Decision Automation: Teaching Machines to Hunt

Kumar Saurabh
2019.05.02
Typical SOC

Decision Automation: Signal vs. noise

BILIONS

BILLIONS of Security Events

THOUSANDS

Eliminate False Positives

HUNDREDS

Incidents

TENS

Ignored Notifications

THOUSANDS

Alerts

Detection Rules

Alert Triage

Incident Response

Signal vs. noise

Typical SOC

LogicHub
Factor Analysis

- A factor which will turn true for alerts, false for non alerts.
- OK to have false positive rate on every factor
- Reduce false positive rates by applying multiple factors
Spot the red signal

1 out of 100

1 out of 10,000

1 out of 100,000,000
Decision Automation

Context & Event Types

Enriched Events

Multi-Dimensional Reductions

Scoring Rules

Threat Ranking

Machine Learning

Human Feedback
Threat Hunting in GitHub Logs

Diagram showing processes and decision points for threat hunting in GitHub logs.
Phishing Triage

Automated Step
Get Emails
- Get emails - IMAP

Automated Step
Select

Emails With Description

Automated Step
VirusTotal: URL Reputation
- VirusTotal check and score - Array of urls

Automated Step
Suspicious Keywords
- Find a keyword match and score

Automated Step
McToolbox
- McToolbox email check

Automated Step
Score using Machine Learning
- Phishing Classifier

Automated Step
Domain Name Similarity
- Edit distance - array of URLs

Automated Step
Merge Enriched Data
- Correlate 5 nodes

Automated Step
Max Score
- Assign max score - 5 fields
Thank you!