Efficient SOC Operations to Tackle Persistent Cyber Threats

Jason Hartley
Global Executive, Threat Detection and Response

Matthew Ambrose
Senior Manager, Threat Detection and Response

DAFITC 2023

IBM Consulting Cybersecurity Operation Centers provide global visibility and diverse expertise to our clients

1700+
Clients delivered from global, regional and local delivery centers

~2 Million
Endpoints & log sources monitored and managed

180 Billion
Logs and events collected and processed daily

2800+
Global security professionals

Global Operations

7 SOC locations operating as one

4 geo specific SOCs operating independently on dedicated platforms

We create and curate the talent pool; role-based curriculum, reskill/upskill courses, mentoring & cohorts, 10,000+ hours of training delivered annually

Our clients benefit from ready access to a core talent base operationally ready to face today's evolving threats

Our Employee Value Proposition is the keystone of our retention strategy

Best in IBM
Employee engagement score: 91% would recommend IBM Security to their friends and family as a great place to work

Deliver both 24x7 and "follow the sun" models to enable seamless delivery from on-shore, near-shore and off-shore resources

Global Certifications: ISO 27001 / 27017, PCI DSS, SSAE-16 SOC 2 Type 2, FFIEC, and Privacy Shield compliant

How does our platform power our threat management services?

SECURITY CONTROL MANAGEMENT

THREAT MANAGEMENT

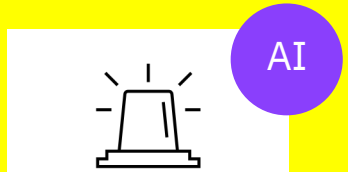
Health & Availability	Policy & Config	Disposition	Investigation	Action
Are the controls healthy, available and current (patches/services)?	Are we watching for the right threats? Will the control properly protect & detect?	What is the best way to handle this attack investigation... Auto-escalate? Close as false positive? Raise for investigation?	Which business processes are potentially impacted by this attack? Can this attack... Spread? Exfiltrate data? Deny service operation?	How do we contain this attack? Can we prevent something like this from happening again?
Device Monitoring & Management 80+ Vendor Platforms Health Alert Correlation Ansible Runbooks	Threat Detection Insights (TDI) Coverage: MITRE ATT&CK Effectiveness Scoring SPEAR Report	Advanced Threat Disposition Scoring (ATDS)	SOAR Threat Intelligence ServiceNow	SOAR ServiceNow Ansible Runbooks

IBM X-FORCE PROTECTION PLATFORM (XFPP)

Our insights drive our actions

Innovation in Action

We have applied AI to automate the investigation of 73% of alerts



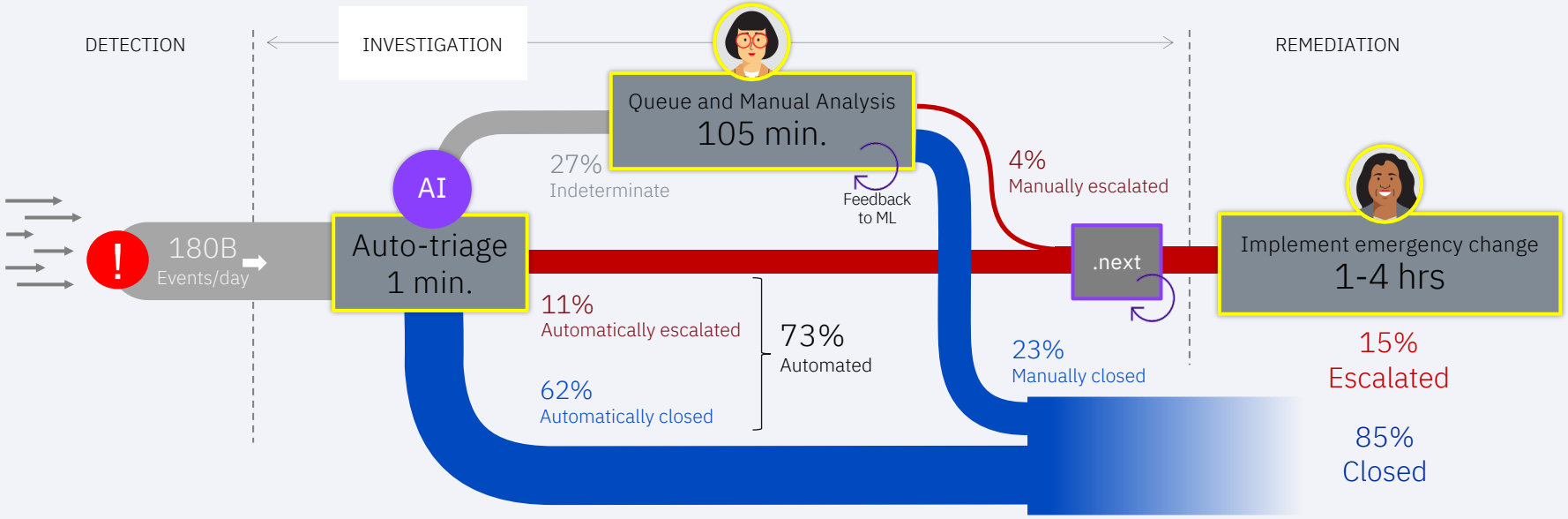
Objective

Triage alerts based on context, severity, and risk

Classify alerts

Recommend disposition

Explain triage decision



Models

- 4 models learn from past alert parameters, historical analyst's disposition
- Rare Event model identifies anomalous behavior
- The ensemble model provides disposition recommendations on new alerts with confidence and explanation

Training

- Learned from 2+ million alerts over 1 year
- 30+ security technology platforms
- Unique learnings for Network, SIEM, EDR telemetry, and analyst past disposition
- Diverse industry data; i.e., manufacturing, FSS, etc.
- Continuous feedback from analysts through audit

Results

- 73% automated at a 90%+ confidence level
- 27% manually processed
  - 23% reviewed by analysts and closed
  - 4% response recommendation after review

Next steps

95% automated:

- Auto-escalate to clients with explanation and reasoning
- Improved confidence through intel enrichment, continuous learning of manually closed and escalated alert

Threat Detection Insights
X-Force Protection Platform
Live Demo