YOU NEVER HAVE ENOUGH

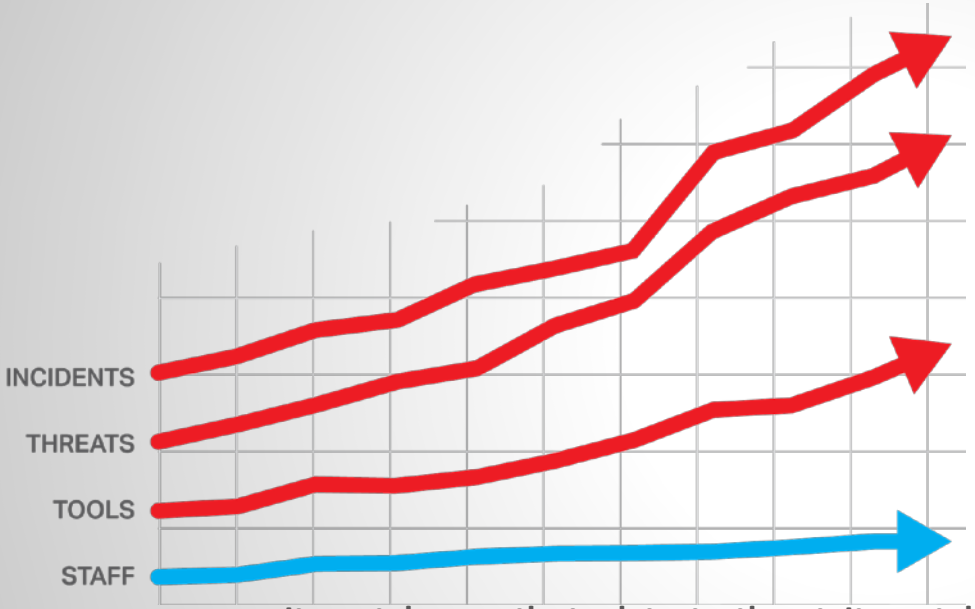
TIME

Time is an equal opportunity employer. Each human being has exactly the same number of hours and minutes every day. Rich people can't buy more hours. Scientists can't invent new minutes. And you can't save time to spend it on another day…

~ Denis Waitely

Where are we losing time today in security?

Too many…



81% say the number of security events increased or remained the same in 2013.*

The number of tools and their complexity continue to increase.

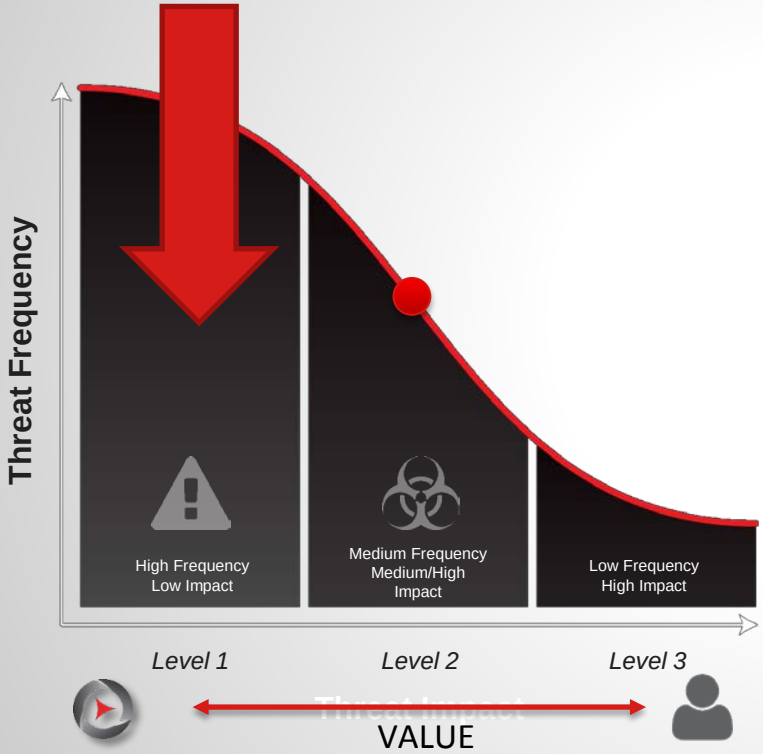
Staffing levels remain the same to slightly higher.

It can take months to detect a threat. It can take days, weeks or months to resolve it.

The longer it takes, the more you are exposed.

* Survey by IDG Research on security automation: info.csgi.com/idg-survey/

Too Much Time on Noise and Low Value Tasks



Level 1: False Positives, Self-Inflicted Wounds…

- Mundane, trivial and repetitive, and time-consuming events that distract your teams with low value returns

Level 2: Sweet Spot for Compromise

- Moderate frequency events that pop up every few weeks or months that have a significant impact on the business

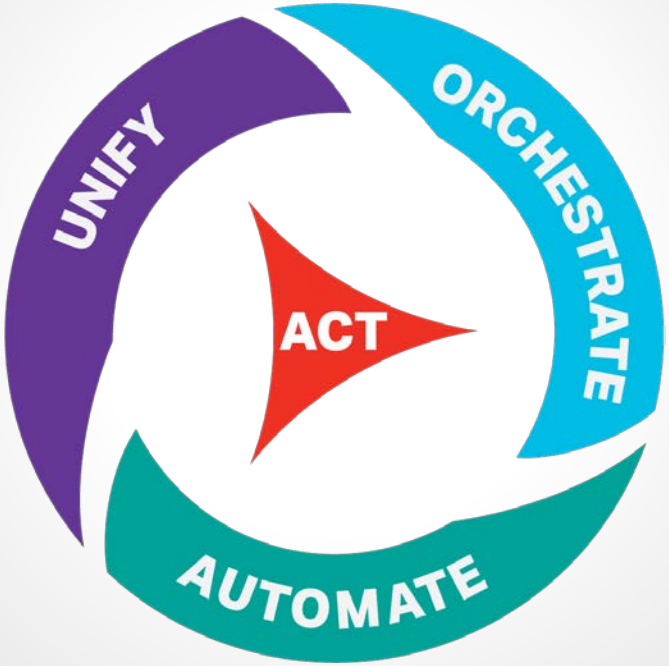
Level 3: Zero-Days and Natural Disasters

- Needle in the hay stack that is hard to detect or just one of those crazy once in a lifetime natural disasters

Security Orchestration and Automation Model

UNIFY
Your Defenses

ORCHESTRATE
Your Response



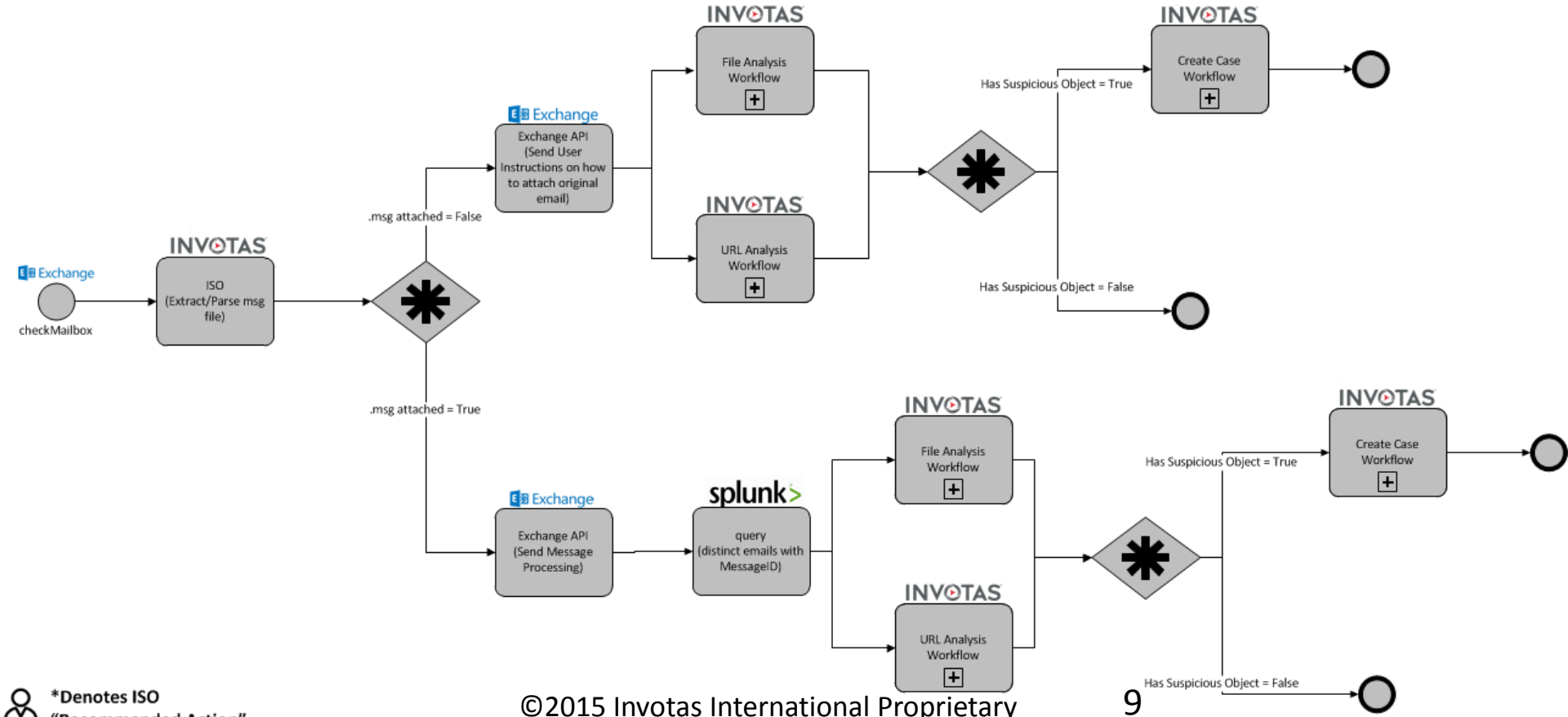
AUTOMATE
Your Win

ACT
With Confidence

Problem Statement – Abuse Mailbox

- Most organizations instruct employees to forward suspicious emails to IT Security – often called “abuse@customer.com”
- Most security teams have dedicated staff and tools assigned to process these emails
- Each email takes between 45 - 60 min for an analyst to process
- Workflow Phases:
  - Email Ingest
  - File Analysis
  - Sending Notifications/Creating Tickets

Abuse Mailbox – Message Ingest Sample



*Denotes ISO "Recommended Action"

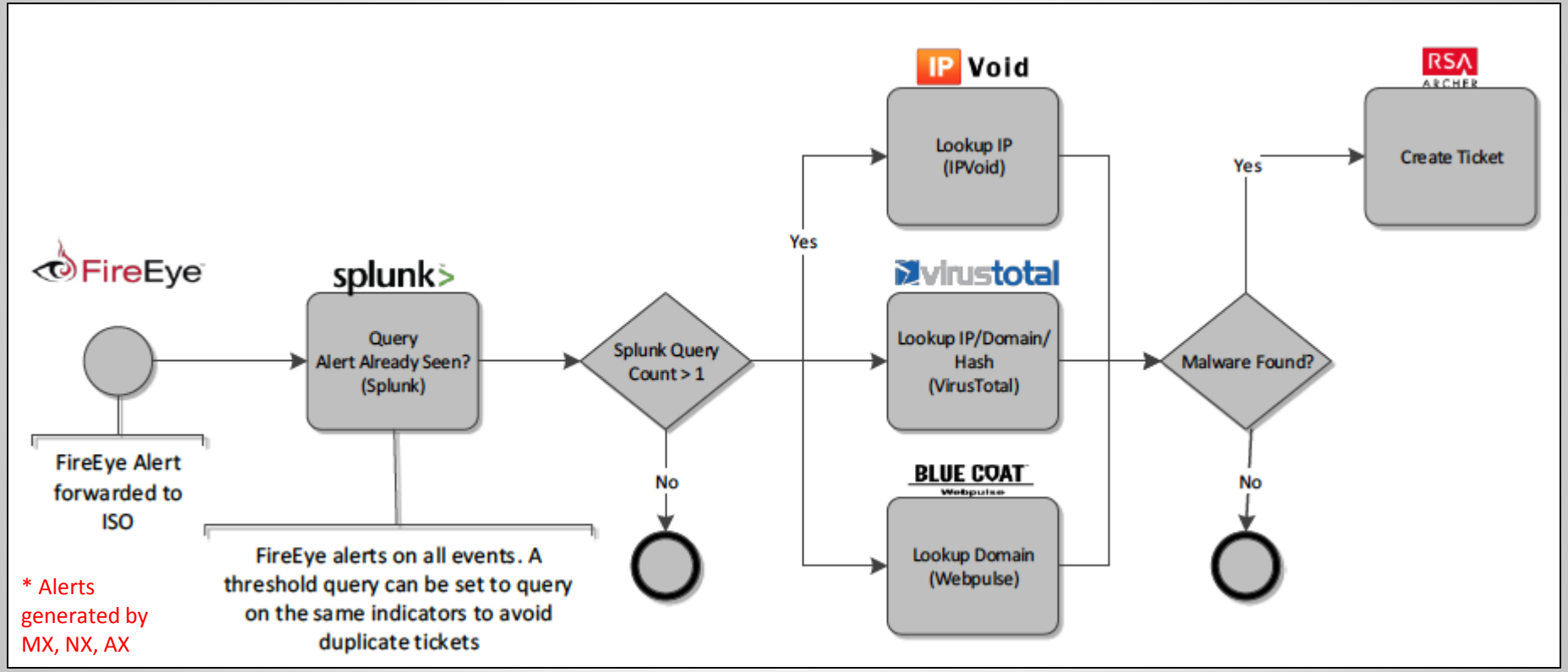
FireEye Alert Management

Financial Customer receives FireEye alerts from the network (NX), email (MX), and sandbox (AX) appliances. Most FireEye alerts require manual data enrichment tasks to be completed before they can be classified as actionable incidents. On a typical day, there are around 40 actionable FireEye alerts with an average of 20 minutes to research the alert and
create a summarized ticket within the Archer platform.

Workflow Phases:

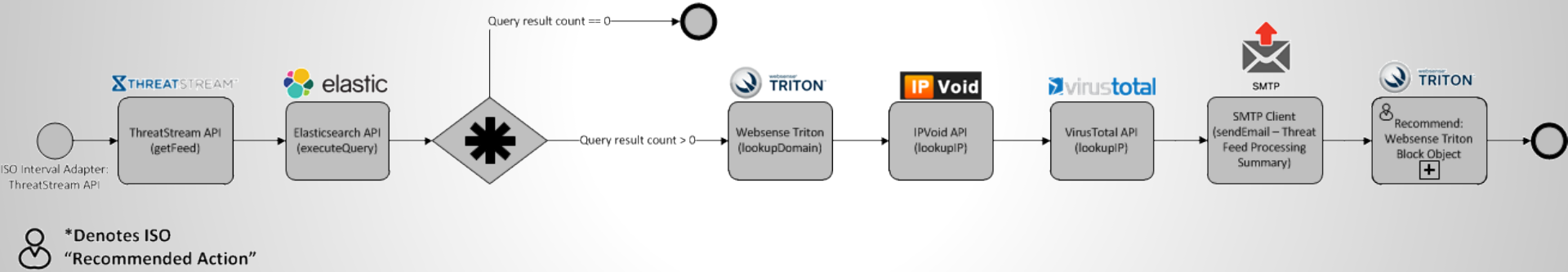
1. Monitor FireEye CMS for new alerts
2. Enrich alert specific indicators such as IP addresses, domain names, hashes, etc. in third party tools such as the following: BlueCoat Webpulse, DomainTools, IPVoid, Norese IPViking, URLQuery, VirusTotal
3. Validate that alerts are actionable based on enriched indicators received via step 2.
4. Compile enrichment data and artifacts and generate a new Archer ticket.

FireEye Alert Management



INVOTAS.IO

Intel Processing



INVOTAS.IO

Where to start with Security Orchestration and Automation?

- High Frequency
- (Repetitive Actions)

- Low Impact / Low Risk Regret

- Known Trigger
- (Alert or Business Objective)

- Known Outcome