



Two Eyes Open

How Network Detection & Response brings perspective to Security Operations

Owen Edwards

Director, Network Product Management

Oct 22, 2024



Owen Edwards

Director, Network Product
Management



OSI Model



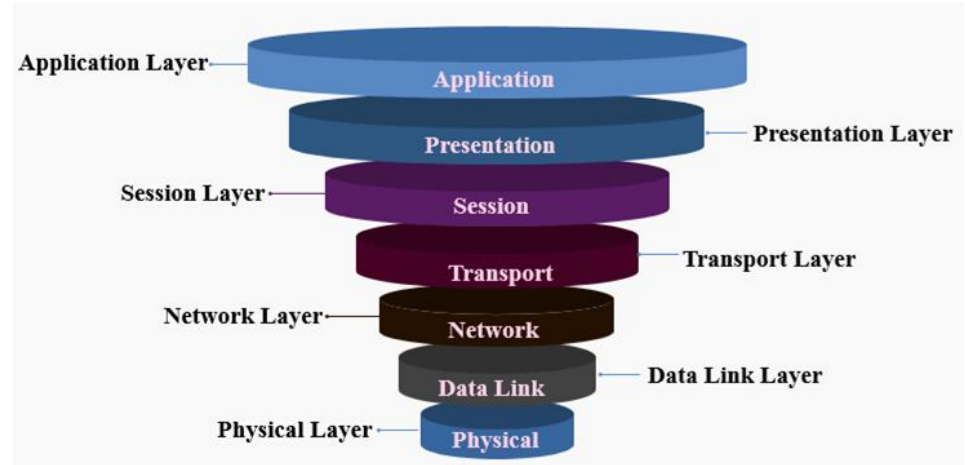
"The common basis for the coordination of standards development for the purpose of systems interconnection."

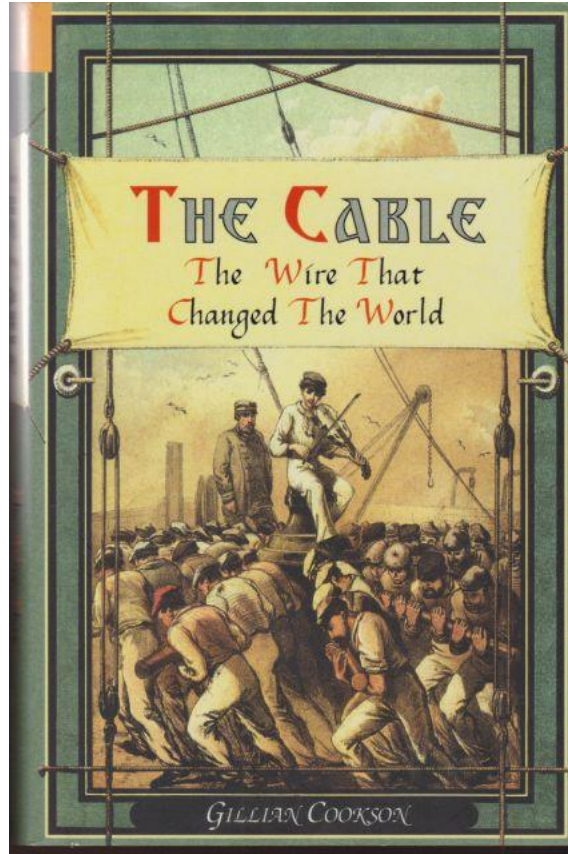


OSI Model



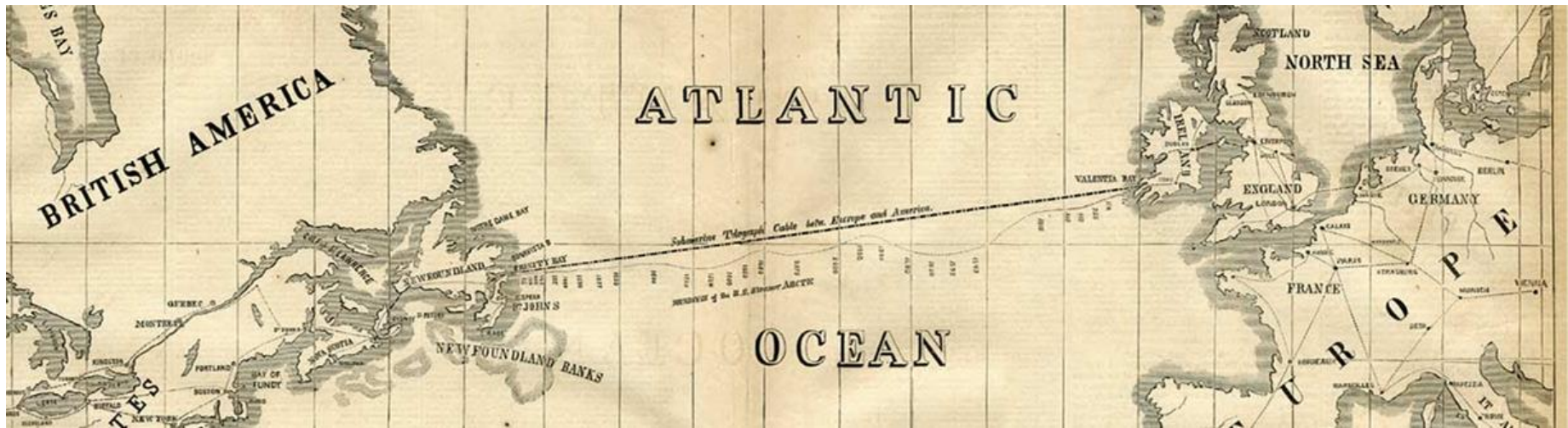
"The common basis for the coordination of standards development for the purpose of systems interconnection."





The Cable

The Wire that Changed the World



Internet 1858

0.066 bits per second

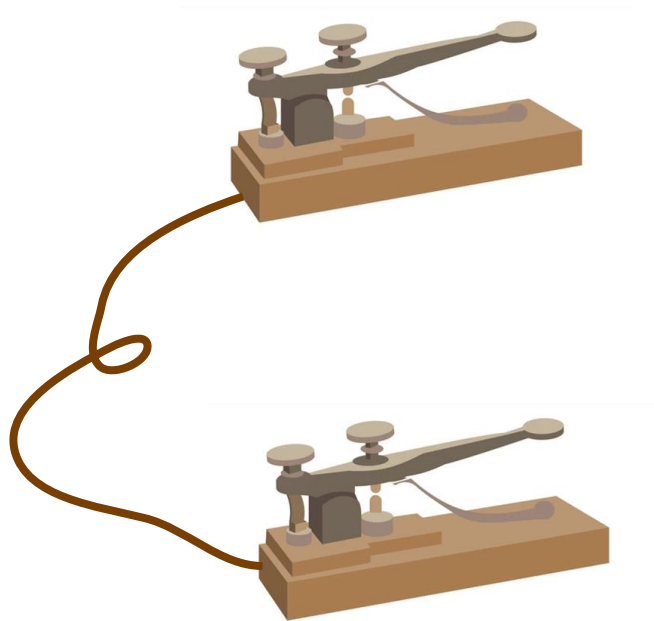
Network Attack



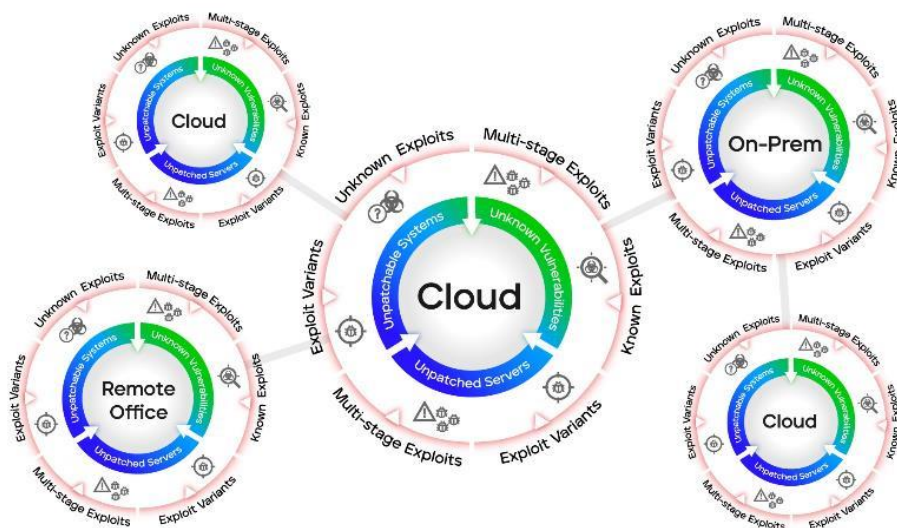
Secure Your Assets



Easy!



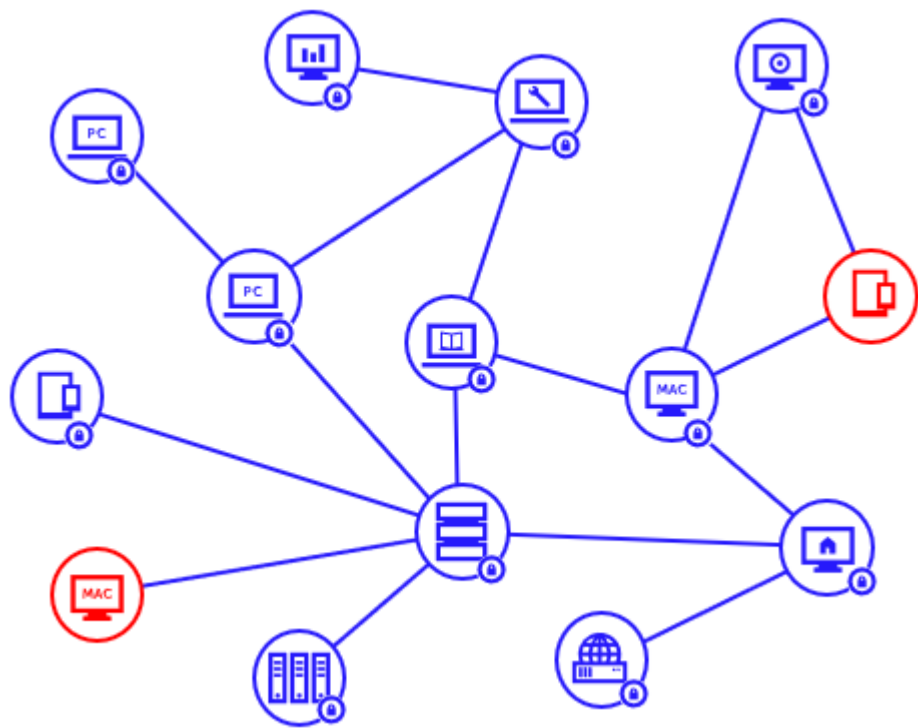
Secure Your Assets



Somewhat Harder!

Network Detection & Response

Security Operations Perspective



Blind Spots

NDR Gets Rid of Them

Analyst Efficiency



NDR Makes Analyst
More Efficient





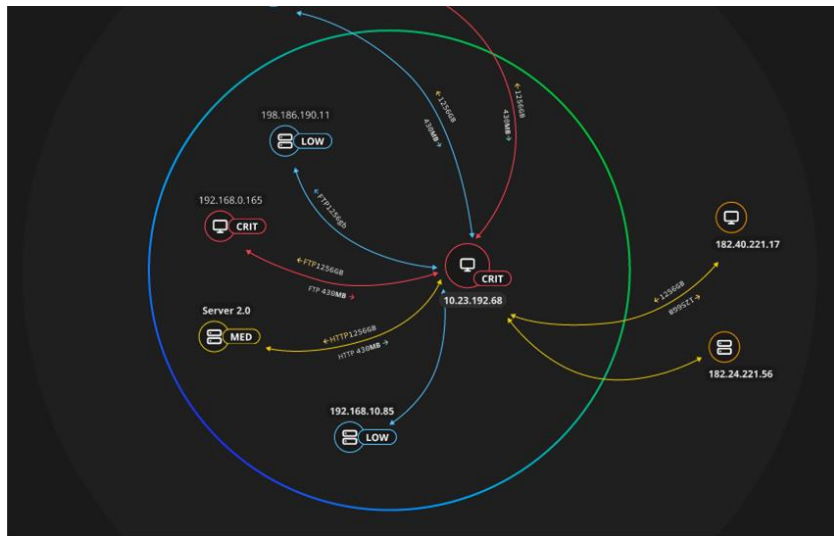
NDR and EDR

NDR enables key SOC playbooks:

- Discover unmanaged endpoints and IOT devices
- Identify suspicious file transfer
- Determine potential compromised devices
- Rapidly scope an incident
- Identify lateral movement attempts



The perfect complement for making security operation more efficient



Respond Faster

Network Shows Where the
Attacker Is



Trellix NDR

Empowering each organization to secure and defend based on continuous visibility into their entire digital footprint

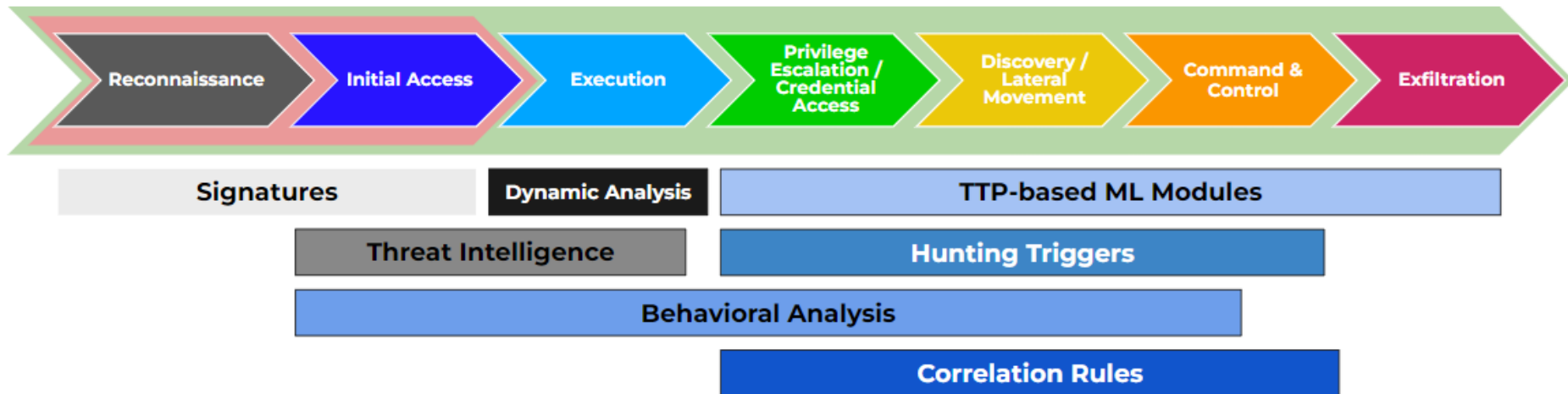


Trellix

Trellix NDR Approach: Threat Model

Traditional Network Perimeter Security

Trellix Network Detection and Response

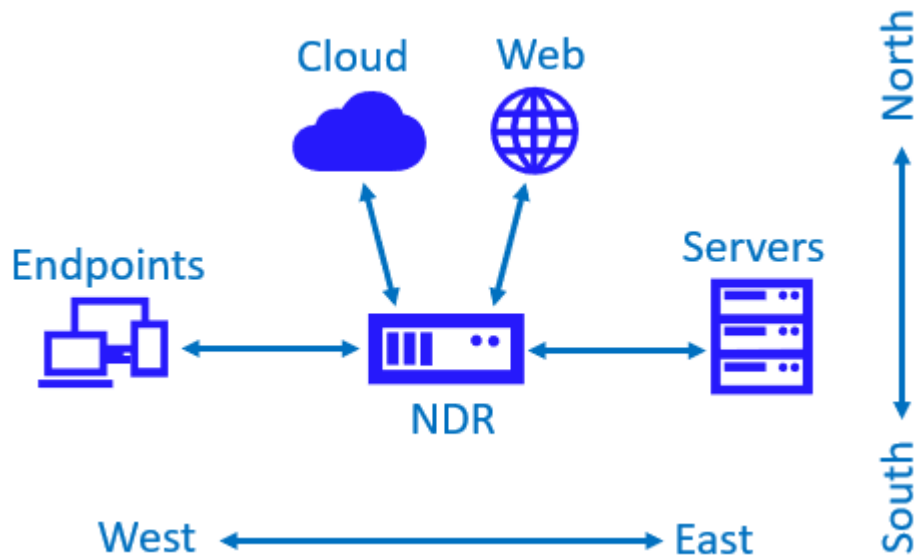


Focus on specific attacker behaviors, beyond just looking for anomalies, ensuring high-fidelity alerts

Trellix NDR Approach

E-W & N-S Focus

Determine the
Intent

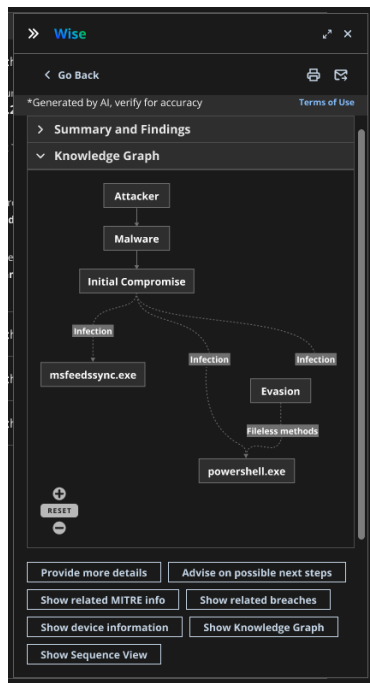


Detect Threats within the Internal Network Traffic,
not just at the Perimeter

Trellix NDR Approach

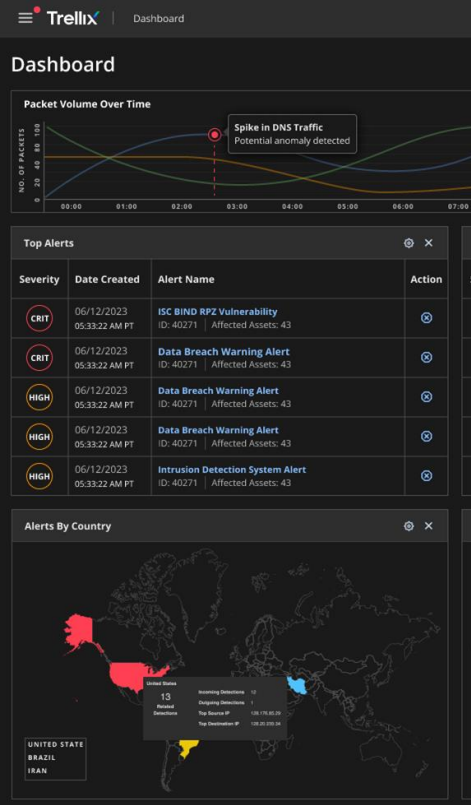
GenAI

SOC Efficiency



Guided Investigations

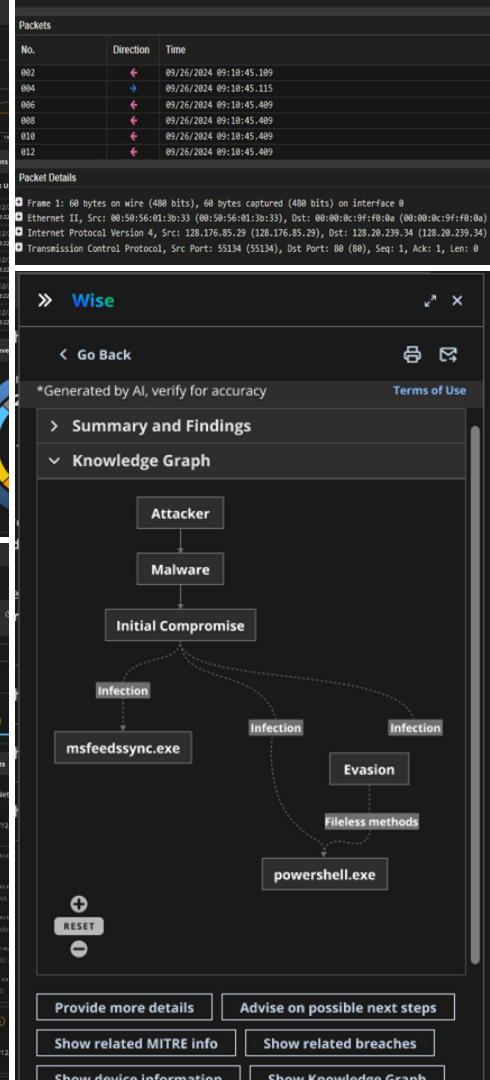
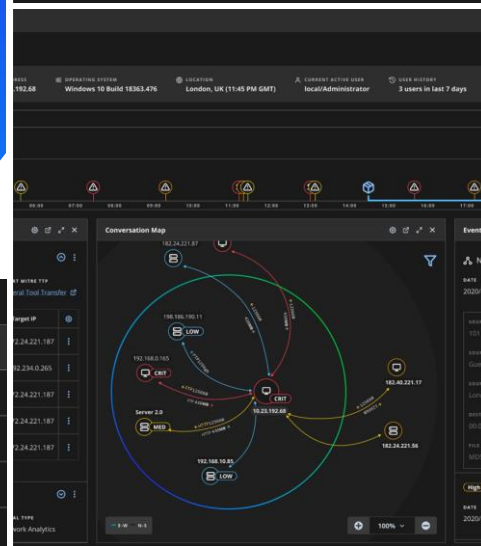
Context



Trellix NDR

- Better Visibility
- Better Detection
- Better Investigation
- Better Response

Assets: All			
	Severity	Last Updated	Asset name
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Local-Hostname-10.Au
<input type="checkbox"/>	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK





Trellix