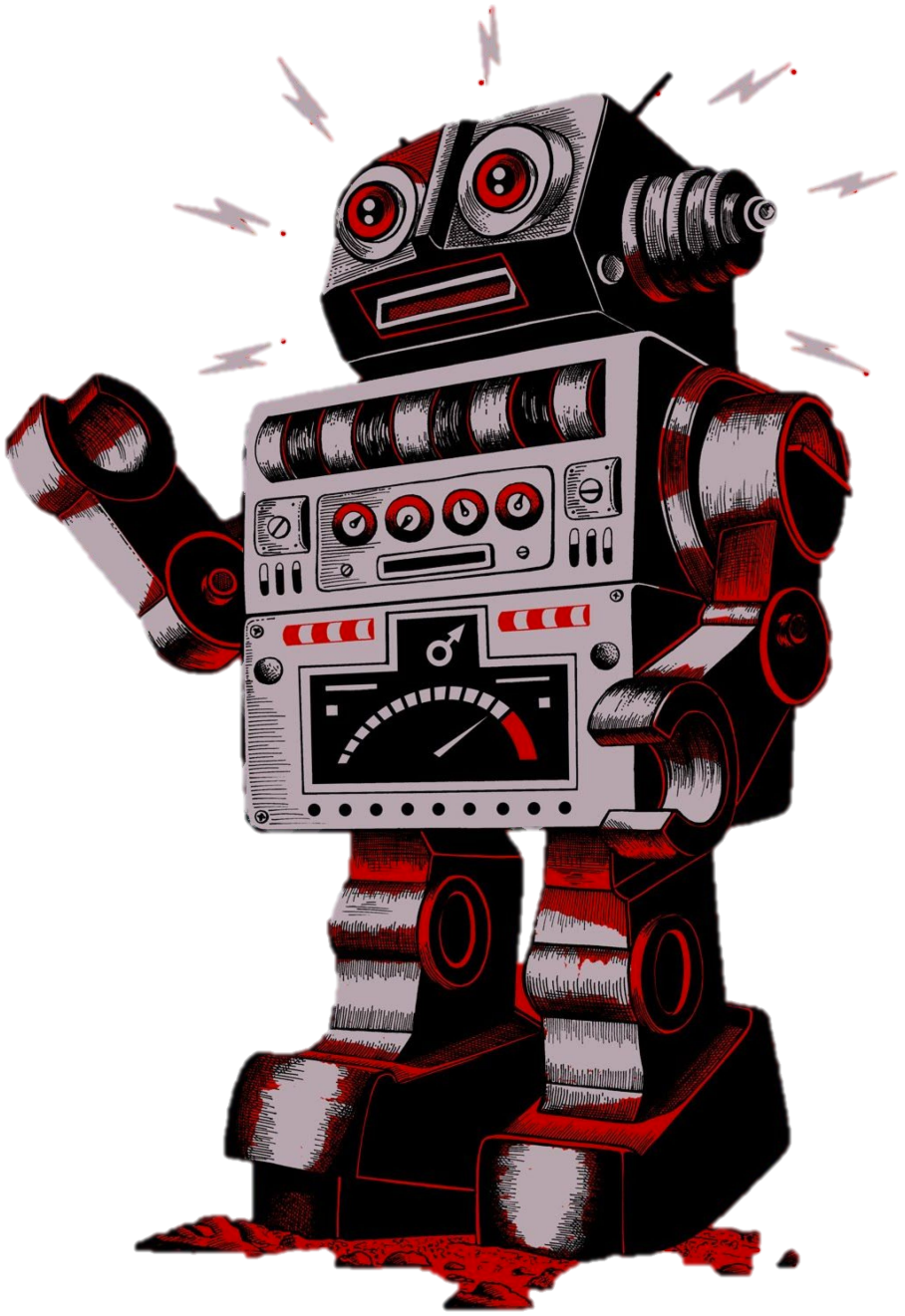
# Automating Analysis Without Automating the Analyst

Mark Orlando
Brandon Denker



BSIDES WASHINGTON D.C.

# Who We Are

## Mark Orlando

18 years in cyber operations

Managed services, consulting, strategy, automation

Founder & CEO, Bionic

## Brandon Denker

12 years in cyber operations

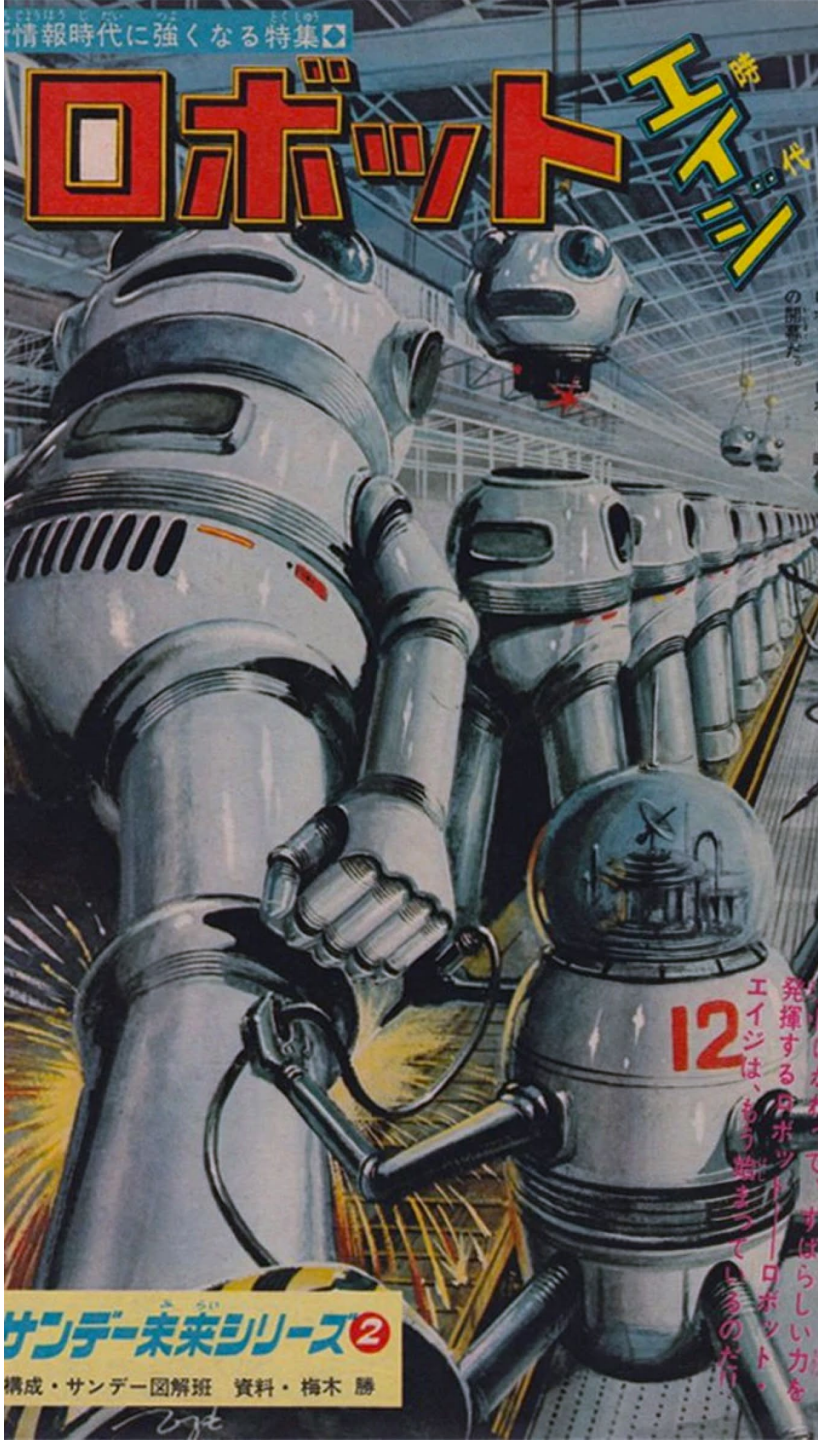
Threat hunting, malware analysis, forensics, SOC automation

Researcher, Cyborg Security

# The Automation Imperative

"Collect everything and figure it out later" was the rallying cry of many SOCs in the 2000's

Everything is electronic now -> more discrete and diverse devices than ever, leading to more data than ever



# The Automation Imperative

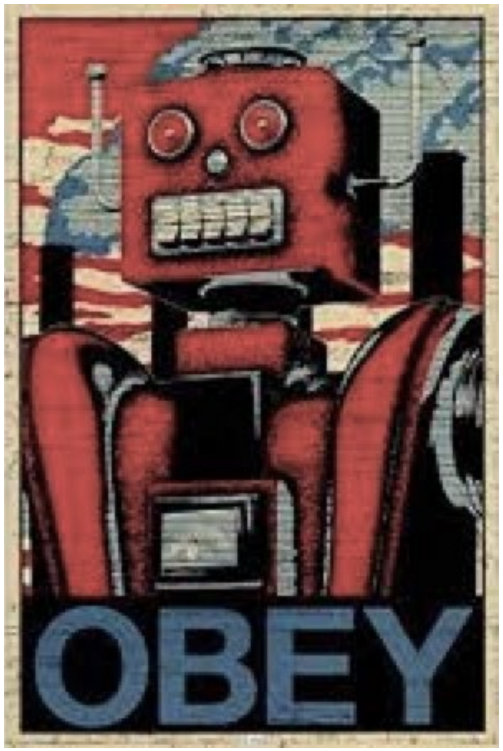
# Aren't We Automating Already?

"Heavy investments in technology have delivered disappointing results [in boosting performance] – largely because companies tend to use technology to mechanize old ways of doing business…speeding up those processes cannot address their fundamental performance deficiencies."

- Michael Hammer, *Harvard Business Review*

# Not All Automation is Equal

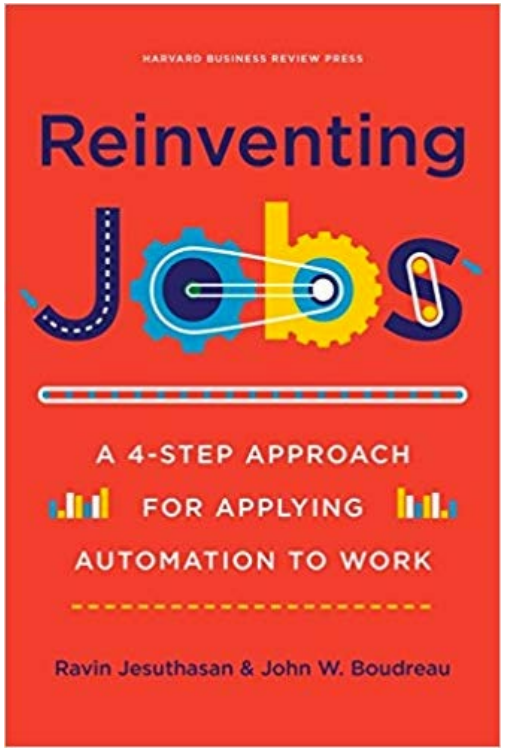
- Automating some tasks will reduce risk (correlation rule)
- Automating others will increase quality (report generation)
- Still others will reduce variance without adding any value (100% alert accountability)



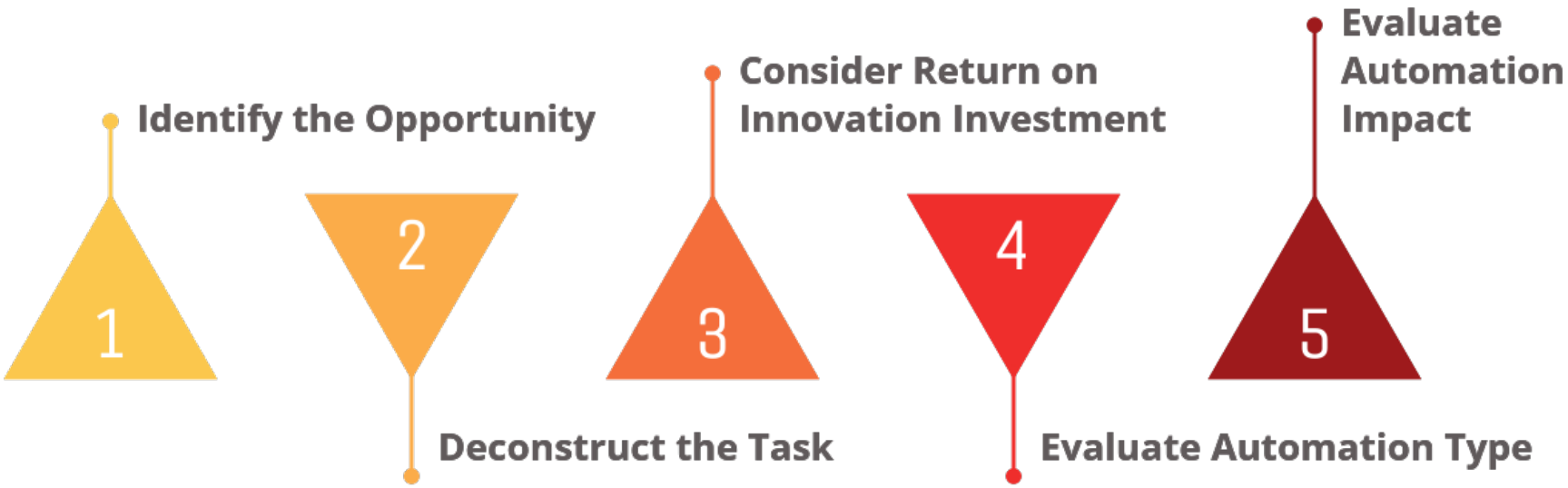

All “improvements” are not equally valuable!

# Reference Material

**Reinventing Jobs: A 4-Step Approach for Applying Automation to Work**, by Ravin Jesuthasan and John Boudreau



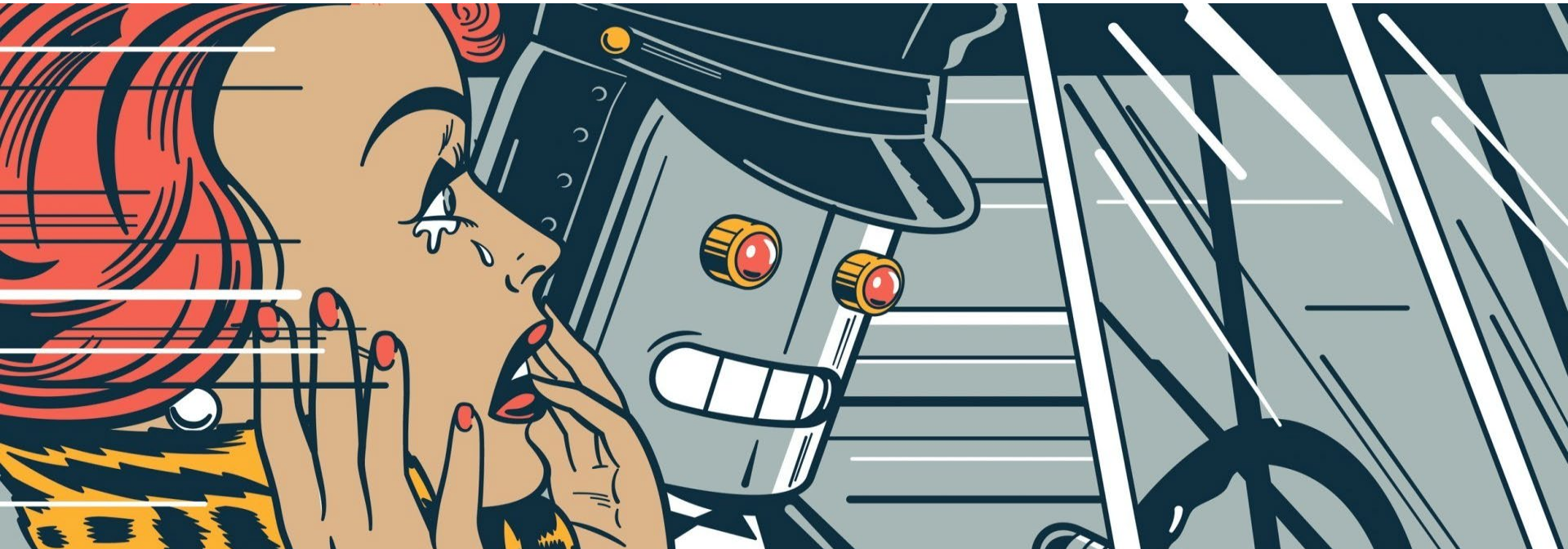
# Five Step Approach




*Desired result: Measurable Improvement*

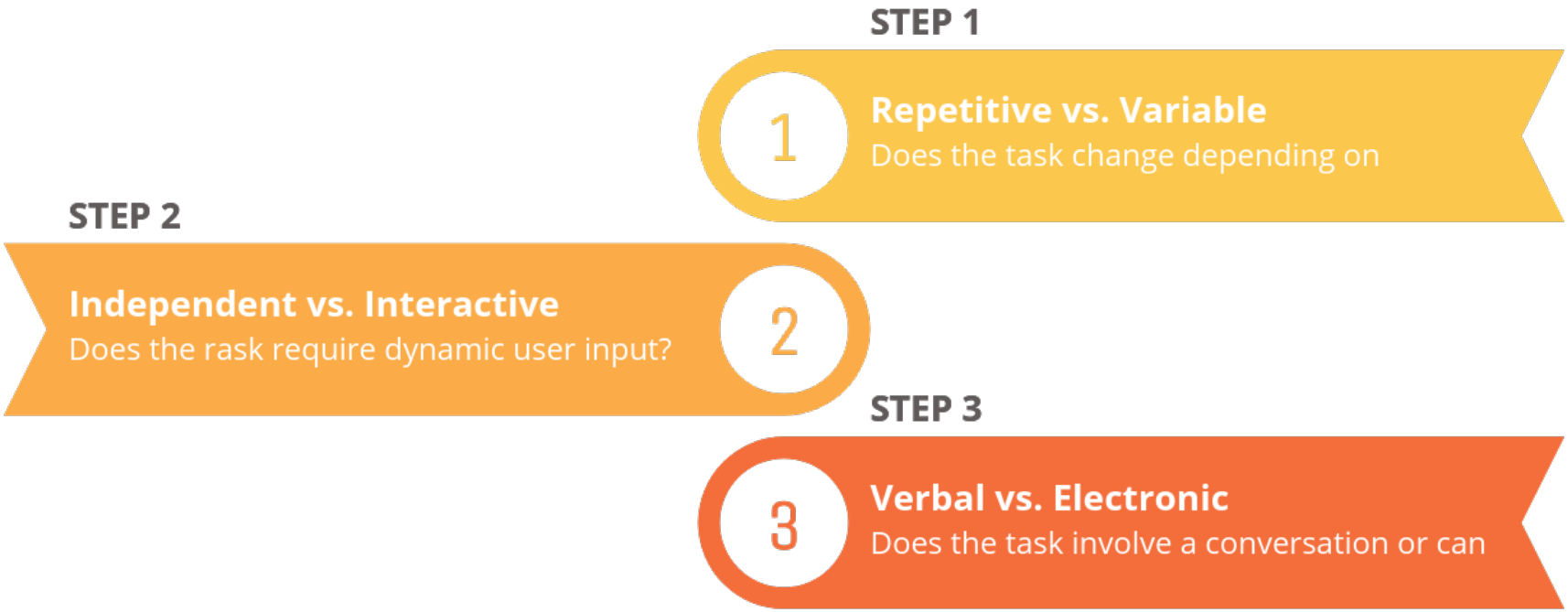
# Can’t We Just, You Know, Do It?

- “Micro-automation” doesn’t require a five step process
- Larger initiatives, advent of AI/ML require more deliberate analysis and planning

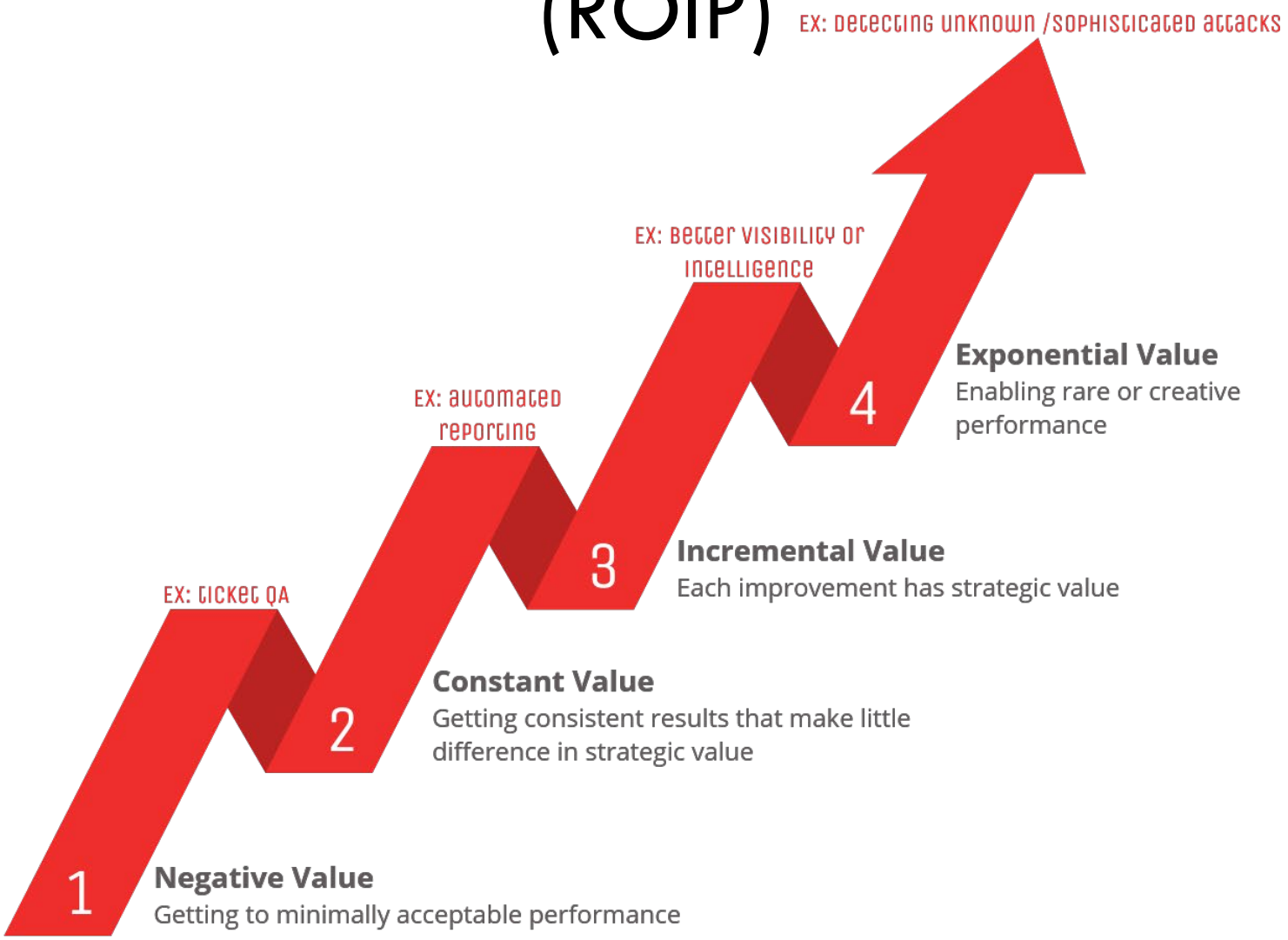


# Identify the Opportunity

# Deconstruct the Task

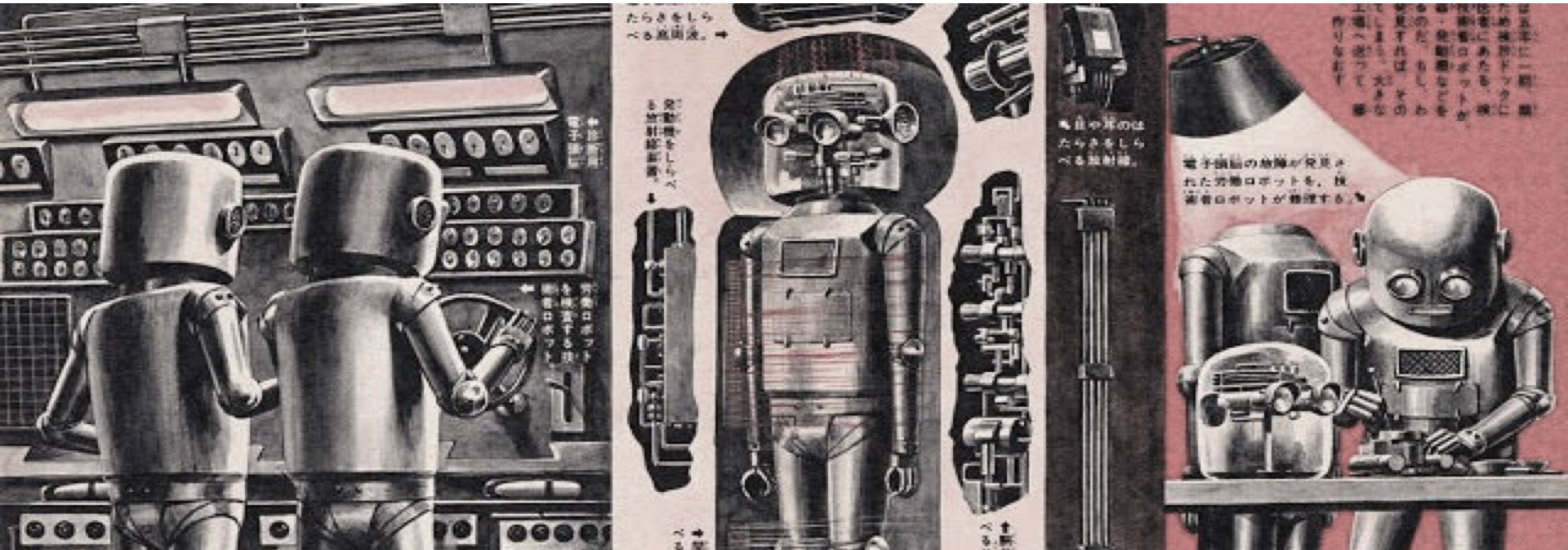


# Return on Improved Performance (ROIP)



# Evaluate Automation Type

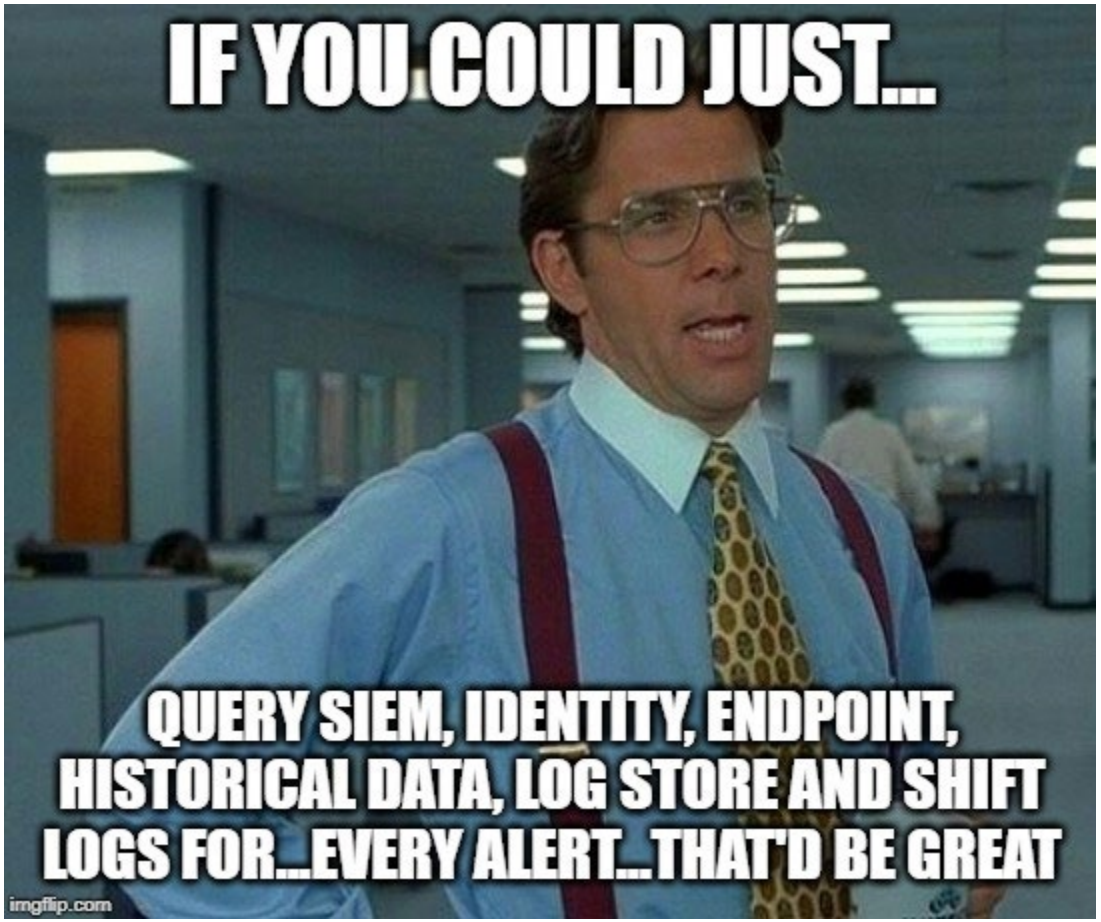
1. Robotic process automation***
2. Cognitive automation
3. Collaborative/social robotics



# Impact of Automation

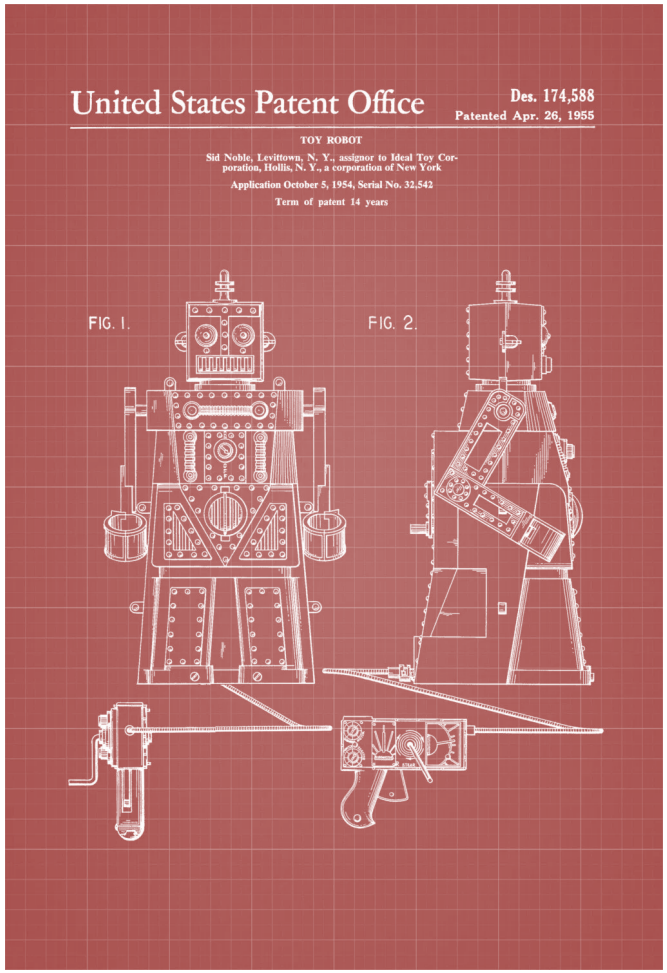
- Substitute for something a human does
- Augment what a human does
- Create new/value-added work not being done today, or previously impossible without automation

# Case Study: Alert Context

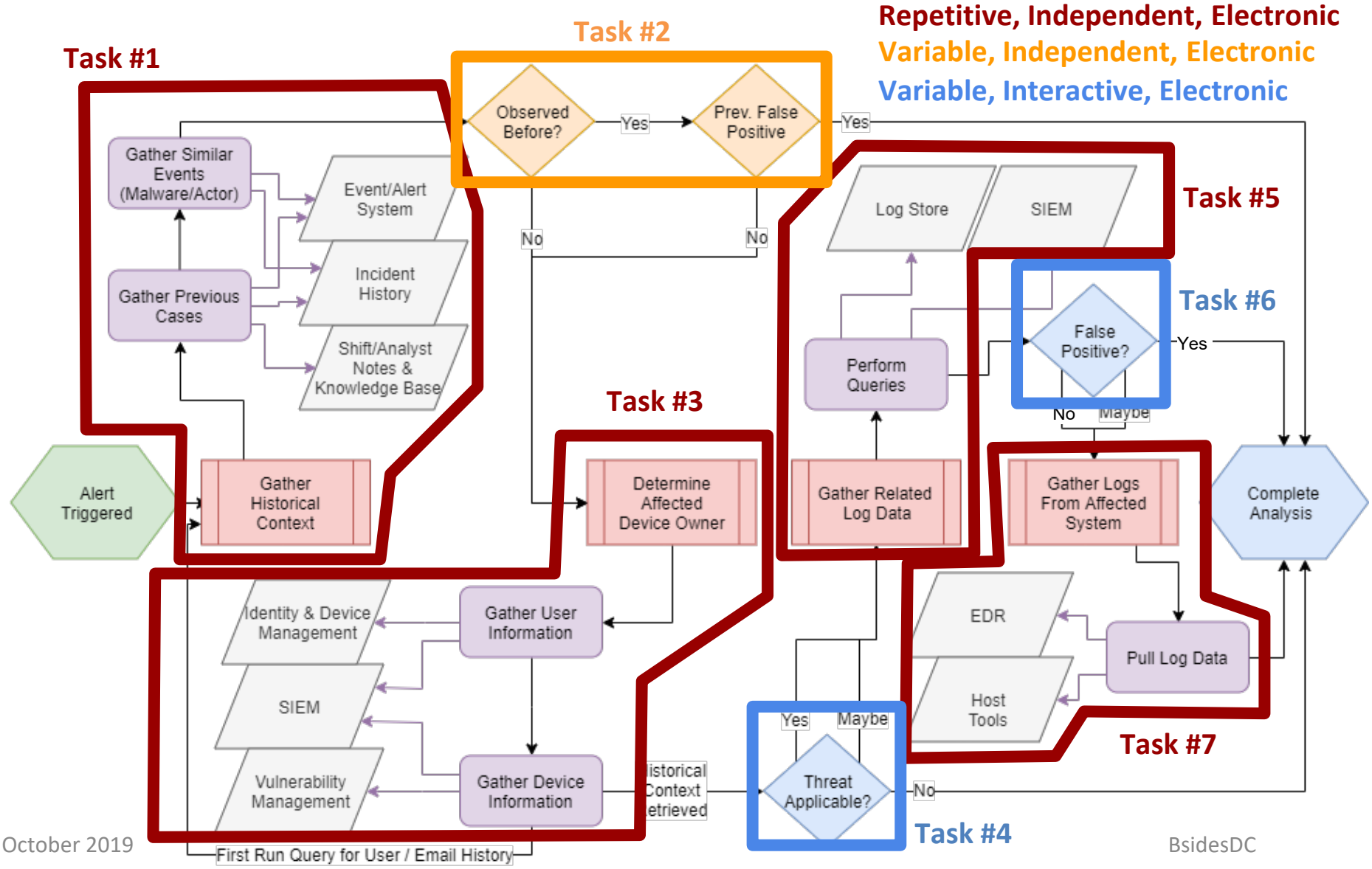


# Alert Context: Identify the Opportunity

- What is it?
  - Gathering related details
    - Historical context
    - Identity context
    - Related events & alerts
- Why Analysts Want it Automated?
  - Common first step in analysis
  - Tedious and Time consuming
  - Similar steps carried out for each alert



# Alert Context: Deconstruct the Task



# Alert Context: Deconstruct the Task

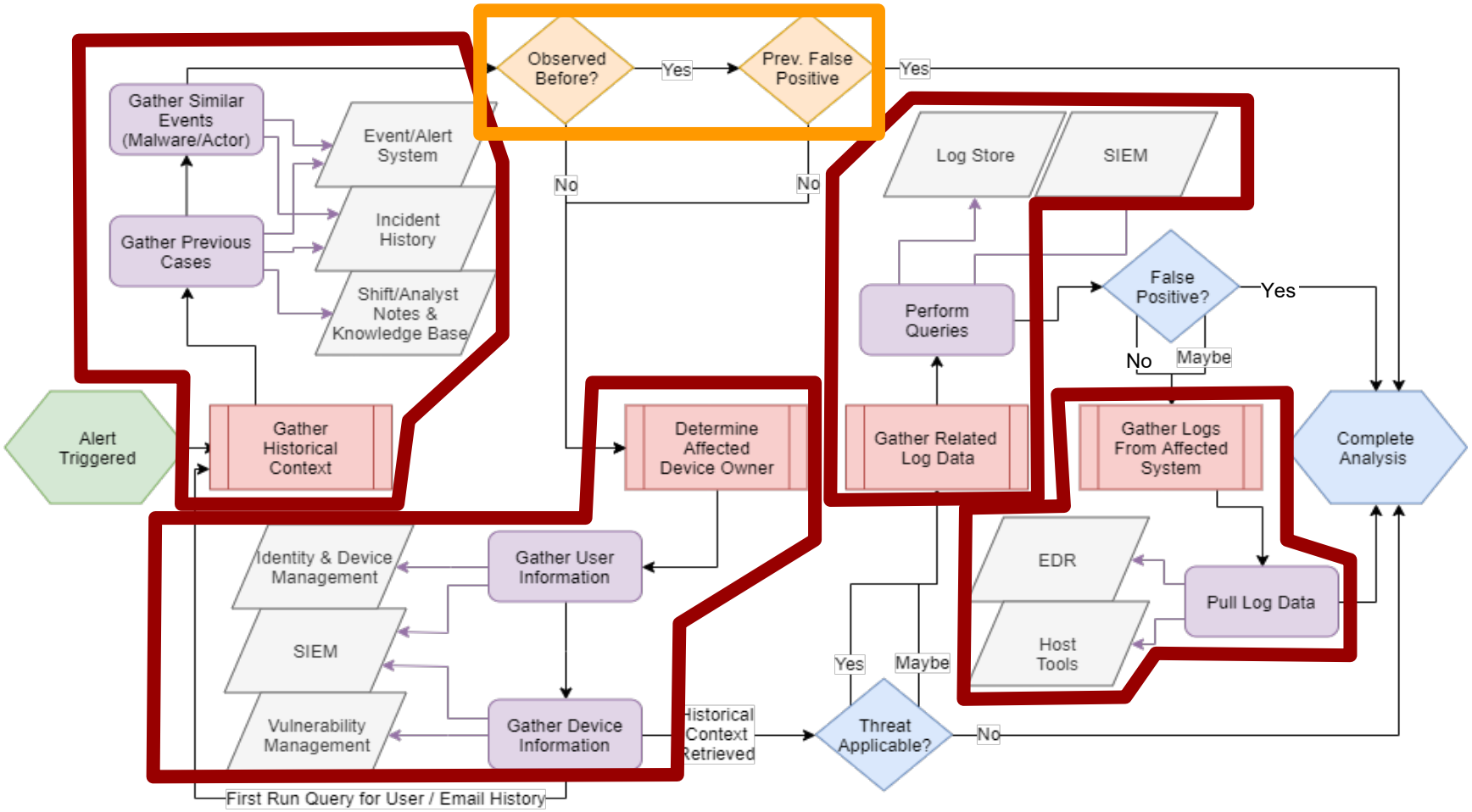
| | Intent | Benefit | Dependency | Difficulty & ROIP |
|---|---|---|---|---|
| **Task #1 Historical Context** | • Learn from our past<br>• Deduplicating effort<br>• Gather related alerts, events, incidents and notes | • More timely analysis and response<br>• Reduce unnecessary data collection<br>• Reduce duplicate effort | • Tool API Access | Moderate Difficulty<br>Incremental value |
| **Task #2 Observed Before?** | • More quickly identify repeat activity<br>• Determine if further data collection is needed | • More efficient alert processing<br>• Reduce duplicate effort | • Task #1 | Low Difficulty<br>Constant value |
| **Task #3 Device Identity** | • Context for threat applicability<br>• Gather who and what to aid response | • Simplify multi-tool data gathering<br>• Potential for more timely response | • Tool API Access | High Difficulty<br>Incremental value |
| **Task #4 Threat Applicable?** | • Human decision point<br>• Determine if further data collection is needed | • Potential for more timely response<br>• Minimize unnecessary effort | • Task #3 | Human Breakpoint<br>Negative Value |
| **Task #5 Gather Log Data** | • Locate supplemental and related data<br>• Provide context as to when, why and how | • Improved analysis efficiency<br>• Consistent data set for analysis<br>• Potential for more timely response | • Tool API Access | Low Difficult<br>Incremental value |
| **Task #6 False Positive?** | • Determine if further data collection is needed | • Minimize unnecessary data gathering | • Task #3 or Task #5<br>• Sufficient context for analysis | Human Breakpoint<br>Negative Value |
| **Task #7 Gather Data from Host** | • Gather deeper context for analysis<br>• Gather data not available in logs | • More complete context | • Endpoint tool or ability to gather data via script/tools | High Difficulty<br>Incremental value |

# Alert Context: Return on Improved Performance

- Where do we start?
  - Historical Context (#1)
  - Device Identity (#3)
  - Gather Log Data (#5)
  - Observed Before? (#2)
  - Gather Host Data (#7)

- Incremental value
  - Every improvement adds strategic value
- Constant value
  - Every improvement adds some value, not necessarily strategic
- Negative value
  - Improvements only add so much value – ex. You can improve your ability to spot false positives, but no value beyond that

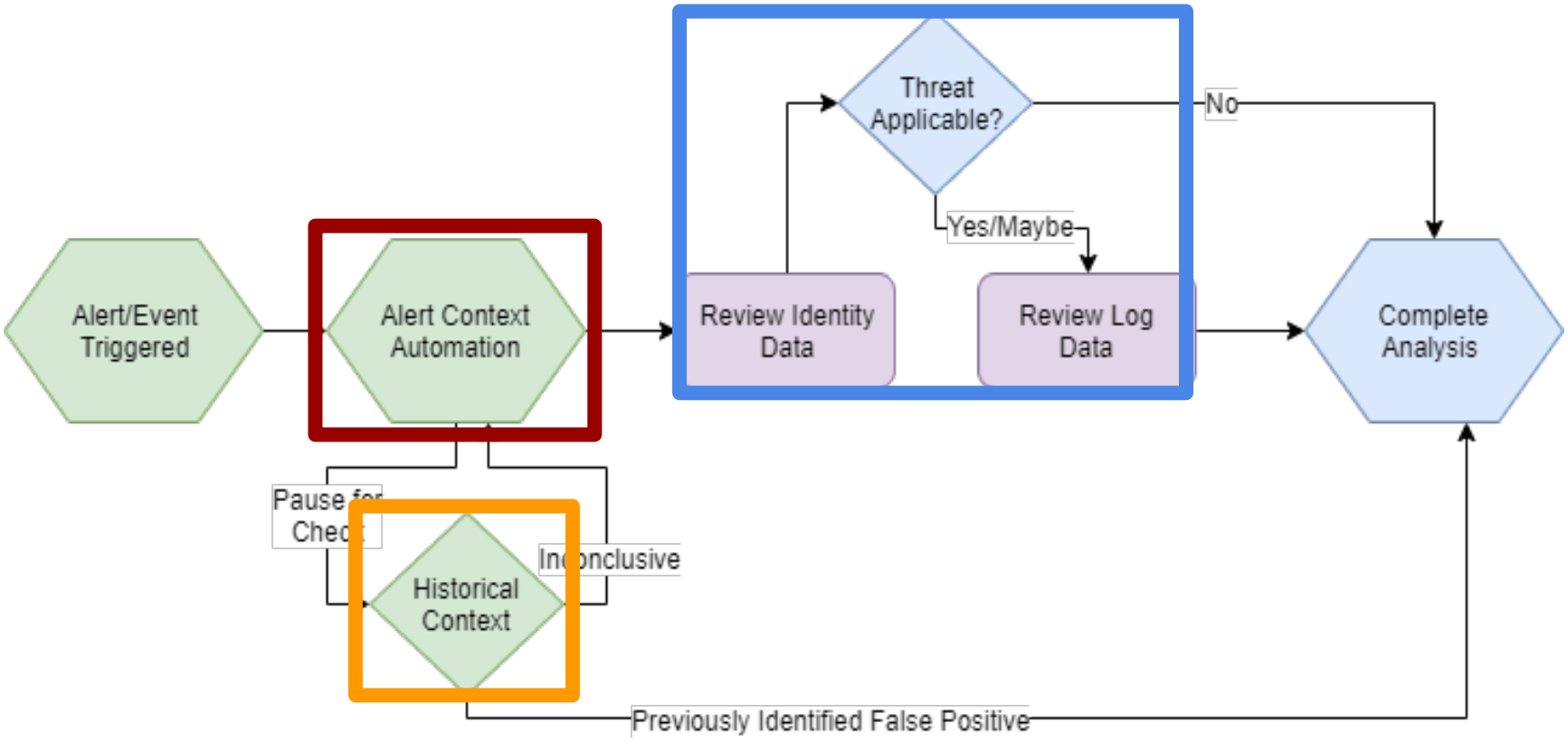
# Alert Context: Evaluate Automation Type




Robotic process automation

Cognitive automation

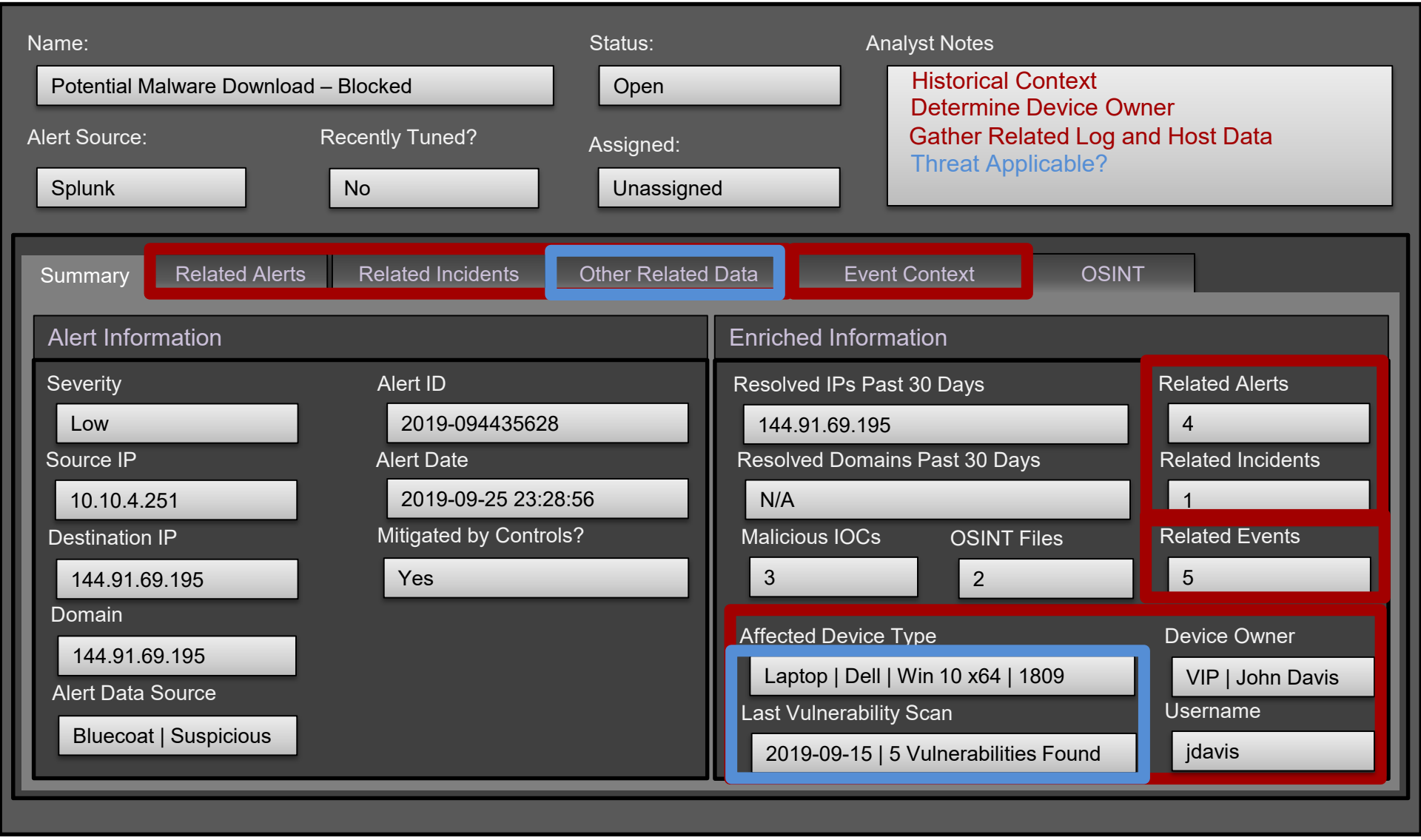
# Alert Context: Evaluate Automation Type



# Alert Context: Impact of Automation

- Time
  - Substitutes something a human would do
    - Automated decisions potentially saves an analyst on average **20 minutes**
    - Potentially saves an **Analyst 15** minutes in data collection
  - Augments what a human would do
    - Holistic context saves an average of **5 minutes** in analysis
- Value
  - Reduces time & effort
  - Reduces Analyst Fatigue

# Alert Context: Example Alert



# Alert Context: Example Alert

Name:

Potential Malware Download – Blocked

Alert Source:

Splunk

Status:

Open

Assigned:

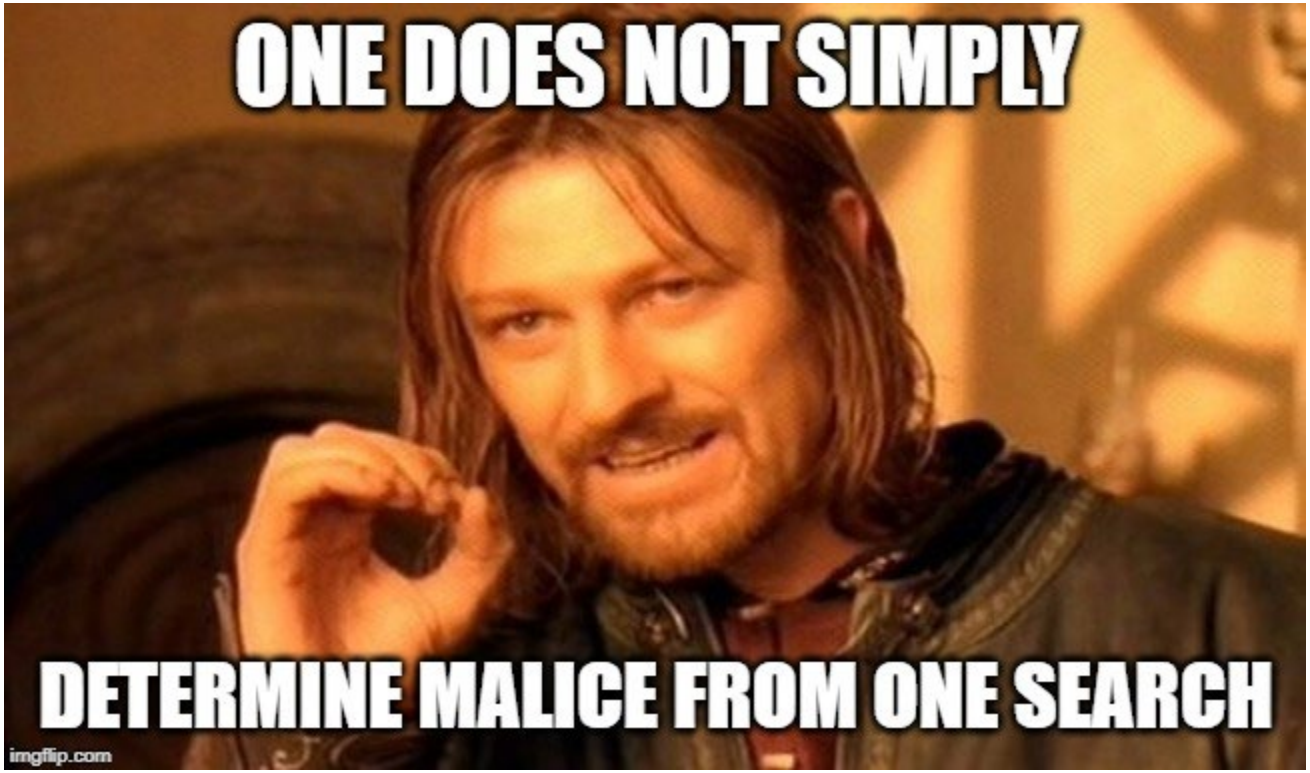
Unassigned

Analyst Notes

Summary | Related Alerts | Related Incidents | Other Related Data | Event Context | OSINT

| Date | Status | Resolution | Name | Severity | Source | Destination | Relationship |
|---|---|---|---|---|---|---|---|
| 2019-09-25 23:27 | Assigned | N/A | Suspicious LNK Execution \| wscript.exe | Low | 10.10.4.251 | 144.91.69.195 | Destination IP |
| 2019-09-25 22:55 | Pending | Removal Request | Suspicious Email \| LNK Attachment | Low | 192.168.15.4 | jdavis@xyz.com | User |
| 2019-09-25 12:10 | Resolved | Remediated | Potential Malware Download – Not Blocked | Moderate | 10.10.4.134 | 144.91.69.195 | Destination IP |
| 2019-09-25 12:10 | Resolved | Remediated | Suspicious LNK Execution \| wscript.exe | Moderate | 10.10.4.134 | 144.91.69.195 | Destination IP |

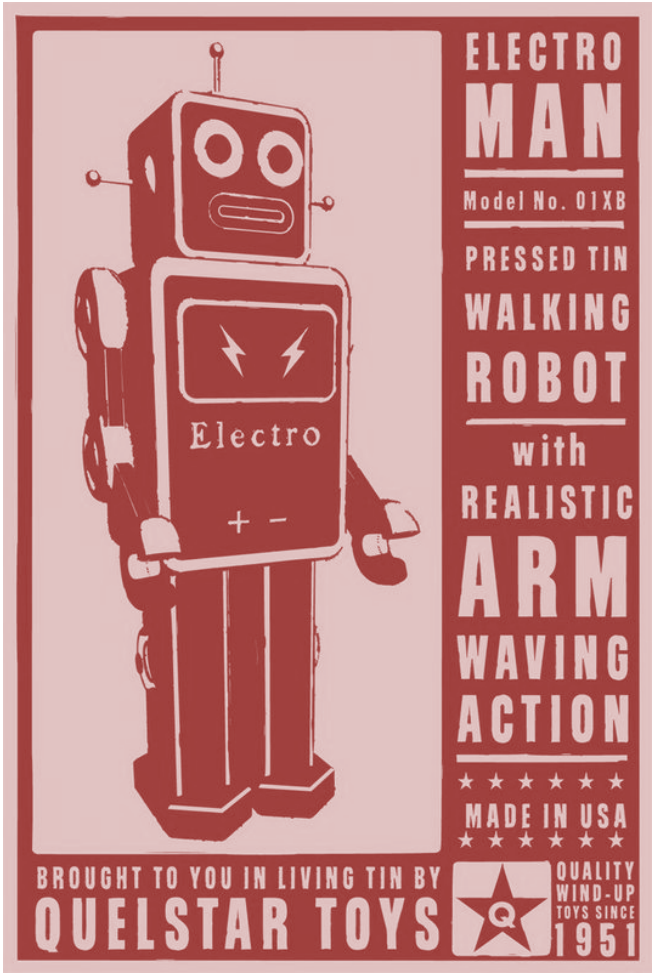
# Case Study: Intelligence Research



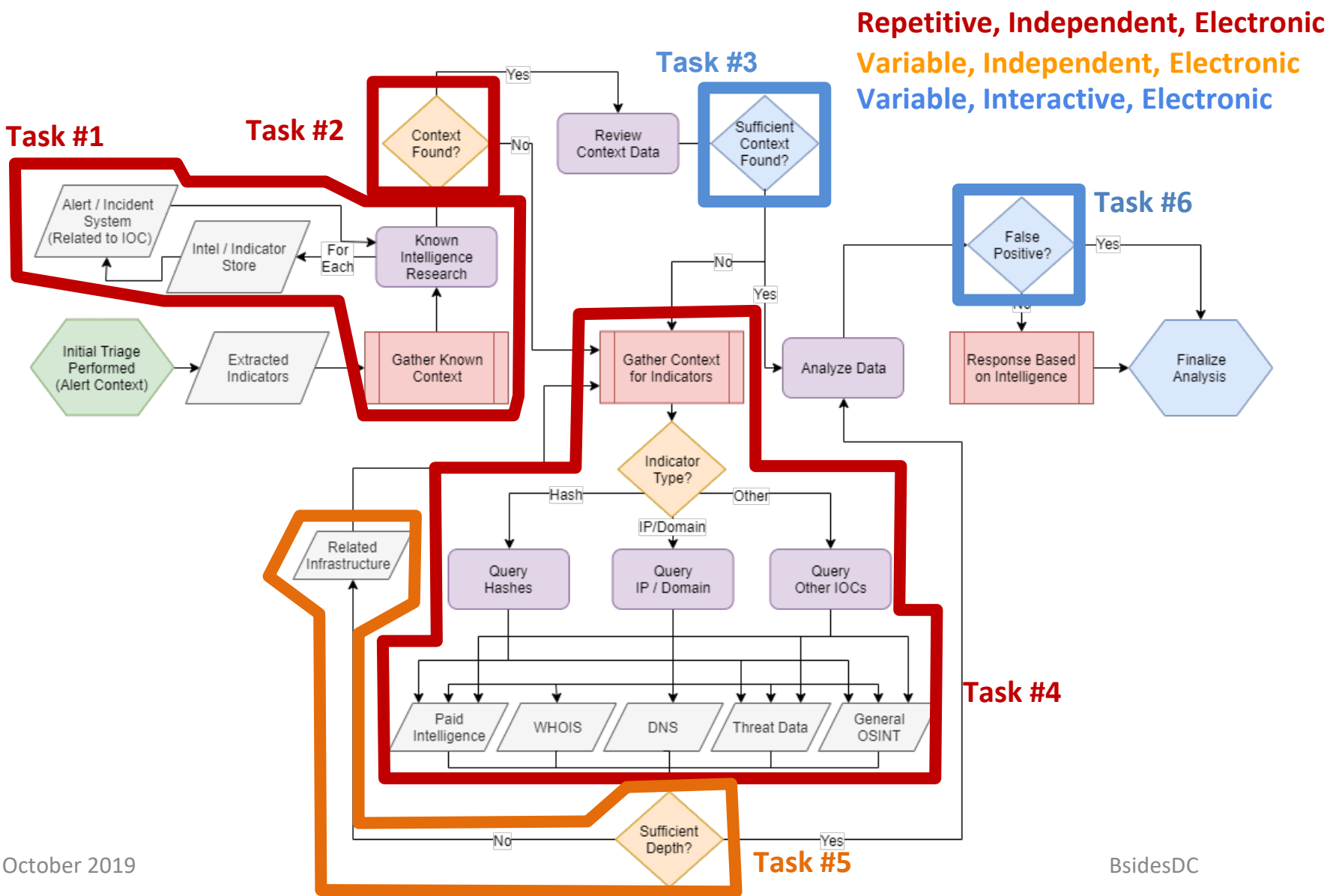
# Intelligence Research: Identify the Opportunity

- What is it?
  - Gathering threat data
    - IOC Context
    - Threat Context
    - Threat Capabilities

- Why Analysts Want it Automated?
  - Often performed during analysis
  - Many of the steps are repetitive
  - Requires searching multiple sources for similar information



# Intelligence Research: Deconstruct the Task



# Intelligence Research: Deconstruct the Task

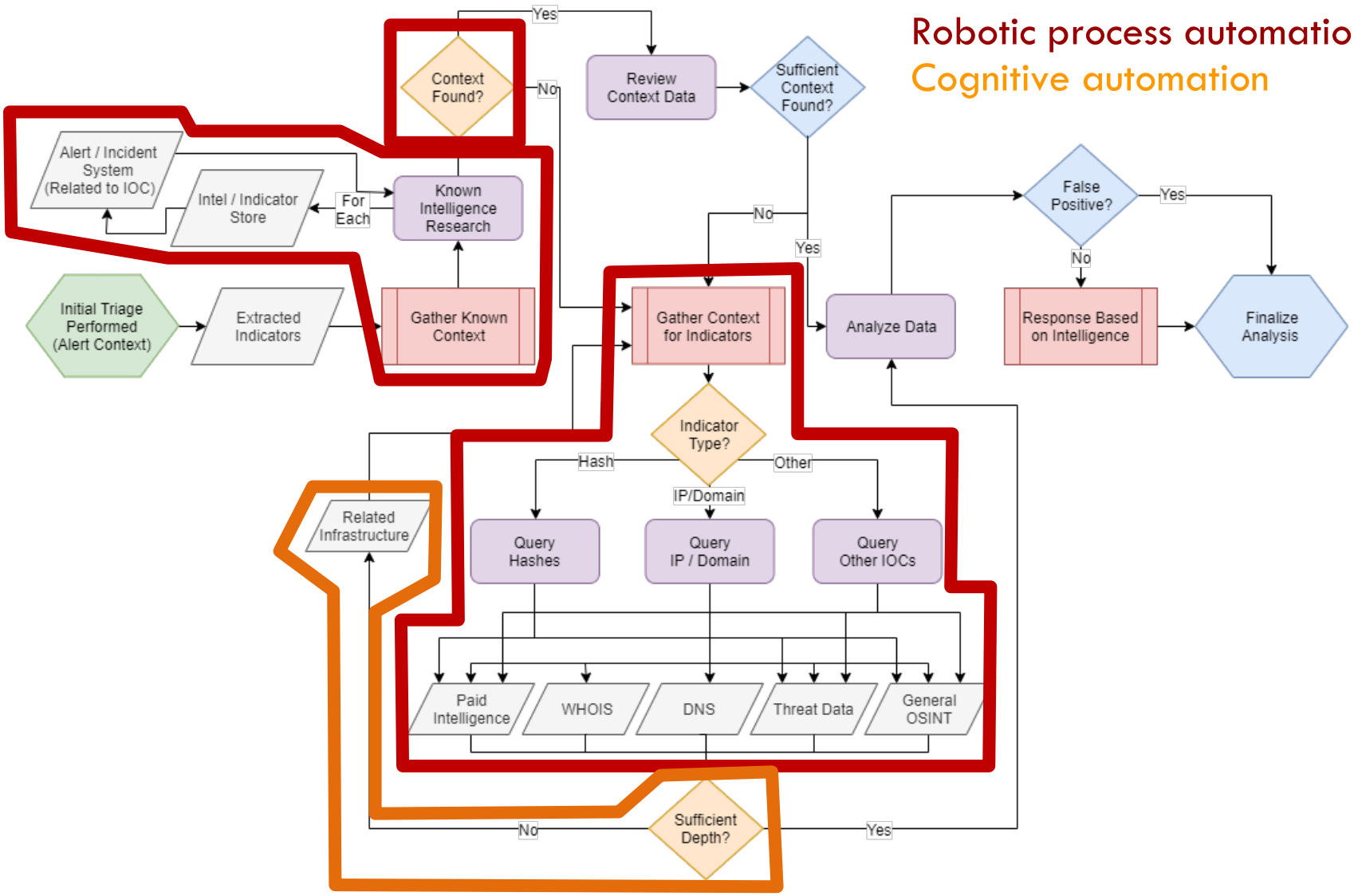
| | Intent | Benefit | Dependency | Difficulty & ROIP |
|---|---|---|---|---|
| **Task #1 Gather Known Context** | • Gather related processed Intelligence<br>• Gather recent context from previous automations | • More timely analysis and response<br>• Reduce subscription API calls<br>• Reduces tools used by analysts | • Tool API Access<br>• Historical or processed Intelligence | Moderate Difficulty<br>Incremental value |
| **Task #2 Context Found?** | • Determine if full Intelligence context is run | • Enables automatic workflow continuation | • Task #1 | Low Difficulty<br>Constant value |
| **Task #3 Sufficient Context Found?** | • Human decision point | • Reduces potential errors | • Known context for analysis OR Task #1 | Human Breakpoint<br>Negative Value |
| **Task #4 Gather Context for Indicators** | • Gather OSINT context for threat identification<br>• Gather related context to original indicators | • More timely analysis and response<br>• Threat context enables more informed response<br>• Reduces tools used by analysts | • Subscription APIs<br>• Free and Open Source APIs | High Difficulty<br>Incremental value |
| **Task #5 Sufficient Depth Check** | • Gather related infrastructure and indicators<br>• Extrapolate related threats | • Extrapolation of indicator relationships<br>• More timely analysis and response | • Intelligence context or Task #4 | Low Difficulty<br>Constant value |
| **Task #6 False Positive Check** | • Human decision point | • Reduces potential errors | • Known context for analysis OR Task #1 | Human Breakpoint<br>Negative Value |

# Intelligence Research: Return on Improved Performance

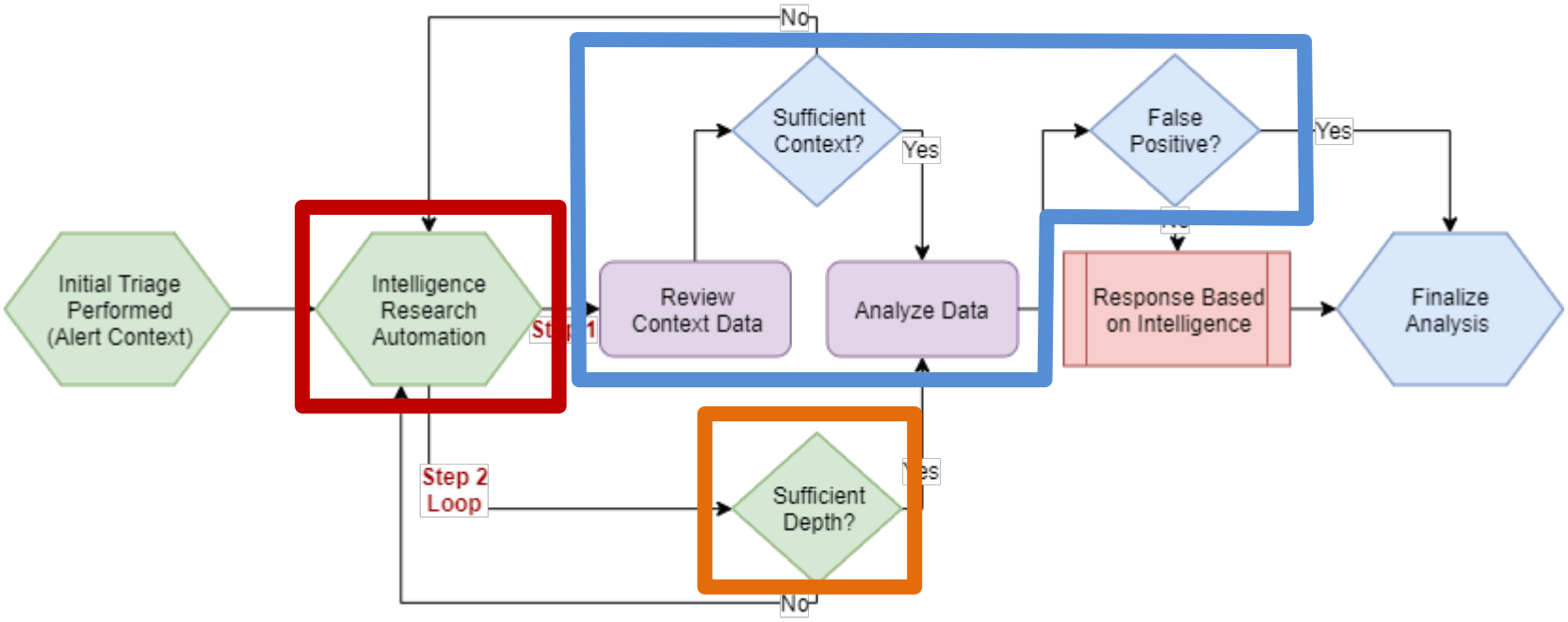
- Where do we start?
  - Gather Known Context (#1)
  - Gather Context for Indicators (#4)
  - Context Found? (#2)
  - Sufficient Depth (#5)

- Incremental value
  - More context = more accurately and timely decisions; every improvement helps
- Constant value
  - More consistent data from consistent sources = easier decision points and removes analyst variability; adds tactical value if not strategic
- Negative value
  - Table stakes like identifying false positives – little value aside beyond doing it consistently and accurately

# Intelligence Research: Evaluate Automation Type



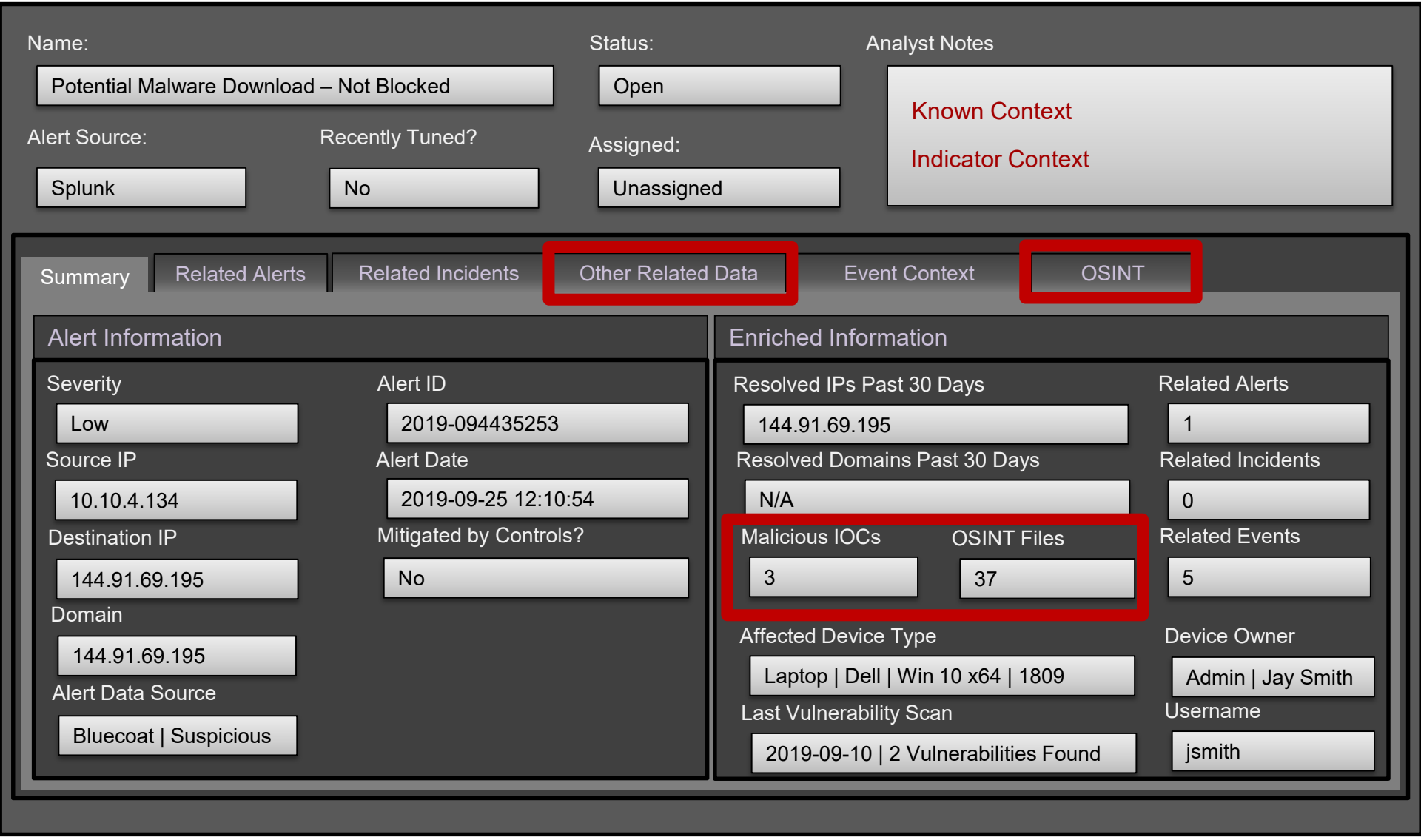
# Intelligence Research: Evaluate Automation Type



# Intelligence Research: Impact of Automation

- Time
  - Substitutes something a human would do
    - Automated several data gathering activity potentially saves an analyst on average **15 minutes**
  - Augments what a human would do
    - Holistic Intelligence saves an average of **5 minutes** in analysis
- Value
  - Reduces effort
  - Reduces time to respond to threats

# Intelligence Research: Example Alert



# Intelligence Research: Example Alert

Name:

Potential Malware Download – Not Blocked

Status:

Open

Analyst Notes

Alert Source:

Splunk

Assigned:

Unassigned

Summary | Related Alerts | Related Incidents | Other Related Data | Event Context | OSINT

| Date | Source | Search Value | Risk Score | Verdict | Key 1 | Key 2 | Key 3 | Key 4 |
|---|---|---|---|---|---|---|---|---|
| 2019-09-25 | urlhaus | dchristjan.com | N/A | Malicious | Tag: Trickbot,Zip,Lnk | Malware Download | Reported: 2019/9/25.. | No. Malware: 1 |
| 2019-09-25 | HybridAnalysis | dchristjan.com | 50 | Malicious | Tag: Unrated Site | - | http://www.dchristja.. | - |
| 2019-09-25 | Feodotracker | 51.254.69.244 | N/A | Malicious | Malware: Trickbot | FR | FirstSeen: 09/18/20.. | No. Malware: 260 |
| 2019-09-25 | PasteBin | 51.254.69.244 | N/A | N/A | Trickbot IoCs | 51.68.247.62:443, 37… | https://pastebin.co.. | 8ae94126db329c2.. |
| 2019-09-25 | Twitter | app.any.run/tas.. | N/A | N/A | @makflwana | 51.254.69.244 | hxxp://www.dchristja.. | C:\Users\admin\A.. |
| 2019-09-25 | RecordedFuture | 144.91.69.195 | 50 | Unusual | Newly Registered, R.. | pasteHits, darkwebHit.. | Antivirus scan for A.. | Additional_info, beh.. |
| 2019-09-25 | HybridAnalysis | 144.91.69.195 | 66 | Malicious | LNK/Autorun.Generic | cmd.exe /c del qEtLd.. | http://144.91.69.19.. | D106885c1c00ff3d.. |
| 2019-09-25 | AnyRun | 144.91.69.195 | N/A | Malicious | Tag: Trickbot, Loader | cmd.exe /c del qEtLd.. | http://144.91.69.19.. | A1AF9D8EEADDF.. |
| 2019-09-25 | VirusTotal | 144.91.69.195 | N/A | Malicious | http://144.91.69.19.. | Solar.php | dd05ce3a-a9c9-4.. | A1AF9D8EEADDF.. |
| 2019-09-25 | PassiveTotal | 144.91.69.195 | N/A | N/A | 10/17/2019 | OpenSSH, CentOS.. | 0 Domains | No History |
| 2019-09-25 | DomainTools | 144.91.69.195 | N/A | N/A | Germany | Germany Munich Co.. | Contabo GmbH | Michael Herpich |

# Risks & Opportunities

- Staff re-training
- Engineering support
- Doing too much

# Take-Aways

1. Automation is a process or a capability
2. Repeatable, agile process helps us avoid rabbit holes with little or no return on our investment
3. Priorities are important: not all improvements provide equal value
4. Take an automation initiative (or proposed initiative) and try to quantify return on automation investment

# Thank You!

@branbot1000 @markaorlando