The Evolution of Network Detection & Response

What's Network Detection and Response (NDR)?

VISIBILITY

- TLS Decryption
- Metadata
- Deep Sessions Inspection/ Deep Packet Inspection
- All Ports and Protocols

DETECTION

- Machine Learning Capabalities
- Heuristics
- Yara Rules
- Signatures
- IOCs from Threat Intelligence Feed

RESPONSE

- Predictive Response
- Retrospective Analysis
- Proactive Capabalities
- Automated Investigation
- Incident Analysis

How Evolved is your Network Security?

Basic Network Security

FIREWALL

- Firewalls are preventive
- Signature/ rule based
  - Covers port, protocol, and Source | Destination
- Requires heavy administration for policy changes
- Lack response capabalities

Intermediate Network

IDS vs IPS

- Lack response capability
- Requires additional security tools for correlation analysis
- Signature and possibly anomaly-based detection

Advanced Network Security

FIDELIS NETWORK DETECTIONS AND RESPONSE (NDR)

- Only combination NDLP and NDR in the market
- Powered by machine learning
- Rich metadata capture and analysis
- Deep Sessions Inspection
- Proactive threat hunting

The Benefits of Fidelis NDR

RAPID VISIBILITY DETECTIONS & RESPONSE

Provides visibility across all ports and all portals

Monitors and Analyzes north/-south traffic and east/west traffic

Leverages machine learning and analytics to detect network traffic anomalities

Provides rich metadata that enables retrospective detection and analysis going back many months

Provides metadata on TLS traffic

Integrated with Fidelis Endpoint to automate relevant response actions based on what has been detected