Security Operations:
Moving to a Narrative-Driven Model

Josh Goldfarb – VP, CTO - Americas
Despite $30B spent on cybersecurity every year, 97% of organizations are breached.

- 67% learn they are breached from a third party
- $3.5M average cost of a breach
- 32 days to respond to a breach on average
- 229 to detect the breach
229 DAYS
MEDIAN NUMBER OF DAYS BEFORE DETECTION

67% OF COMPANIES LEARNED THEY WERE BREACHED FROM AN EXTERNAL ENTITY

100% OF VICTIMS HAD FIREWALLS OR UP-TO-DATE ANTI-VIRUS SIGNATURES

SOURCE: MANDIANT M-TRENDS REPORT
ATTACKERS UTILIZE MULTIPLE VECTORS AND MULTIPLE FLOWS TO COMPLETE THEIR MISSION
CONTINUOUS SECURITY MONITORING
So Many Important Questions

- How long have I been under attack?
- How many endpoints are infected?
- What was the extent of the damage?
- What are the Indicators of Compromise?
Challenges: Alert-Driven Detection Model

1. Alerts lack context, making accurate and timely detection difficult
   - Snapshot, moment in time
   - Limited context, “straw” view
   - One detail, not the whole story

2. Forensics technologies lack performance for immediate response
   - Manual context-building
   - Not timely
   - Precise data extraction challenging
Putting Together the Story: Narrative Driven Security

Did the attack succeed?
What else can I learn about the attack?
**Endpoint**

Where is the attack destined?
Do I see artifacts of intrusion?
**Network**

What does the complete picture look like?
What is my exposure?
**Forensics**
COMPONENTS THAT BUILD THE NARRATIVE

TECHNOLOGY

INTELLIGENCE

EXPERTISE
How?

• Identify risks, goals, and priorities
• Identify gaps in telemetry
• Develop content
• Improve signal-to-noise ratio
• Concentrate into unified work queue
• Enrich with supporting evidence
• Automate common analysis steps
• Interleave intelligence
• Present the narrative
THANK YOU

@ananalytical