RSAConference2017

Singapore | 26 – 28 July | Marina Bay Sands

POWER OF OPPORTUNITY

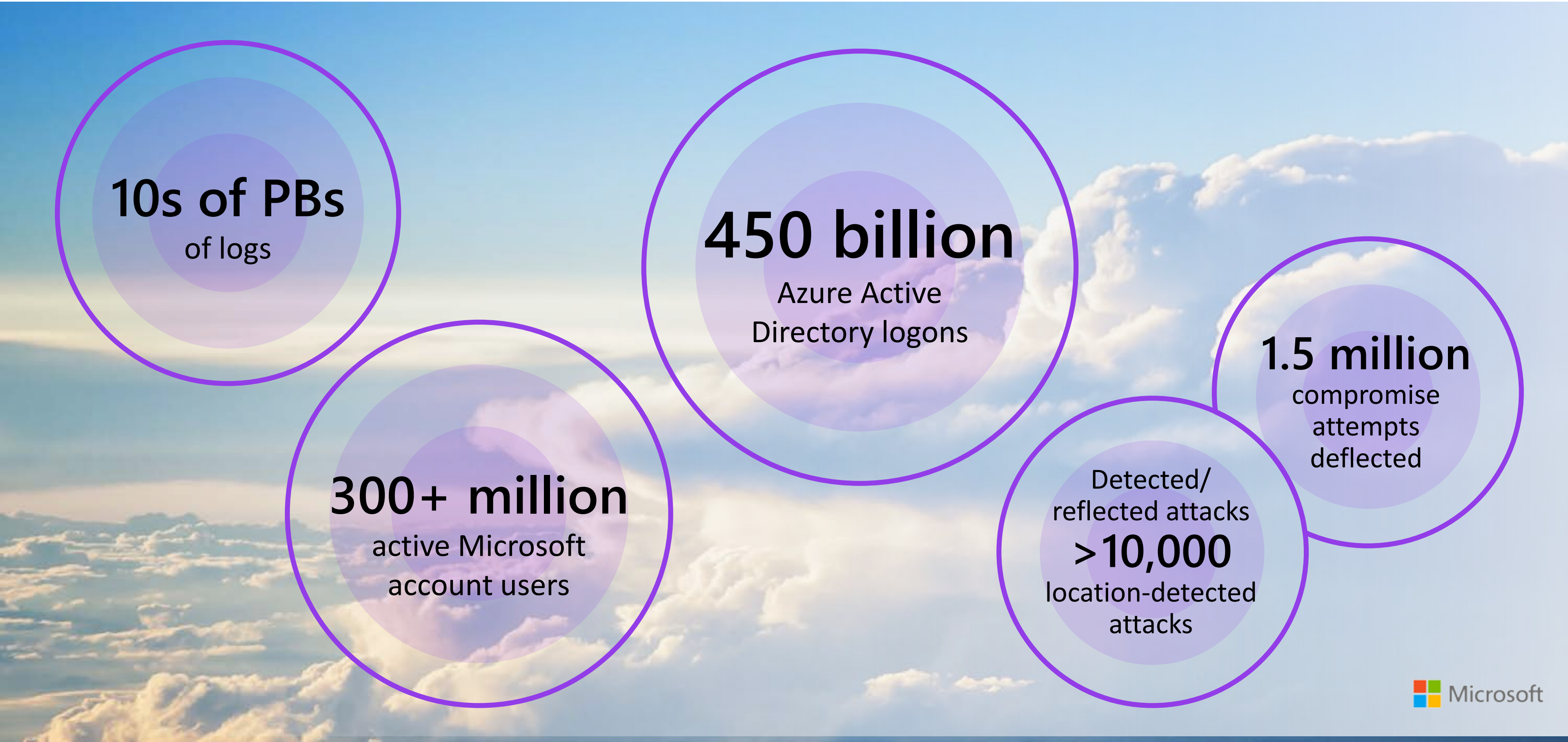
SESSION ID: TTA-R02

10x – Increase Your Team's Effectiveness by Automating the Boring Stuff

Jonathan Trull
Chief Cybersecurity Advisor
Microsoft
@jonathantrull

Vidhi Agarwal
Senior Program Manager
Microsoft Cyber Defense Operations Center

Microsoft’s daily cloud security scale



10s of PBs
of logs

300+ million
active Microsoft account users

450 billion
Azure Active Directory logons

Detected/ reflected attacks
>10,000
location-detected attacks

1.5 million
compromise attempts deflected

WE HAVE A PROBLEM

DETECTION

Insights come from logs, support calls, core services, humans, ‘scanners’, etc.

DROWNING IN **DATA**

INTELLIGENCE

TI is acquired from providers, web searches, news feeds, peers, suppliers, etc.

Ingestion is difficult, untimely and ad-hoc: purchased TI is a ‘lookup resource’

SIEMS

Signals growing far faster than staffing; New sources welcomed with a <sigh>

WE HAVE A PROBLEM

WHERE WE **NEED** TO BE

INTELLIGENCE

should be **part of the security framework**, not just a referenced artifact

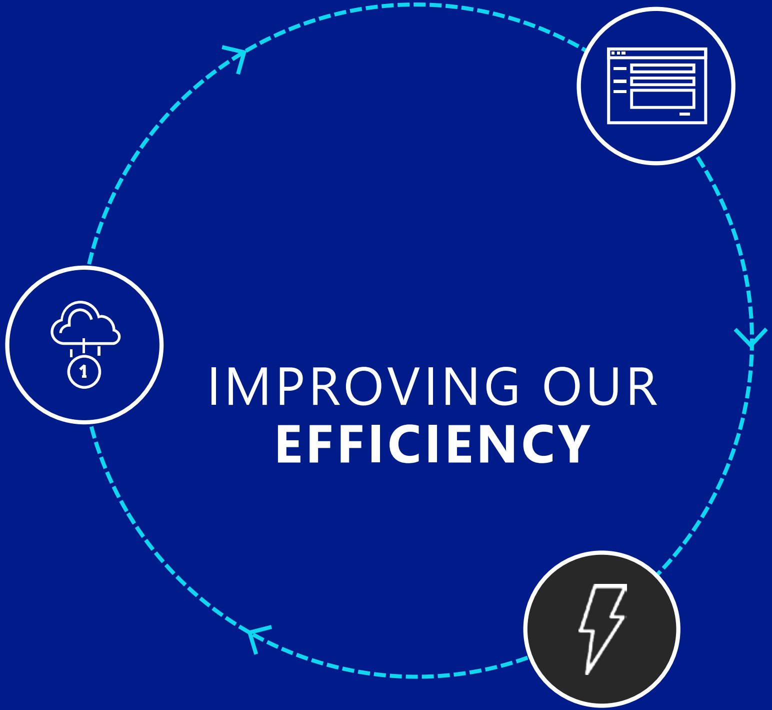
SIEMS

Must **reduce busy work** of incident roll-up, response, and management

DETECTION

Detectors should be **automated, correlated and interlinked** in their findings

(LESS) OBVIOUS, SECOND-ORDER PROBLEMS



IMPROVING OUR **EFFICIENCY**

FEEDS

Orgs seek industry/geo specific intelligence to correlate against their signals

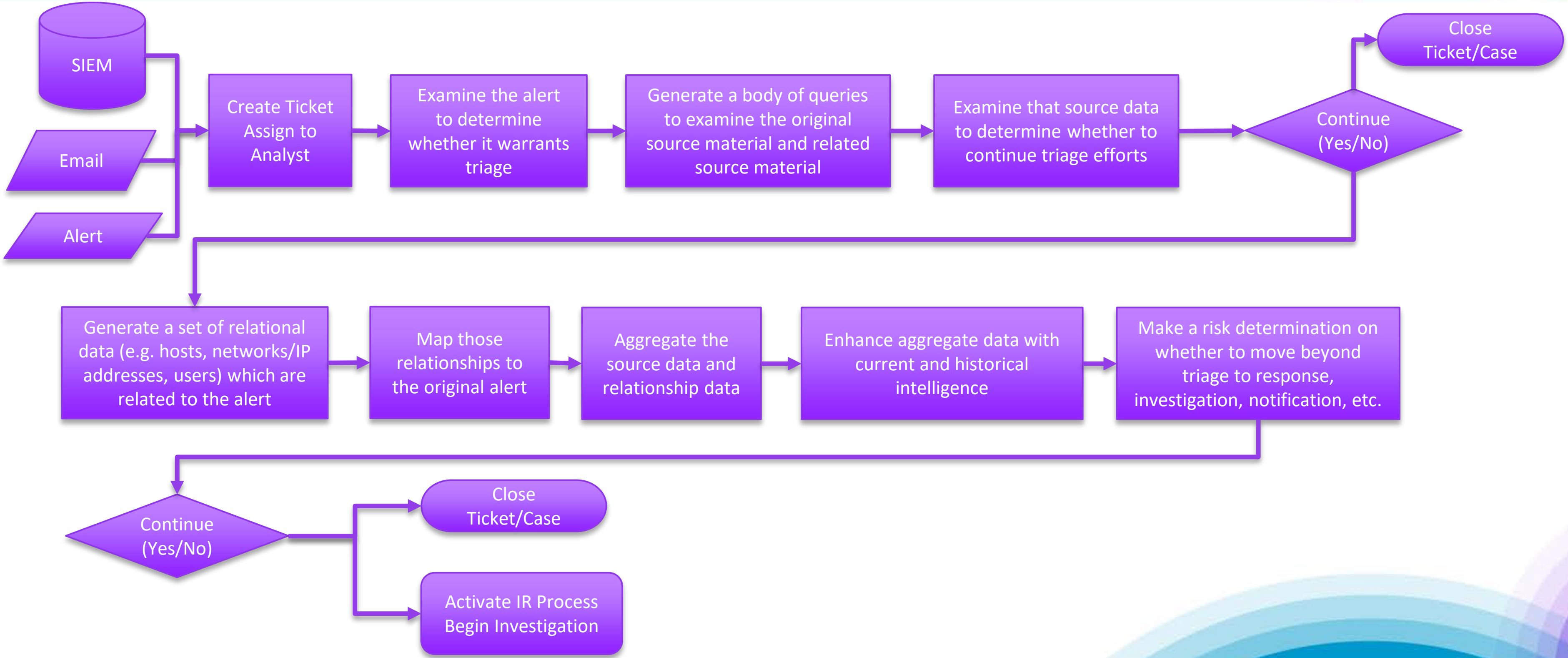
EVENTS

ML/AI should make the data work for humans, not the other way round

INCIDENTS

Software should consolidate, de-dupe, and otherwise prepare ‘Incidents’.

Common SOC Analyst Activities



SIEM

Email

Alert

Create Ticket Assign to Analyst

Examine the alert to determine whether it warrants triage

Generate a body of queries to examine the original source material and related source material

Examine that source data to determine whether to continue triage efforts

Continue (Yes/No)

Close Ticket/Case

Generate a set of relational data (e.g. hosts, networks/IP addresses, users) which are related to the alert

Map those relationships to the original alert

Aggregate the source data and relationship data

Enhance aggregate data with current and historical intelligence

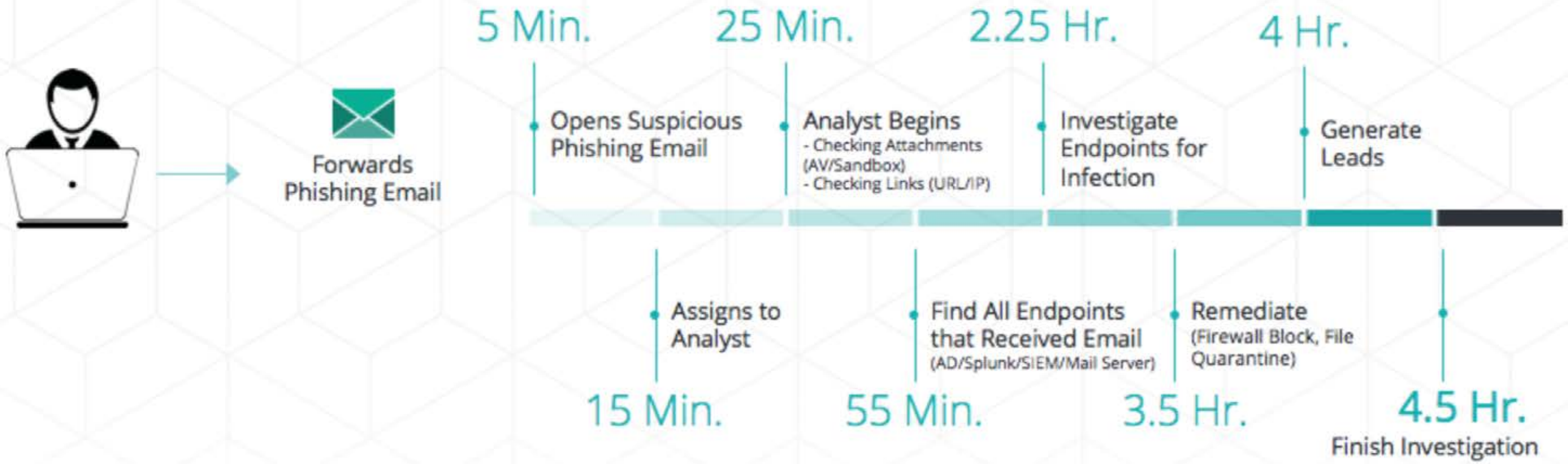
Make a risk determination on whether to move beyond triage to response, investigation, notification, etc.

Continue (Yes/No)

Close Ticket/Case

Activate IR Process Begin Investigation

Phishing Example



Forwards Phishing Email

5 Min. Opens Suspicious Phishing Email

15 Min. Assigns to Analyst

25 Min. Analyst Begins
- Checking Attachments (AV/Sandbox)
- Checking Links (URL/IP)

55 Min. Find All Endpoints that Received Email (AD/Splunk/SIEM/Mail Server)

2.25 Hr. Investigate Endpoints for Infection

3.5 Hr. Remediate (Firewall Block, File Quarantine)

4 Hr. Generate Leads

4.5 Hr. Finish Investigation

Security Automation – Start with High ROI Tasks

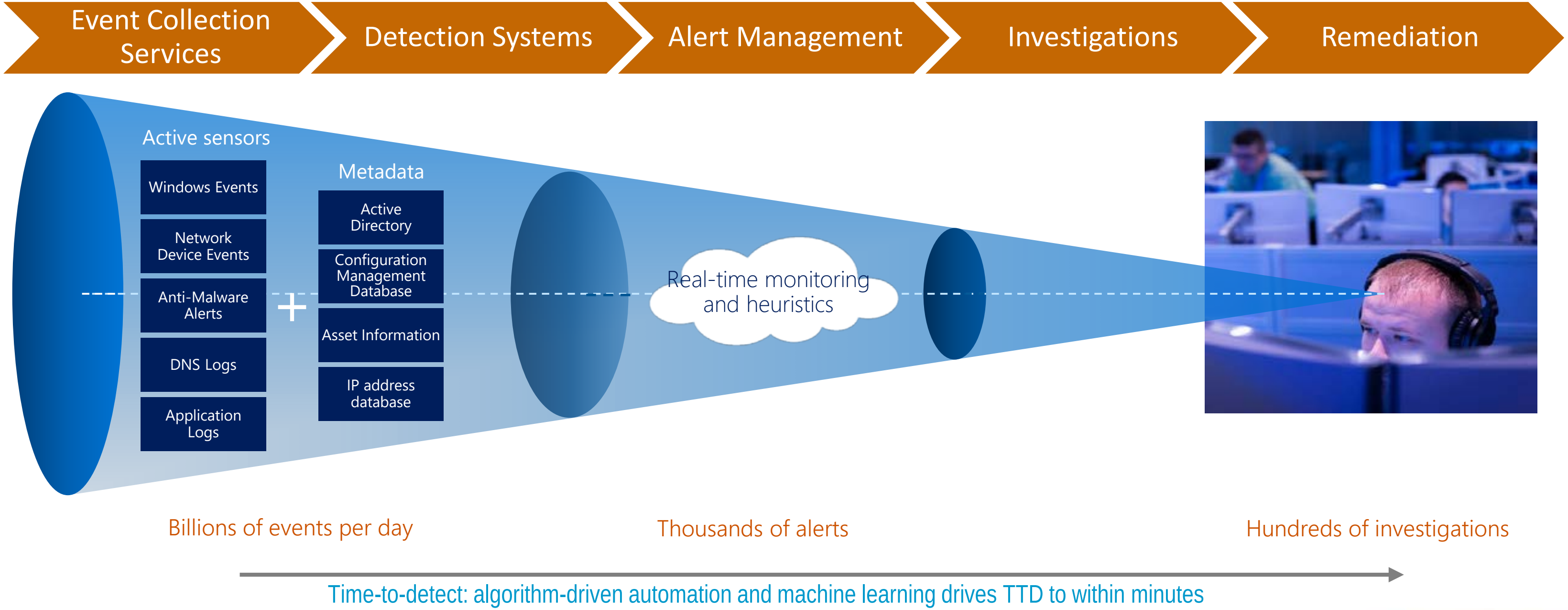
- Automate alert collection
- Automate alert prioritization
- Automate tasks and processes
  - Target common, repetitive, and time-consuming administrative processes first
  - Standardize processes and security controls within SOC

RSA Conference 2017

Singapore

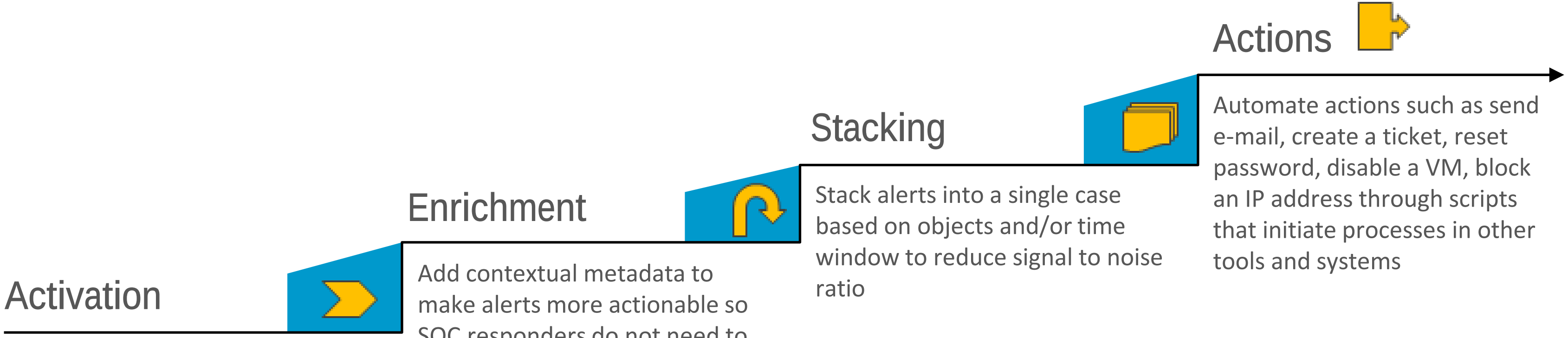
Automation in Action

SOC Event to Incident Life-cycle


Event Collection Services
Detection Systems
Alert Management
Investigations
Remediation
Active sensors
Windows Events
Network Device Events
Anti-Malware Alerts
DNS Logs
Application Logs
+
Metadata
Active Directory
Configuration Management Database
Asset Information
IP address database
Real-time monitoring and heuristics
Billions of events per day
Thousands of alerts
Hundreds of investigations
Time-to-detect: algorithm-driven automation and machine learning drives TTD to within minutes

Microsoft SOC Automation Approach

SOC Workflow Automation Components to Reduce MTTD and MTTR while Increasing # of cases/SOC defender



Activation

Enable ingestion of security alerts from multiple sources to a single case management system to enable a single queue

Enrichment

Add contextual metadata to make alerts more actionable so SOC responders do not need to access multiple tools and systems

Stacking

Stack alerts into a single case based on objects and/or time window to reduce signal to noise ratio

Actions

Automate actions such as send e-mail, create a ticket, reset password, disable a VM, block an IP address through scripts that initiate processes in other tools and systems

SOC Automation Example 1: Brute Force Attack

Activation

Alert from a detection system | Reported Incident |Invoke query on a timer on stored data

Enrichment

Contextual information from systems such as asset management, configuration management, vulnerability management and logs such as application logs, DNS and network traffic logs added

Stacking

Alert clustering to a single case based on Time-Window | Aggregation |Objects | Deduplication

Decision

Evaluate Condition | Stay on the workflow path (sequence) | Invoke another workflow

Action

Send e-mail | Create a ticket | Reset password | Disable VM | Block an IP Address

SIEM alerts on Failed Log-on Event

Multiple failed log-on events occurred

Asset Ownership Identified | Validated | Added

The owner of the asset associated with the targeted destination IP was identified an, Account validated and information added to the case

Stacking by Source IP or Destination IP

Source IP subsequent report for the same Source IP Address can be stacked in a single case for a valid account OR Destination IP Identify the target that adversary is trying to Brute Force through a bot network

Severity Reassignment and Case Designation

Change severity based on volumes for queue jumping and evaluate whether it is Brute Force or DDoS for the action playbook

Action

Automated account disablement or shut off RDP for the Source IP associated with DDoS

SOC Automation Example 2: AV Alert

Activation

Alert from a detection system | Reported Incident |Invoke query on a timer on stored data

Enrichment

Contextual information from systems such as asset management, configuration management, vulnerability management and logs such as application logs, DNS and network traffic logs added

Stacking

Alert clustering to a single case based on Time-Window | Aggregation |Objects | Deduplication

Decision

Evaluate Condition | Stay on the workflow path (sequence) | Invoke another workflow

Action

Send e-mail | Create a ticket | Reset password | Disable VM | Block an IP Address

AV Solution generates an alerts

An AV alerts was fired

Process Logs | Asset Ownership

Alert appended with the process logs to identify if malicious executables were running and impacting availability, integrity or confidentiality; Host ownership was determined from Asset Management System

Stacking by Process Name

Stacked by process name to determine the extent of AV proliferation in the environment

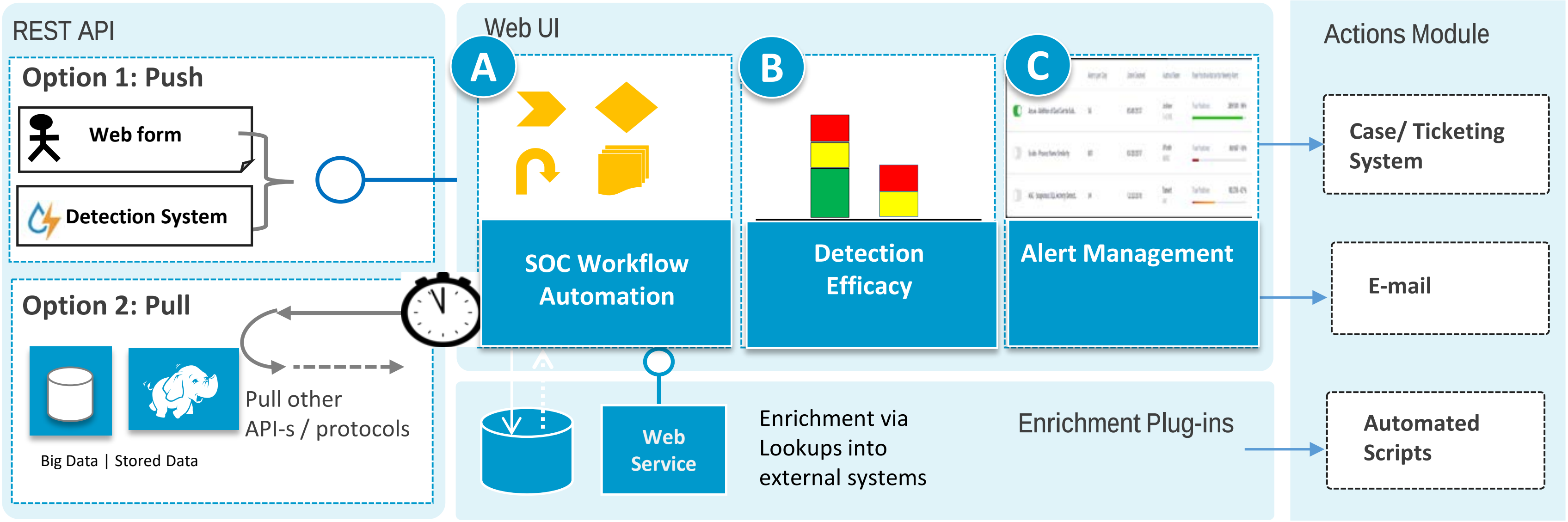
Severity Reassignment

Stacking the alerts indicated 500+ hosts were infected and it is worm proliferation

Action

Automated patching script or account disablement or new firewall rule to quarantine the environment

SOC Automation Typical Engineering Capabilities



REST API

Option 1: Push

Web form

Detection System

Option 2: Pull

Big Data | Stored Data

Pull other API-s / protocols

Web UI

A

SOC Workflow Automation

B

Detection Efficacy

C

Alert Management

Web Service

Enrichment via Lookups into external systems

Enrichment Plug-ins

Actions Module

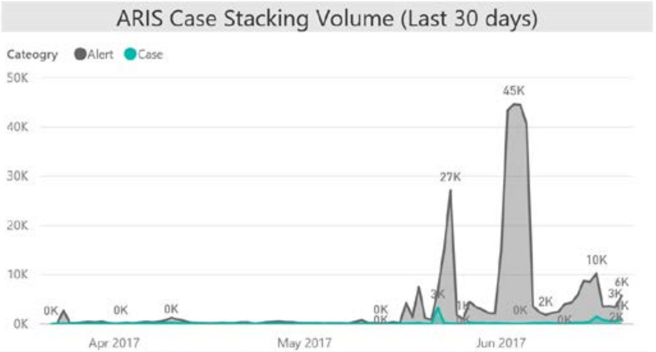
Case/ Ticketing System

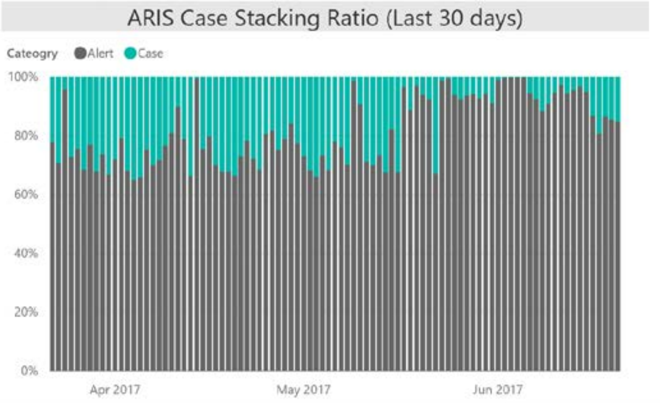
E-mail

Automated Scripts

Automated Response Investigation Service Architecture

SOC Metrics: Noise Reduction


ARIS Case Stacking Volume (Last 30 days)


ARIS Case Stacking Ratio (Last 30 days)

Microsoft

Trend with Increased Automation

Signal to Noise Ratio

Stacking Ratio: Indicator of alert to case compression

$$1- \frac{\# \; of \; cases}{\# \; of \; alerts}$$

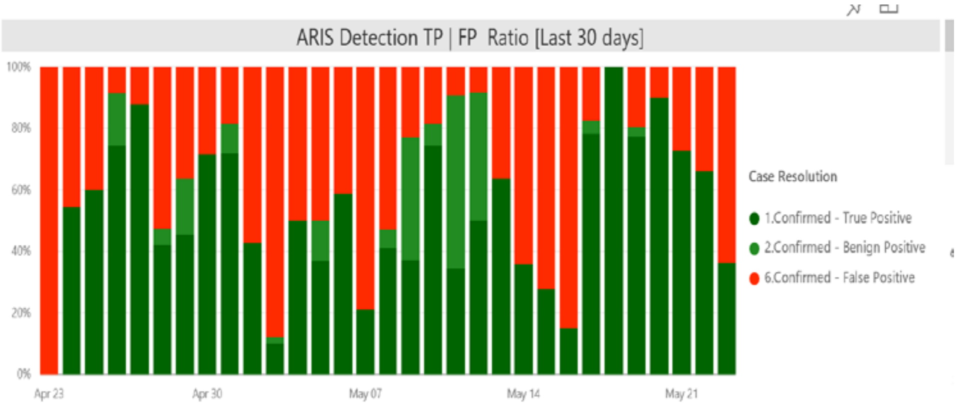
Target: 70-90% noise reduction feasible

Pivots: Alert Source, Time

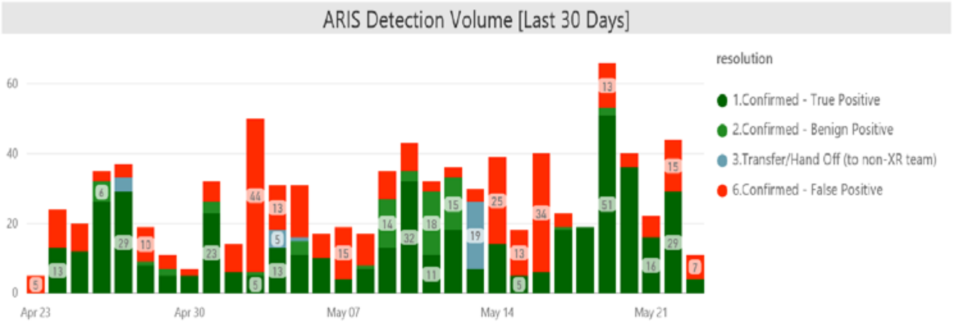
SOC Metrics: Ensure High Fidelity Signal

Efficacy	Definition
Confirmed - True Positive	Security Incident – Security Incident Response processes are invoked and executed
Confirmed - Benign Positive	Suspicious behavior detected while benign does not require action and is not expected to fire repeatedly.
Confirmed - False Positive	The event was benign in nature and is expected to repeatedly happen. All FPs result in tuning/feedback to improve signal fidelity.
False Negative	Security Incident where no alert fired and monitoring and/or detections are needed
Service Health	Alerts on the service operations or security state but not necessary a security incident

SOC Metrics: Ensure High Fidelity Signal



ARIS Detection TP | FP Ratio [Last 30 days]



ARIS Detection Volume [Last 30 Days]

Detection Efficacy

TP/FP Ratio: True positive to total alerts for a given detection and/or detection platform

$$\sum_t \frac{\#\ of\ TP}{\#\ of\ alerts} \Big/ \sum_t Alerts$$

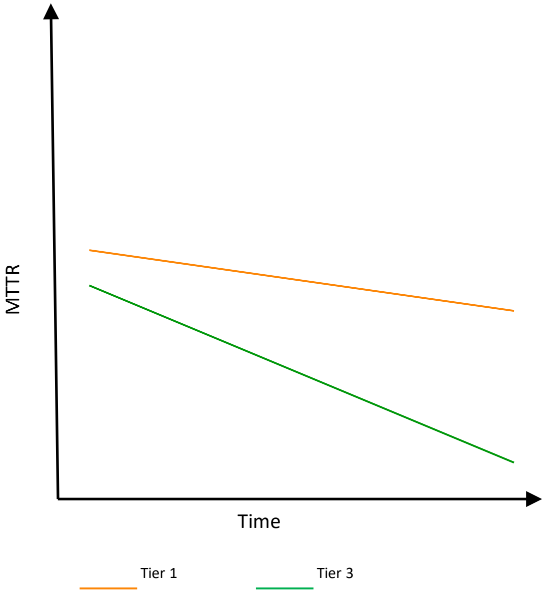
Target: >50%

Pivots: Detection Source, Time, Specific Alert ID

Microsoft

Trend with Increased Automation

SOC Metrics: Speed to Remediation



⬇ Mean Time to Remediate

MTTR: Mean Time to Resolve is the time from case creation to case remediation

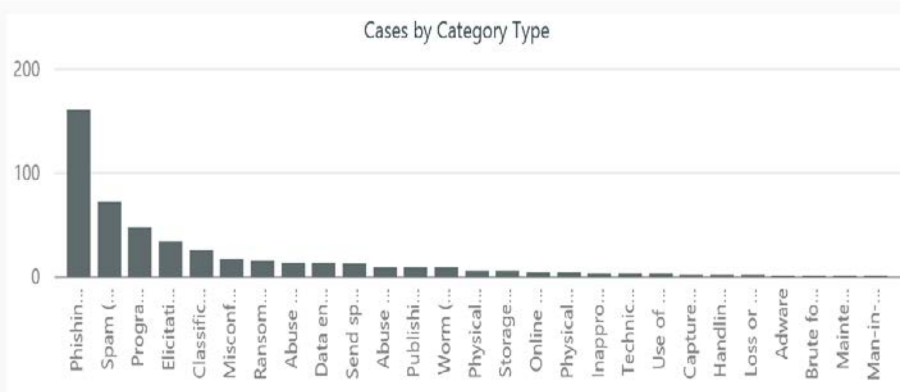
$$\frac{\sum_{All\ Cases} Time\ \ Stamp\ [Case\ Closed - Case\ Created]}{\sum \#\ of\ cases}$$

Target: Varies by severity, complexity and level of automation

Pivot: Assigned Severity, SOC Tier, Alert Source, Attack Category

⬆ Trend with Increased Automation

SOC Metrics: SOC Efficiency



⬆ **Cases/Analyst**: Automation enables SOC to do more with the same resources

⬇ **Top 10 offenders:** Automating or eliminating repeat occurrences

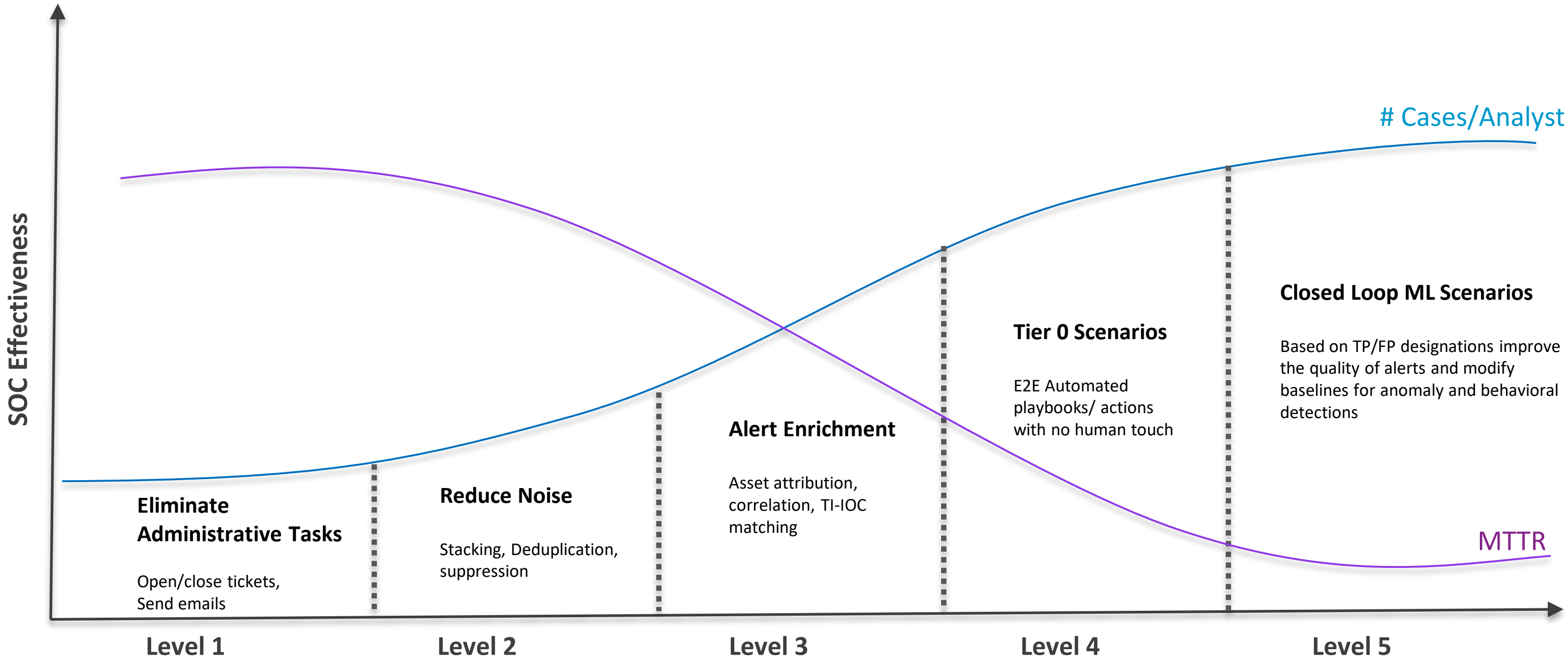
Target: Prevent and Automate top offenders

Pivots: Attack Vectors or Detections or Response Playbook

Microsoft

⬆ Trend with Increased Automation

SOC Automation Maturity Model



Eliminate Administrative Tasks

Open/close tickets,
Send emails

Reduce Noise

Stacking, Deduplication, suppression

Alert Enrichment

Asset attribution, correlation, TI-IOC matching

Tier 0 Scenarios

E2E Automated playbooks/ actions with no human touch

Closed Loop ML Scenarios

Based on TP/FP designations improve the quality of alerts and modify baselines for anomaly and behavioral detections

“Apply” what you have heard today

Within 30 days from this session you should:

- Identify common, repetitive and time-consuming tasks performed by SOC analysts
- Establish and begin measuring key SOC metrics

Within 90 days from this session you should:

- Standardize processes and procedures for responding to common attacks and alerts
- Push workloads to detectors and sensors

Within 180 days from this session you should:

- Automate alert collection, enrichment, and prioritization ensuring enterprise coverage across common attacker techniques, tactics, and procedures

Microsoft