

Network Visibility and Proactive Threat Hunting with Network Detection and Response

Carl Bolterstein, Director of Product Management, NDR

June 22nd, 2022

How Network Detection and Response (NDR) Empowers Cyber in ever evolving environments

Visibility is basis of everything

- Cannot see what you are not monitoring
- Commoditize data collection across all platforms
 - Traditional enterprise network
 - Cloud
 - Container native
 - Borderless enterprise
- Leverage visibility to build novel detections
- Reduce complexity of monitoring

Analyze Everything or Tactical?

- Analyze Everything
 - Pros
 - Ensures nothing is missed
 - Largest possible dataset for hunting
 - Cons
 - Largest possible data..
 - Dimensioning returns of collecting more vs usable
- Tactical
 - Pros
 - Starting with reduced noise to be as targeted as possible
 - Reduce cost to process data in both human and computing
 - Cons
 - May miss something
 - Will you have enough to influence new detections

Threat Hunting in a modern enterprise

- Proactively look for malicious activity on the network
- May not know where traffic is going
 - What is truly external?
- Hybrid computing platforms
- Heavily dynamic environments
 - Cloud
 - Container
- How do you influence detections

Building the attacker minefield

- Moving beyond the blocking mindset
- Network visibility is key for knowing where threats come from
- Influence automated responses to threats
- Map novel detections to stages of attacks

The background is a deep blue with several glowing, curved lines that intersect and radiate from the right side towards the left. Small, bright white and light blue dots are scattered along these lines, creating a sense of motion or a network. The overall aesthetic is modern and technological.

Questions?