Trellix

Trellix Native XDR

So schützen Sie sich vor Ransomware

October 11, 2023

Today's Presenter

Josef Gillhuber

Senior Solutions Engineer, CISSP

Trellix

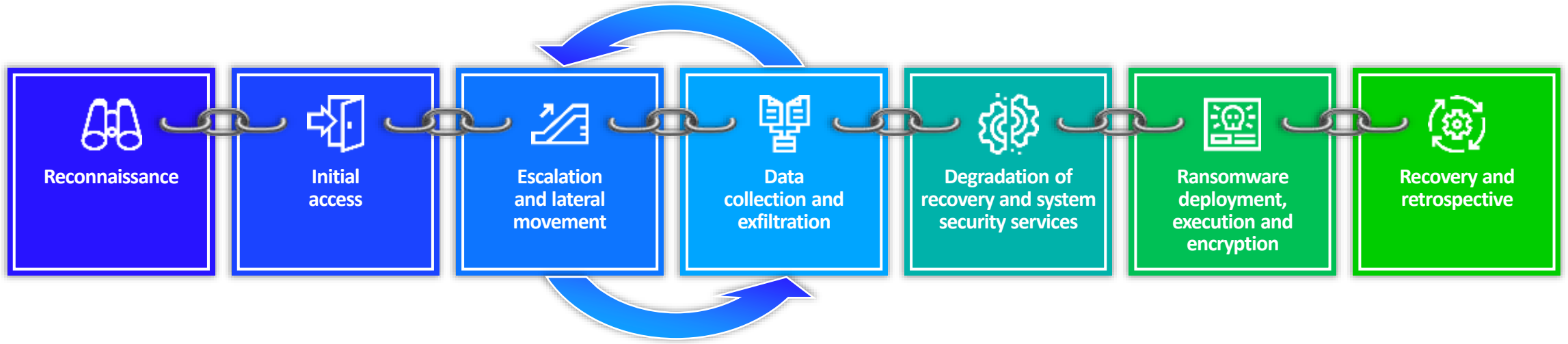
Agenda

- Anatomy of an Attack
- Ransomware Defence
- Trellix Native XDR

Trellix

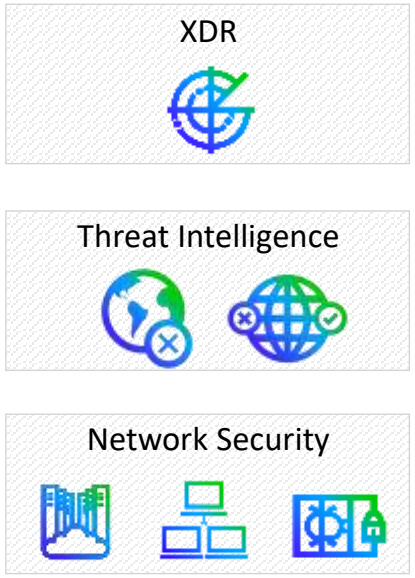
The Phases of a Ransomware Attack

Trellix Ransomware Kill Chain



Trellix

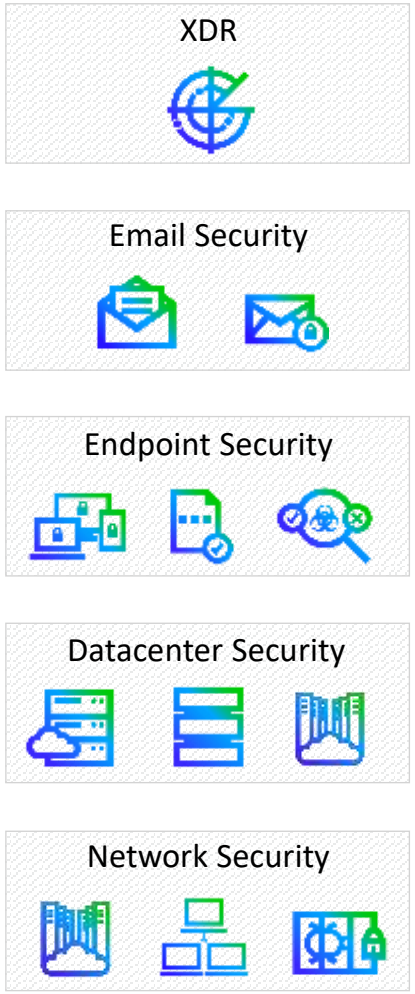
Reconnaissance



- Gather Victim Org Information - T1591
- Phishing for Information - T1598
- Active Scanning - T1595

Trellix

Initial Access

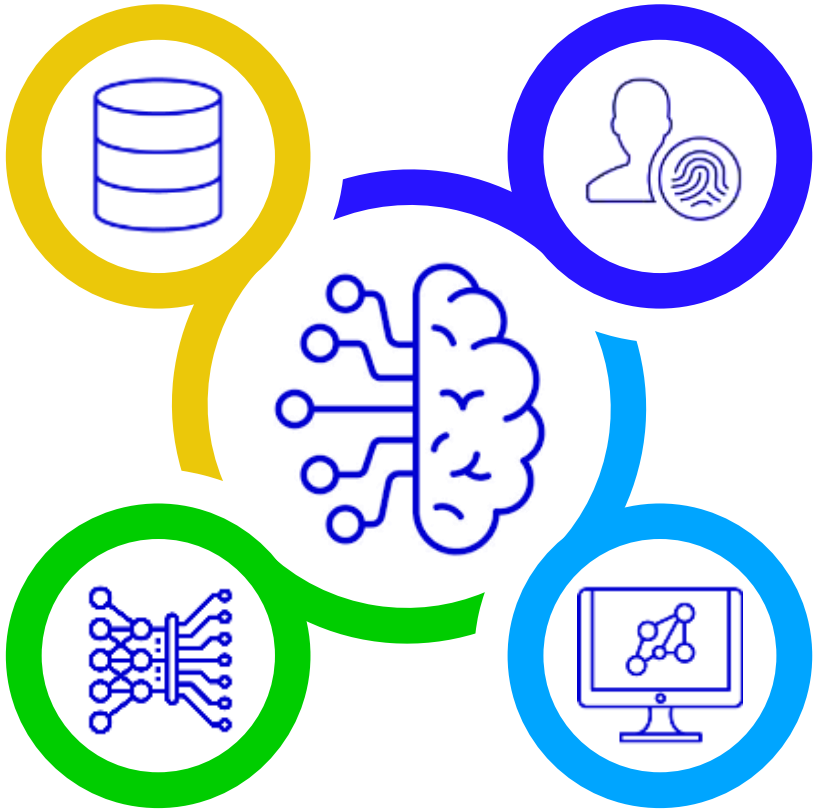


- Valid Accounts-T11078
- Phishing–T1566 (Phishing Kits)
- Exploit Public-Facing Application-T1190 (Metasploit)
- Drive-by Compromise-T1189 (RIG)
- Remote Desktop Protocol-T1021.001 (NLBrute)

Trellix

What do you need to do Machine Learning well?

Massive data set
Persistent and relevant data collection from >40,000 global customer, technology partner, and service provider networks



Security researchers
Determine what to look for based on known threat actors, current campaigns, or ttps

ML algorithms / models
+10 years investing in machine learning to detect the threats that matter

Data scientists
Translate research finding into workable models. Supervise, train and tune the models to ensure low false positives

Trellix

XDR Market Guide

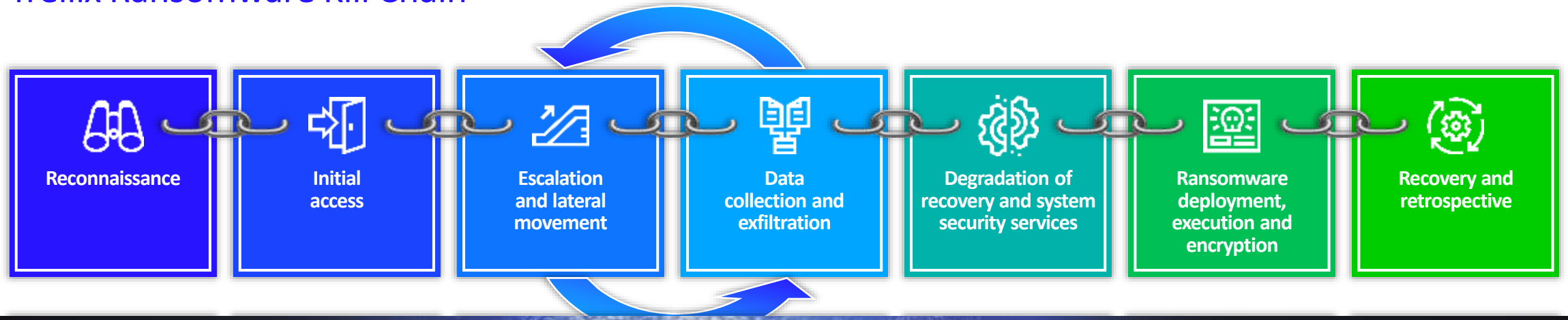
- “…minimum of two native security sensors,…”
- “…Converge Security Products to a Single Vendor with Prebuilt Integration…”
- „…Operationalizing Threat Intelligence…“

Source: Gartner: Market Guide for Extended Detection and Response: https://www.gartner.com/doc/reprints?id=1-2EOYTQA6&ct=230811&st=sb

Trellix

The Phases of a Ransomware Attack

Trellix Ransomware Kill Chain

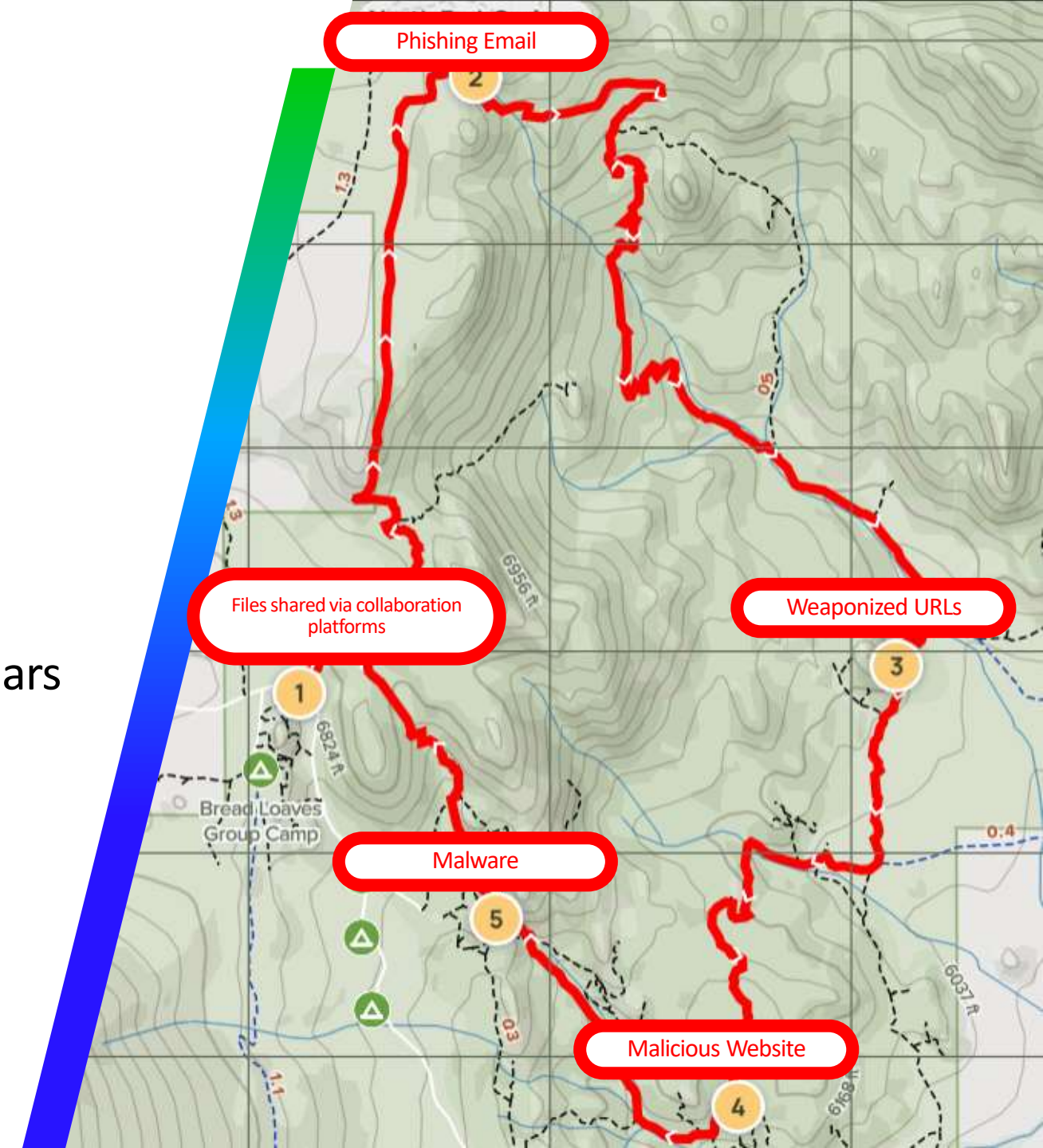


Key Take Aways

Good enough security won't protect you from ransomware

'Detection-in-depth' is our heritage, we've invested 10+ years in AI/ML models

Add Trellix Email Security to detect what others miss



Thank You

Trellix