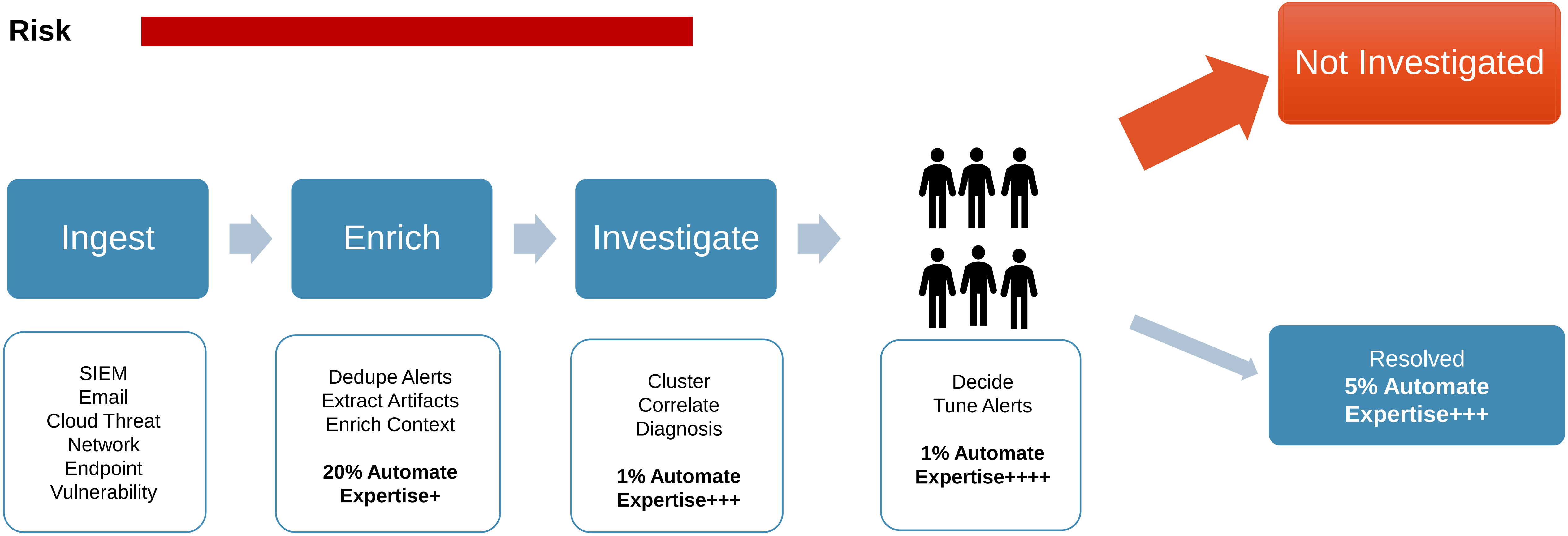
# Resolving Security Alerts with Augmented Intelligence

Peter Luo
Founder, CEO of DTonomy

# Manual Security Investigation and Response (MSIR)



Risk

Ingest

Enrich

Investigate

SIEM
Email
Cloud Threat
Network
Endpoint
Vulnerability

Dedupe Alerts
Extract Artifacts
Enrich Context

**20% Automate**
**Expertise+**

Cluster
Correlate
Diagnosis

**1% Automate**
**Expertise+++**

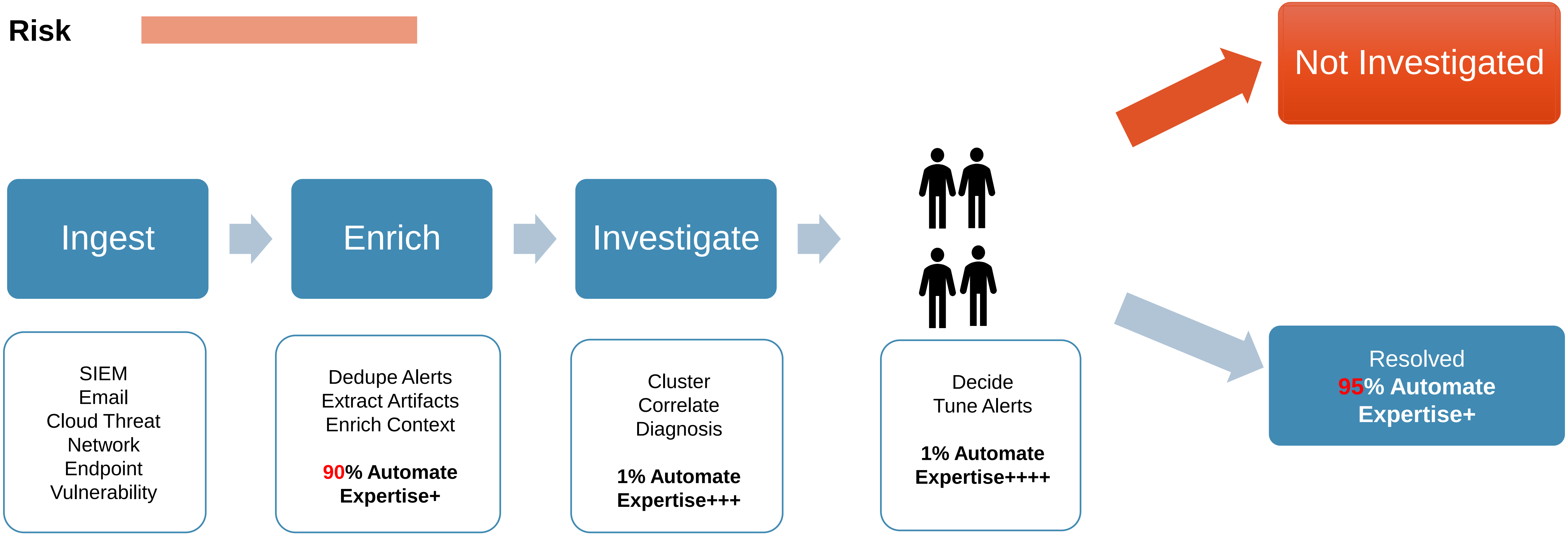
Decide
Tune Alerts

**1% Automate**
**Expertise++++**

Not Investigated

Resolved
**5% Automate**
**Expertise+++**

# Manual Security Investigation and Response (MSIR) + SOAR



Risk

Not Investigated

Ingest

Enrich

Investigate

SIEM
Email
Cloud Threat
Network
Endpoint
Vulnerability

Dedupe Alerts
Extract Artifacts
Enrich Context

**90% Automate**
**Expertise+**

Cluster
Correlate
Diagnosis

**1% Automate**
**Expertise+++**

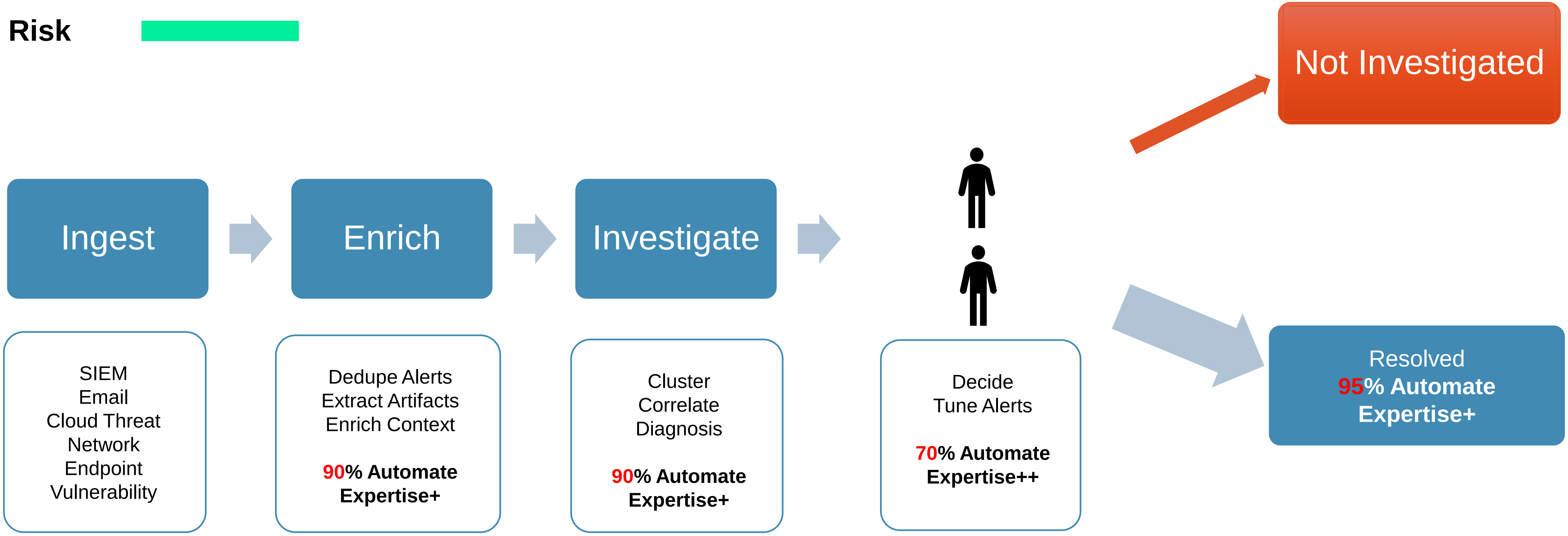
Decide
Tune Alerts

**1% Automate**
**Expertise++++**

Resolved
**95% Automate**
**Expertise+**

# Manual Security Investigation and Response (MSIR)
# + SOAR
# + AI

Risk 🟩



Ingest

SIEM
Email
Cloud Threat
Network
Endpoint
Vulnerability

Enrich

Dedupe Alerts
Extract Artifacts
Enrich Context

**90% Automate**
**Expertise+**

Investigate

Cluster
Correlate
Diagnosis

**90% Automate**
**Expertise+**

Decide
Tune Alerts

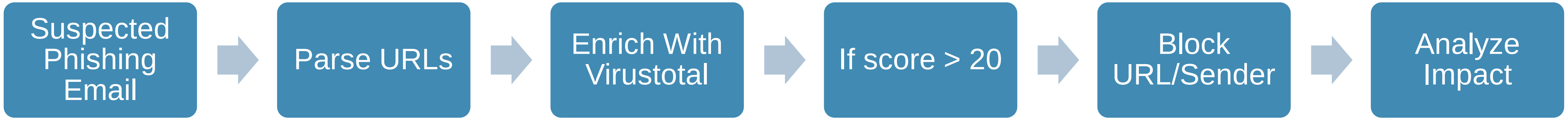
**70% Automate**
**Expertise++**

Not Investigated

Resolved
**95% Automate**
**Expertise+**

# SOAR

- If you have a procedure in place, automate it with SOAR



Simplified Phishing IR workflow

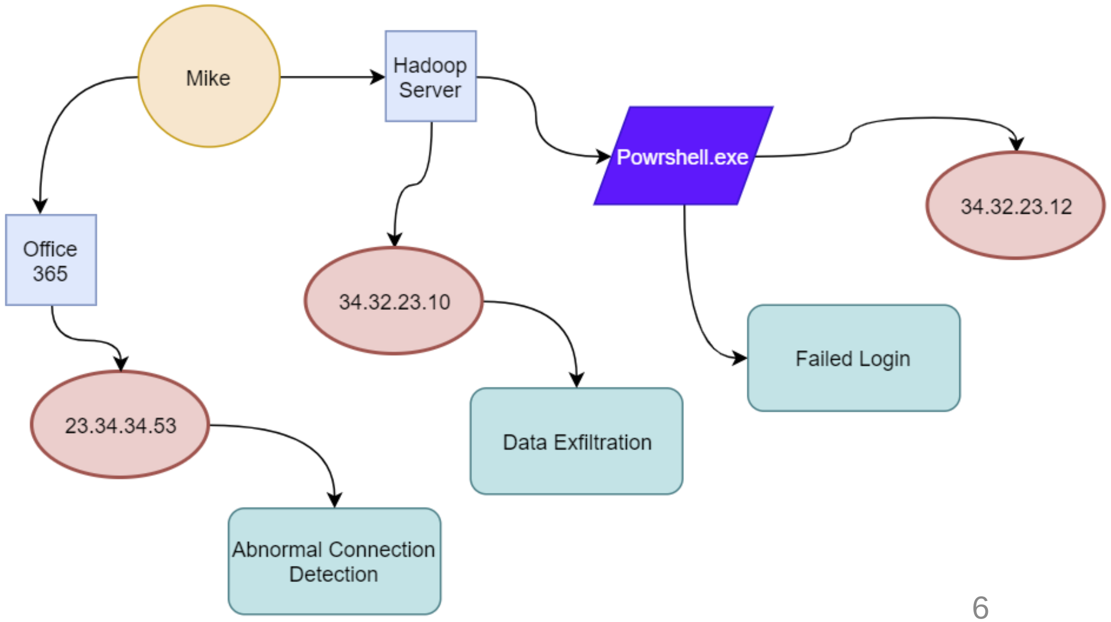
# AI - Augmented Intelligence

## - Cluster Your Alerts

| |
|---|
| Alert 1 – End point detection:<br>Mike \| Hadoop Server \| Powershell.exe \| 34.32.23.12 \| Abnormal Connection Detection |
| Alert 2 – Network detection:<br>Hadoop Server \| 34.32.23.10 \| 200MB \| Data exfiltration Detection |
| Alert 3 – Cloud detection:<br>Mike \| 23.34.34.53 \| Office 365 \| 5 times \| Failed Login |

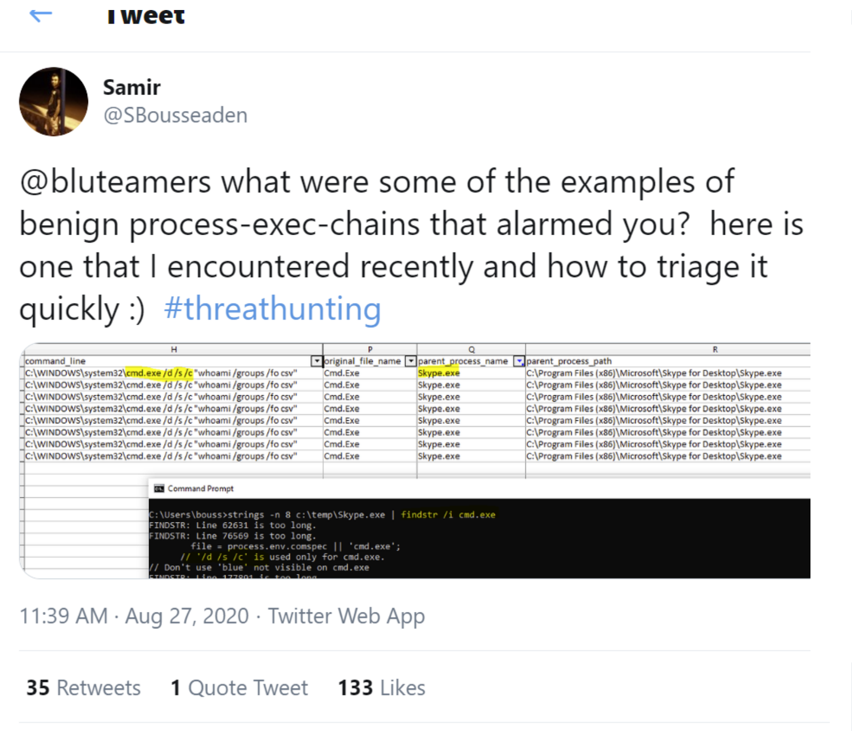
**Recommendation:**

Alert 1&2&3 belong to same group



# AI - Augmented Intelligence

## - Normal Pattern Recognition



Tweet

**Samir**
@SBousseaden

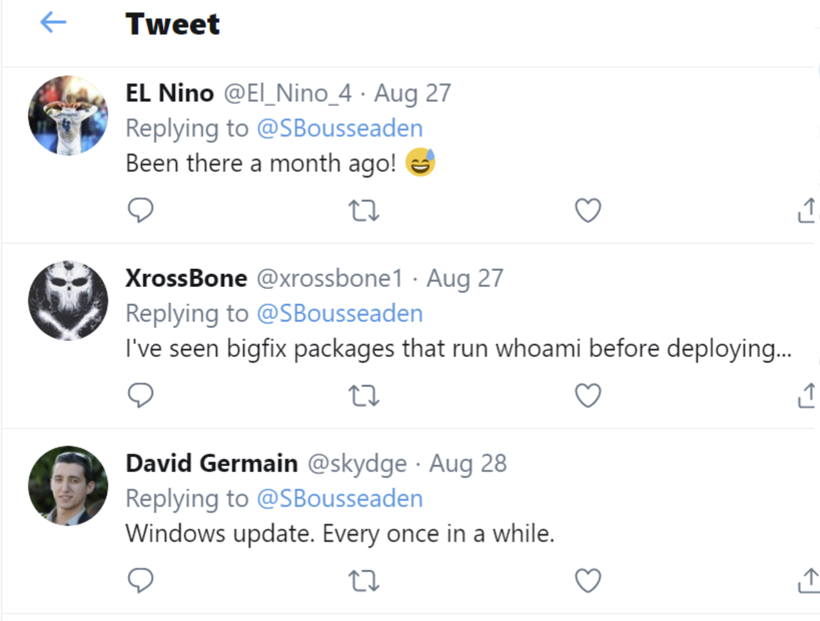
@bluteamers what were some of the examples of benign process-exec-chains that alarmed you? here is one that I encountered recently and how to triage it quickly :) #threathunting

| H | P | Q | R |
|---|---|---|---|
| command_line | original_file_name | parent_process_name | parent_process_path |
| C:\WINDOWS\system32\cmd.exe /d /s /c "whoami /groups /fo csv" | Cmd.Exe | Skype.exe | C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe |
| C:\WINDOWS\system32\cmd.exe /d /s /c "whoami /groups /fo csv" | Cmd.Exe | Skype.exe | C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe |
| C:\WINDOWS\system32\cmd.exe /d /s /c "whoami /groups /fo csv" | Cmd.Exe | Skype.exe | C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe |
| C:\WINDOWS\system32\cmd.exe /d /s /c "whoami /groups /fo csv" | Cmd.Exe | Skype.exe | C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe |
| C:\WINDOWS\system32\cmd.exe /d /s /c "whoami /groups /fo csv" | Cmd.Exe | Skype.exe | C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe |
| C:\WINDOWS\system32\cmd.exe /d /s /c "whoami /groups /fo csv" | Cmd.Exe | Skype.exe | C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe |
| C:\WINDOWS\system32\cmd.exe /d /s /c "whoami /groups /fo csv" | Cmd.Exe | Skype.exe | C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe |
| C:\WINDOWS\system32\cmd.exe /d /s /c "whoami /groups /fo csv" | Cmd.Exe | Skype.exe | C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe |

```
C:\Users\bouss>strings -n 8 c:\temp\Skype.exe | findstr /i cmd.exe
FINDSTR: Line 62631 is too long.
FINDSTR: Line 76569 is too long.
        file = process.env.comspec || 'cmd.exe';
      // '/d /s /c' is used only for cmd.exe.
// Don't use 'blue' not visible on cmd.exe
FINDSTR: Line 177891 is too long.
```

11:39 AM · Aug 27, 2020 · Twitter Web App

**35** Retweets **1** Quote Tweet **133** Likes

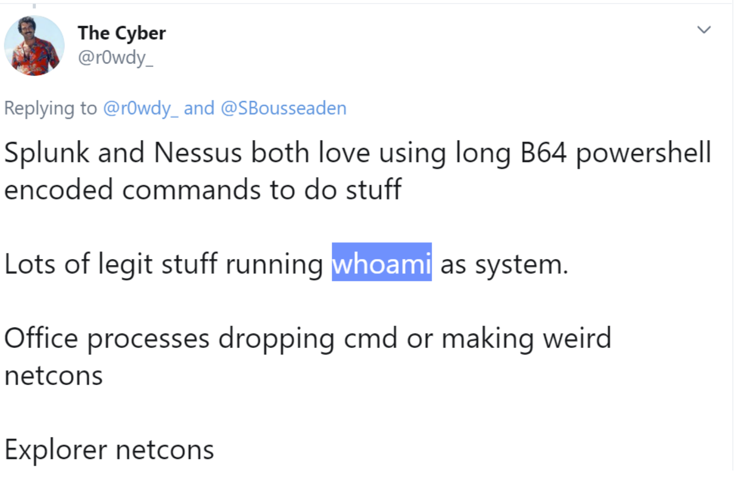


Tweet

**EL Nino** @El_Nino_4 · Aug 27
Replying to @SBousseaden
Been there a month ago! 😅

**XrossBone** @xrossbone1 · Aug 27
Replying to @SBousseaden
I've seen bigfix packages that run whoami before deploying...

**David Germain** @skydge · Aug 28
Replying to @SBousseaden
Windows update. Every once in a while.



**The Cyber**
@r0wdy_

Replying to @r0wdy_ and @SBousseaden

Splunk and Nessus both love using long B64 powershell encoded commands to do stuff

Lots of legit stuff running whoami as system.

Office processes dropping cmd or making weird netcons

Explorer netcons

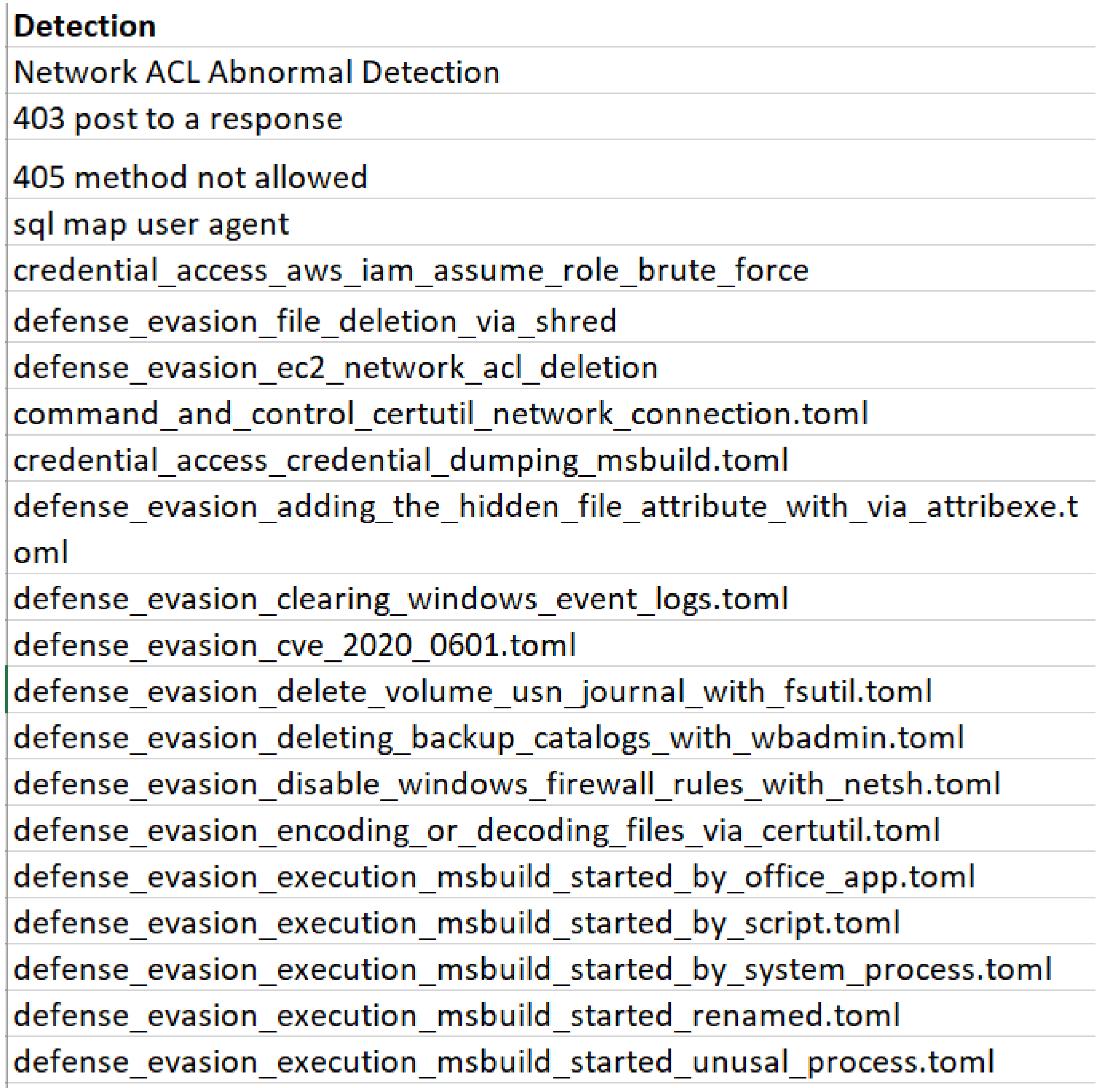
**Recommendation**:

bigfix -> whoami is normal

# AI - Augmented Intelligence

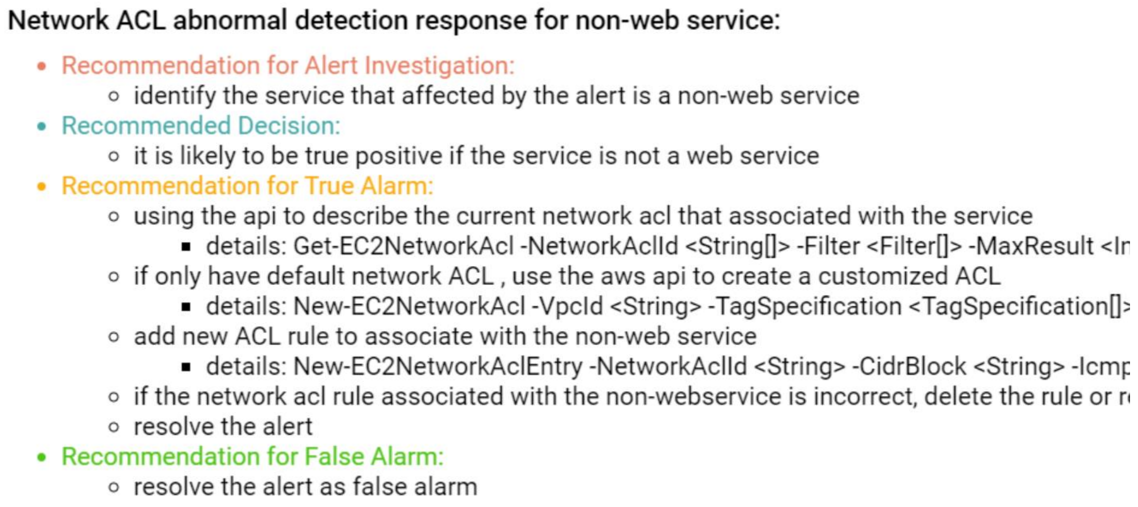
## - Recommend Response to any alerts

### Variety Different Type Of Security Alerts



| Detection |
|---|
| Network ACL Abnormal Detection |
| 403 post to a response |
| 405 method not allowed |
| sql map user agent |
| credential_access_aws_iam_assume_role_brute_force |
| defense_evasion_file_deletion_via_shred |
| defense_evasion_ec2_network_acl_deletion |
| command_and_control_certutil_network_connection.toml |
| credential_access_credential_dumping_msbuild.toml |
| defense_evasion_adding_the_hidden_file_attribute_with_via_attribexe.toml |
| defense_evasion_clearing_windows_event_logs.toml |
| defense_evasion_cve_2020_0601.toml |
| defense_evasion_delete_volume_usn_journal_with_fsutil.toml |
| defense_evasion_deleting_backup_catalogs_with_wbadmin.toml |
| defense_evasion_disable_windows_firewall_rules_with_netsh.toml |
| defense_evasion_encoding_or_decoding_files_via_certutil.toml |
| defense_evasion_execution_msbuild_started_by_office_app.toml |
| defense_evasion_execution_msbuild_started_by_script.toml |
| defense_evasion_execution_msbuild_started_by_system_process.toml |
| defense_evasion_execution_msbuild_started_renamed.toml |
| defense_evasion_execution_msbuild_started_unusal_process.toml |

### Recommend Response



**Network ACL abnormal detection response for non-web service:**

- Recommendation for Alert Investigation:
  - identify the service that affected by the alert is a non-web service
- Recommended Decision:
  - it is likely to be true positive if the service is not a web service
- Recommendation for True Alarm:
  - using the api to describe the current network acl that associated with the service
    - details: Get-EC2NetworkAcl -NetworkAclId <String[]> -Filter <Filter[]> -MaxResult <I
  - if only have default network ACL , use the aws api to create a customized ACL
    - details: New-EC2NetworkAcl -VpcId <String> -TagSpecification <TagSpecification[]>
  - add new ACL rule to associate with the non-web service
    - details: New-EC2NetworkAclEntry -NetworkAclId <String> -CidrBlock <String> -Icmp
  - if the network acl rule associated with the non-webservice is incorrect, delete the rule or r
  - resolve the alert
- Recommendation for False Alarm:
  - resolve the alert as false alarm

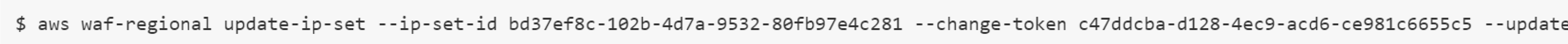
# AI - Augmented Intelligence

## - Recommend Personalized Action

Block IP

*Your Environment: AWS*

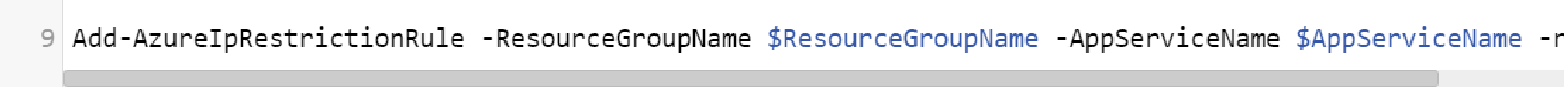
Recommend Action:



```
$ aws waf-regional update-ip-set --ip-set-id bd37ef8c-102b-4d7a-9532-80fb97e4c281 --change-token c47ddcba-d128-4ec9-acd6-ce981c6655c5 --update
```

*Your Environment: Azure*

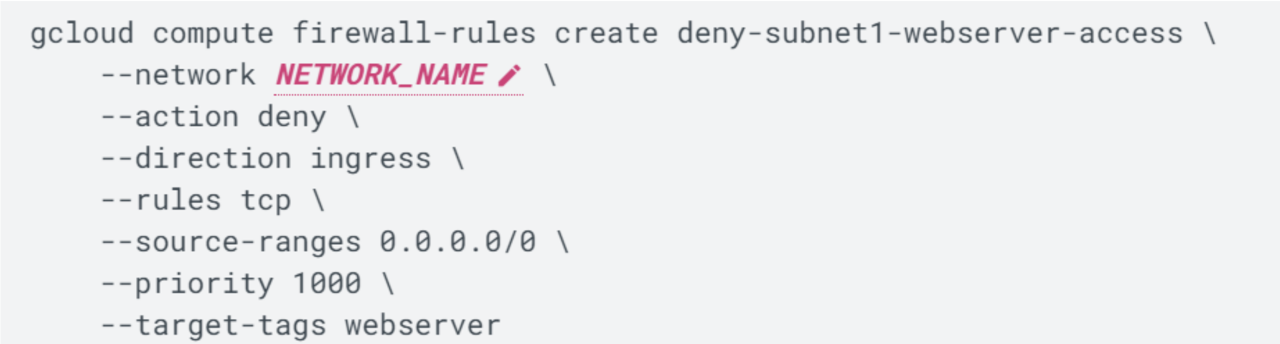
Recommend Action:



```
Add-AzureIpRestrictionRule -ResourceGroupName $ResourceGroupName -AppServiceName $AppServiceName -r
```

*Your Environment: GCP*

Recommend Action:



```
gcloud compute firewall-rules create deny-subnet1-webserver-access \
    --network NETWORK_NAME \
    --action deny \
    --direction ingress \
    --rules tcp \
    --source-ranges 0.0.0.0/0 \
    --priority 1000 \
    --target-tags webserver
```

# AI - Augmented Intelligence

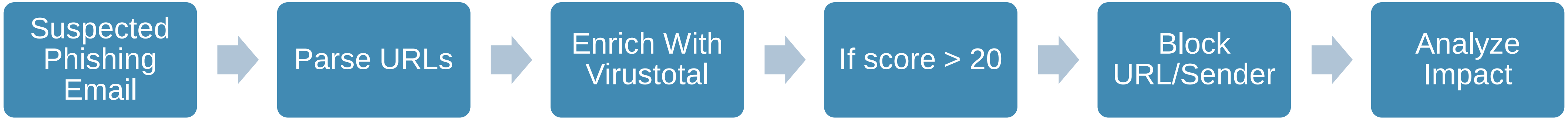
## - Suggest Correlation

| Alerts | Your Resolution |
|---|---|
| sender@gmail.com \| receiver@company.com \| does not have attachment \| | False positive |
| sender1@gmail.com \| receiver1@company.com \| does have attachment \| | False positive |
| sender2@gmail.com \| receiver2@company.com \| does not have attachment \| | True positive |

Recommend **Decision Insights:**
“Does not have attachment” => “False positive” with 67% confidence

# AI - Augmented Intelligence

## - SOAR Improvement Recommendation



Suspected Phishing Email

Parse URLs

Enrich With Virustotal

If score > 20

Block URL/Sender

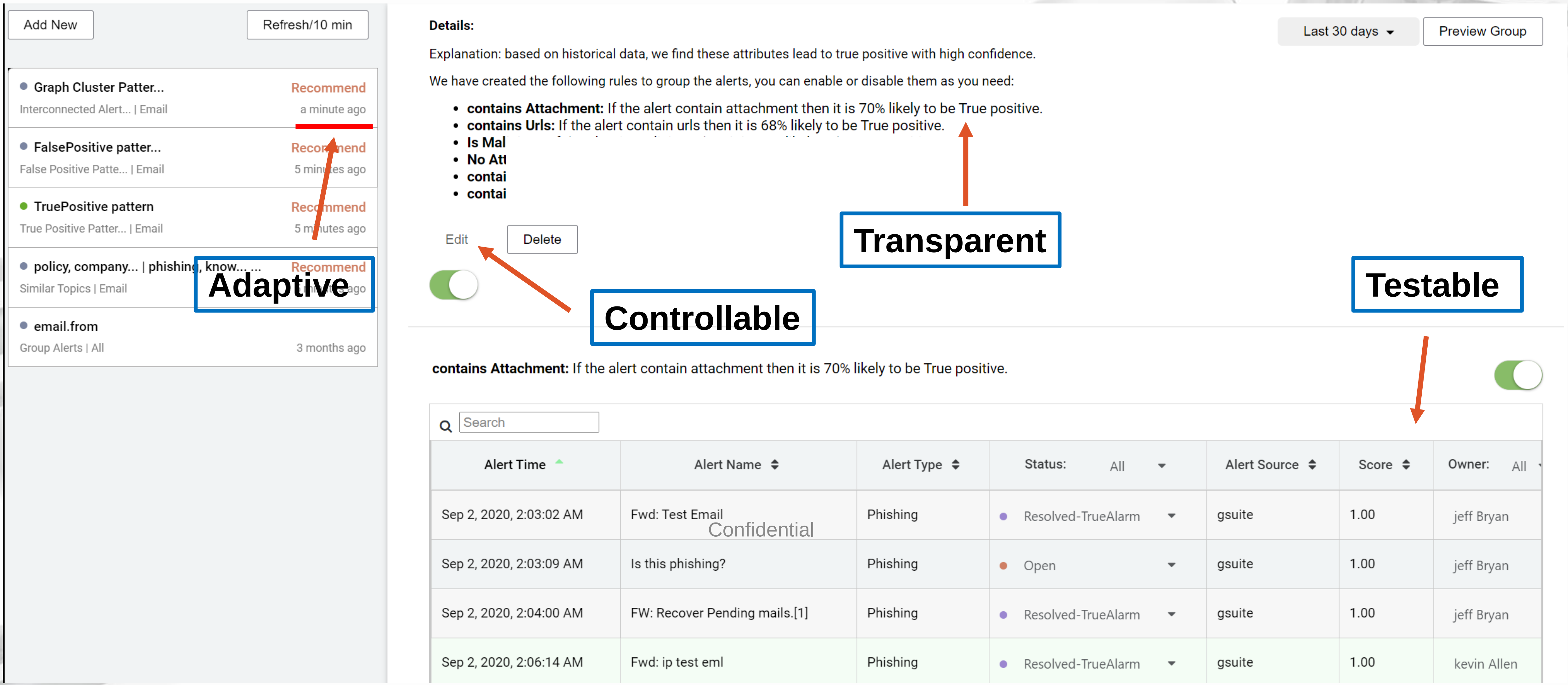
Analyze Impact

**Recommendation:**

Your score generates too many false positives alerts, please adjust to 30!

# Traditional AI = Black Box

## A Good AI System



- Graph Cluster Patter... — Recommend
  Interconnected Alert... | Email — a minute ago
- FalsePositive patter... — Recommend
  False Positive Patte... | Email — 5 minutes ago
- TruePositive pattern — Recommend
  True Positive Patter... | Email — 5 minutes ago
- policy, company... | phishing, know... ... — Recommend
  Similar Topics | Email — minutes ago
- email.from
  Group Alerts | All — 3 months ago

**Details:**

Explanation: based on historical data, we find these attributes lead to true positive with high confidence.

We have created the following rules to group the alerts, you can enable or disable them as you need:

- **contains Attachment:** If the alert contain attachment then it is 70% likely to be True positive.
- **contains Urls:** If the alert contain urls then it is 68% likely to be True positive.
- **Is Mal**
- **No Att**
- **contai**
- **contai**

Adaptive

Transparent

Controllable

Testable

**contains Attachment:** If the alert contain attachment then it is 70% likely to be True positive.

| Alert Time | Alert Name | Alert Type | Status: All | Alert Source | Score | Owner: All |
|---|---|---|---|---|---|---|
| Sep 2, 2020, 2:03:02 AM | Fwd: Test Email | Phishing | ● Resolved-TrueAlarm | gsuite | 1.00 | jeff Bryan |
| Sep 2, 2020, 2:03:09 AM | Is this phishing? | Phishing | ● Open | gsuite | 1.00 | jeff Bryan |
| Sep 2, 2020, 2:04:00 AM | FW: Recover Pending mails.[1] | Phishing | ● Resolved-TrueAlarm | gsuite | 1.00 | jeff Bryan |
| Sep 2, 2020, 2:06:14 AM | Fwd: ip test eml | Phishing | ● Resolved-TrueAlarm | gsuite | 1.00 | kevin Allen |

# Summary

- **SOAR**
  - Set up a procedure and automate it
- **AI – Augmented Intelligence**
  - Discover unknown unknowns for you
- Website: www.dtonomy.com
- Contact: pchluo@dtonomy.com