MENA
INFORMATION SECURITY
CONFERENCE 2018

Leveraging Machine Learning & AI in Cyber Defense

Fahad I. Aljutaily
Cyber Security VP, STCS

Changing the Game with Orchestration

VIRTUPORT

@VirtuPortMEA

www.menaisc.com

Security Challenges are Compounding

EVOLVING THREATS

$3 Trillion
Expected global cost
of cybercrime by 2021

LACK OF VISIBILITY

70+
Apps to manage

SKILL SHORTAGE

3.5 Million
Unfilled cybersecurity jobs by 2021
75% YOY increases

Operational Challenges

Resources

Resource ***shortage of 1 million*** security professionals

Products

Endless assembly line of point products

Alerts

Escalating volume of ***security alerts***

Static

Static independent controls with ***no orchestration***

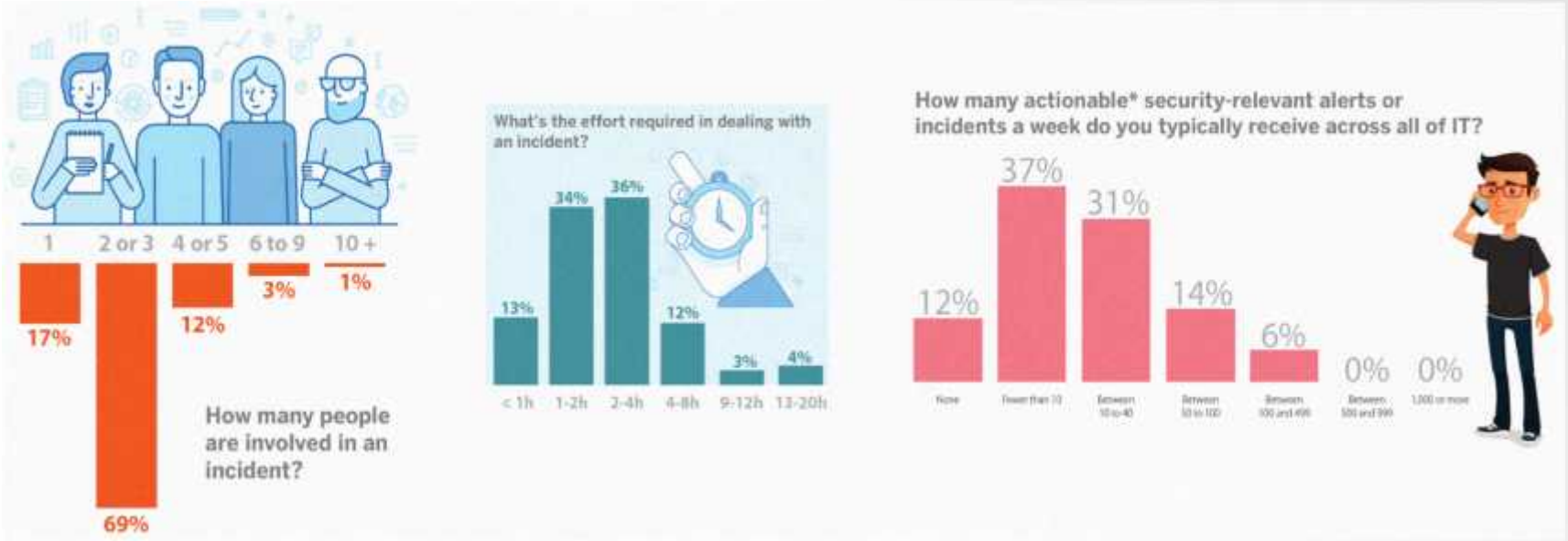
Speed

Speed of detection, triage, & response time ***must improve***

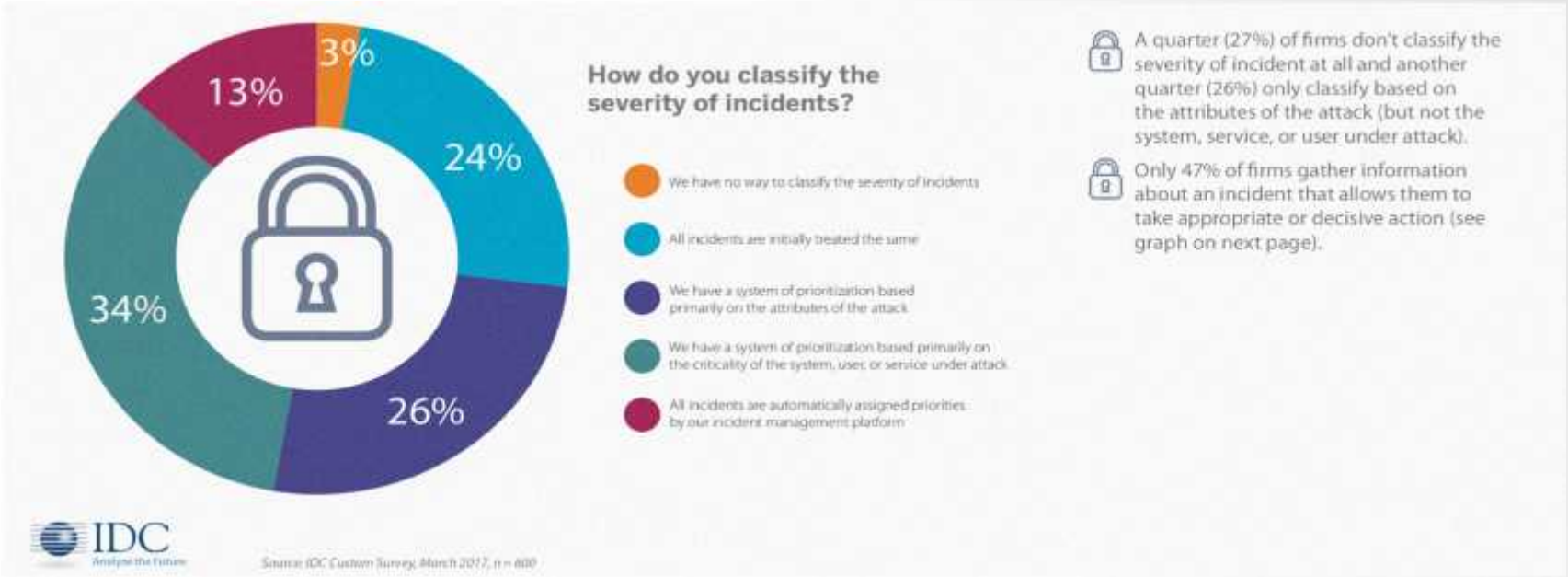
Costs

Costs ***continue to increase***

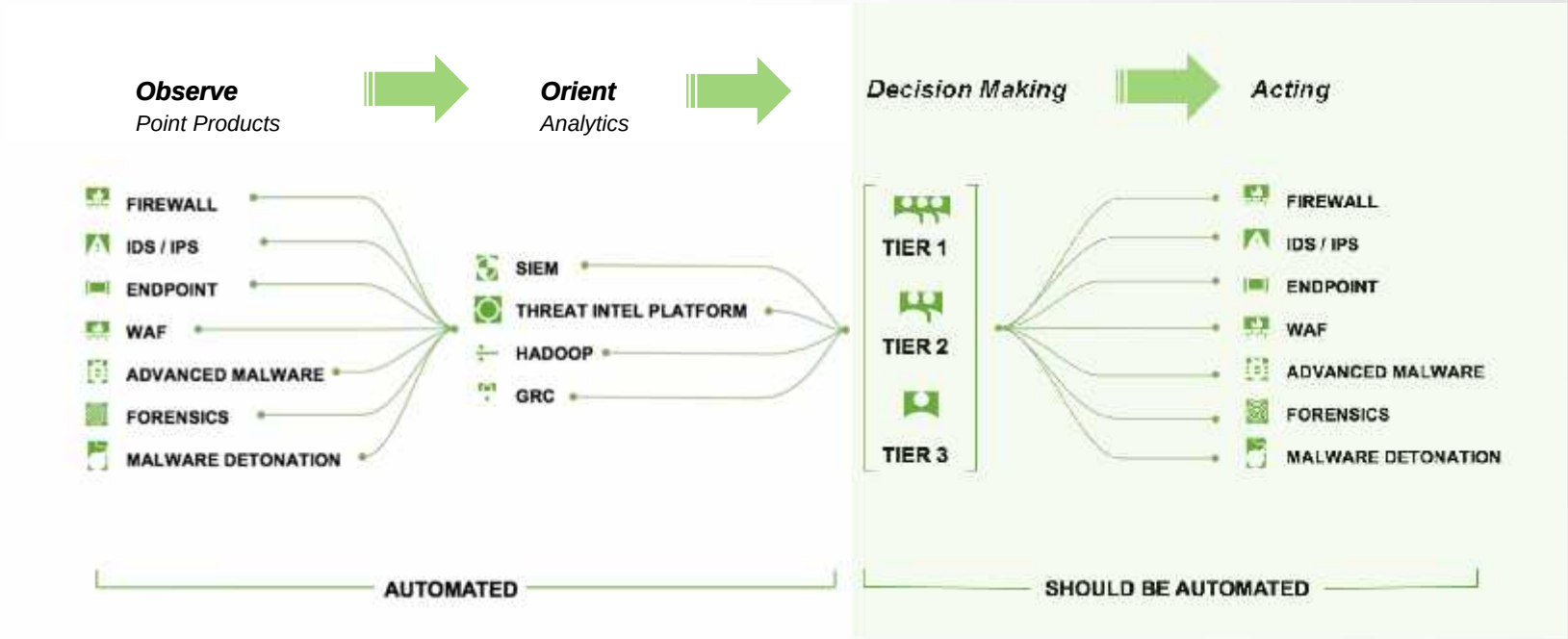
Security Analysts are Overwhelmed



We're Failing to Operationalize and Prioritize



Partial SOC Automation Today



** Decision Making consumes most of the Analyst time*
***Acting is the riskiest*

Market Trends

Security Strategy Reliant on Data Strategy

Demand for Automation and Adaptive Response

Shift From Prevention to Detection and Response

Convergence of IT and OT

Analytics and Machine Learning for Threat Detection

SOAR

"By Year-end 2020, **15%** of Organizations with a security team **larger than five people** will leverage SOAR tools for orchestration and automation reasons, up from **less than 1%** today."

Gartner, November 2017, SOAR Report

MENA INFORMATION SECURITY CONFERENCE 2018

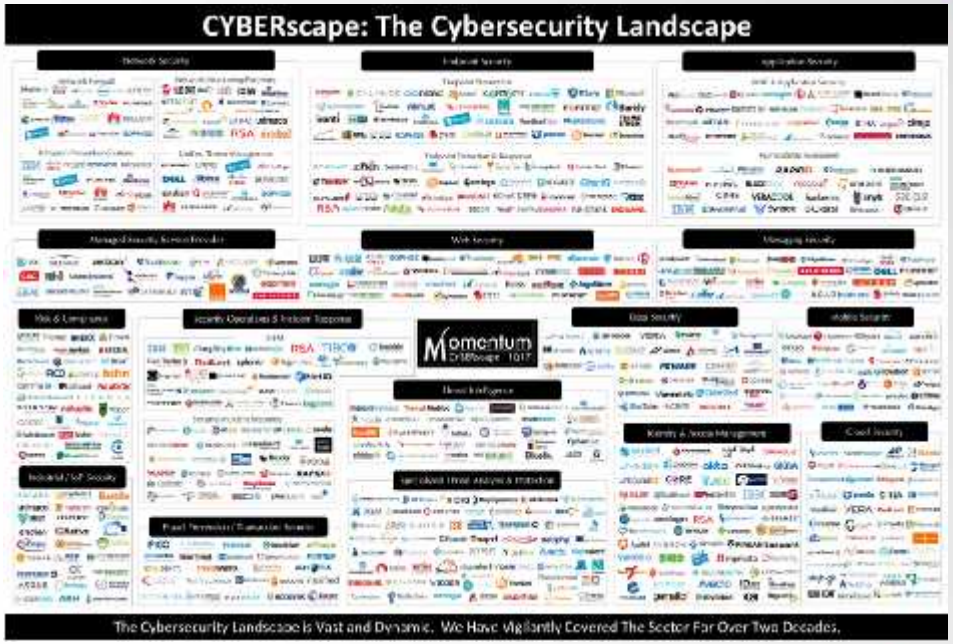
What is a SOAR?

SOAR = Security Orchestration, Automation & Response

Security Orchestration *is the machine-based coordination security actions across a complex infrastructure.*

Security Automation *is the machine-based execution of security actions.*

Security Response *refers to the policy-based coordination of human and machine-based activities for vent/case/incident workflows.*



SOAR Use Cases…

Operations

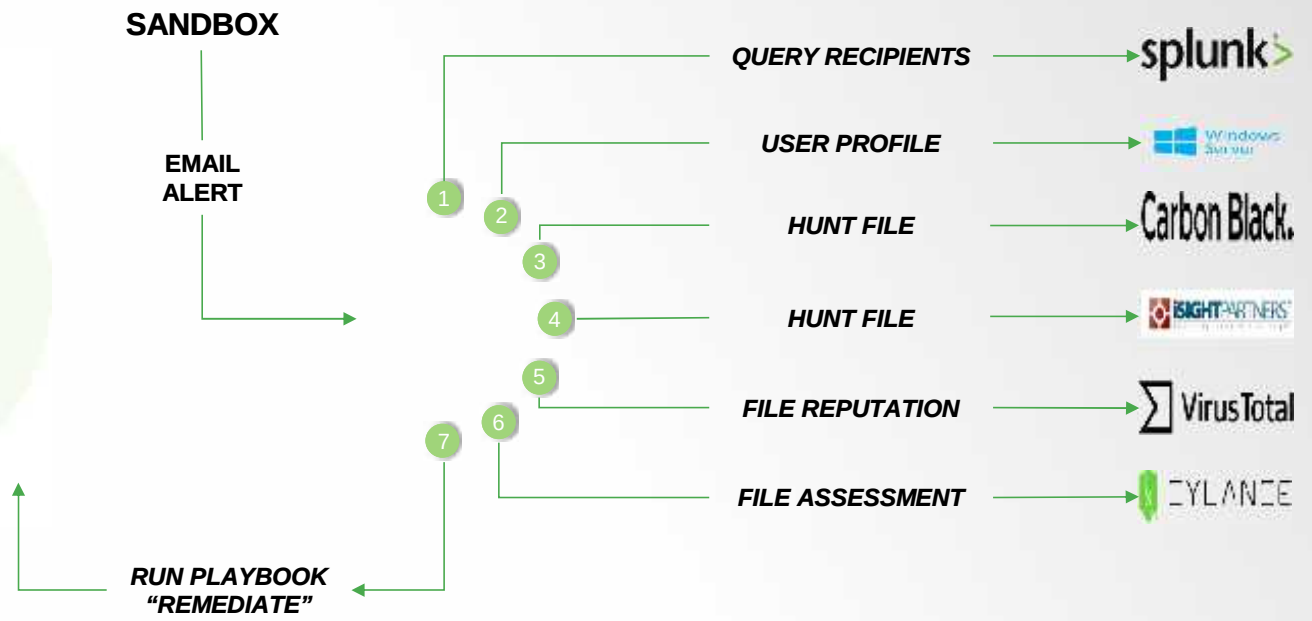
- *Phishing Investigation*
- *Threat Hunting*
- *Threat Intelligence*
- *Malware Investigation*
- *Event Triage*
- *Insider Threat Team*

Management

- *Team Performance*
- *Process & Operations*
- *Metrics & Reporting*

Use Case – Malware Investigation

With SOAR, a malware investigation process will take few seconds vs. a typical 30 to 60 minutes



Re-imagine the SOC

50%

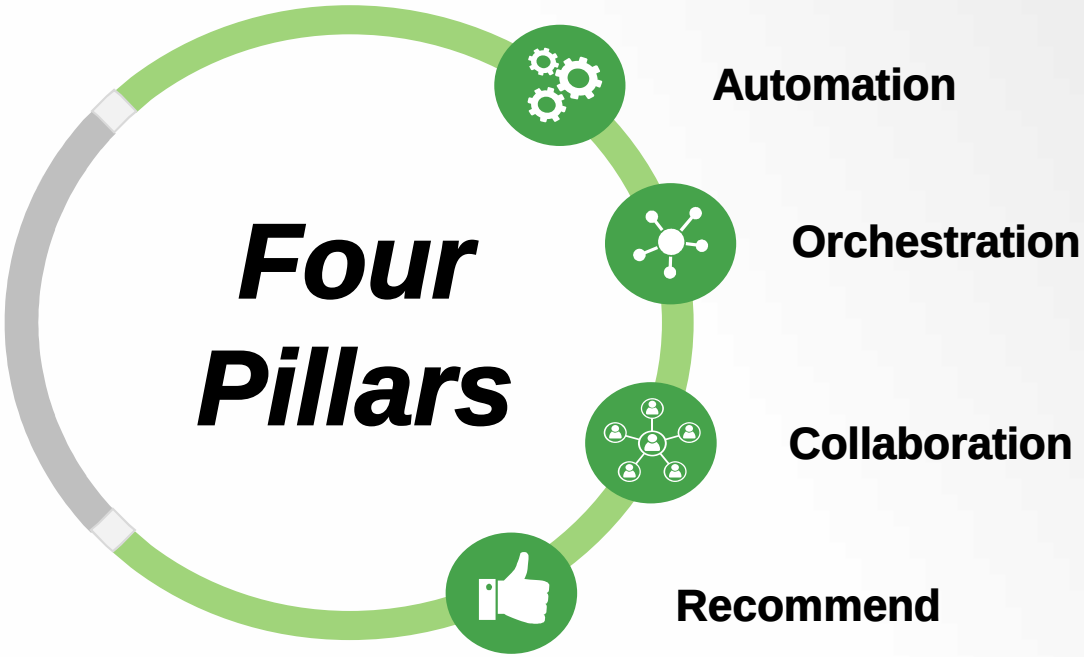
TIME will be on SPENT TUNING DETECTION AND RESPONSE LOGIC

90%

TIER 1 ANALYST WORK WILL BE AUTOMATED

MENA INFORMATION SECURITY CONFERENCE 2018

Tomorrow's SOC Starts Today



MENA INFORMATION SECURITY CONFERENCE 2018

A multinational Food Production Company hit by a Ransomware Attack – caused *$150 million* loss

Detect Early

Recover Fast

MENA INFORMATION SECURITY CONFERENCE 2018

with SOAR = Security Orchestration, Automation & Response

THANK YOU

MENA
INFORMATION SECURITY
CONFERENCE 2018