Vision: A World Safe for Exchanging Digital Information

1988
Peace of mind computing

1998
Your Internet Virus Wall

2008
Securing Your Journey to the Cloud

2018
Securing Your Connected World
Today: Value Creation from Massive Data

Big data collection and analysis used for direct value like better service or advertising (e.g. Facebook, Google, Amazon)

A → B
Today: Data Often Collected/Analyzed in Silos
Today: Data Often Collected/Analyzed in Silos

Connected, extended value creation → more efficient, cost-effective, safer city!

A + B + C = D
Example: AI-enabled Security Operations Center

A + B + C = D

Cyber Security Problem
Important to Enable Service Providers as Part of Strategy for SOC

Customers may choose multiple approaches to address their needs.
Building a connected data lake to enable AI

Hunting platform
AI/Machine Learning To Discover unknown threat

SOC-compliant
REST APIs/SDK Log Export STIX/TAXII SIEM App Ticketing

Each Product Requirements

Cross Products Hunting Luwak

Hybrid Cloud DS Server Hunting

Network Hunting TP/DD

Endpoint Hunting OFSC/iES/Safelock/TMIC

Account based Hunting CAS/TMCat/HES

TM Threat Intel Services
3rd Party Feeds
3rd Party Feeds

Trend backend Hosted MISP

CTD Orchestration TMCM

STIX/IOC

SIEM, Data Lake, CLM Threat intelligent management/IOC life cycle management

SOAR None Trend security products

SOC Management tools None Trend Specific

Advanced CTD Receive and report IOC sweeping to TMCM

SOAR

SI Monitoring IOC sweeping Command issue and reports consolidate For Trend products

For Trend products

3rd Party Feeds

For Trend products

STIX/IOC

MISP

3rd Party Feeds

SOC-management tools None Trend Specific

TM Threat Intel Services

3rd Party Feeds

3rd Party Feeds

SOC Management tools None Trend Specific
Building a Connected Organization for Securing a Connected world

\[ x = i + u - t \]

- Architects, Market intelligent, engineering, devops, AI
- Consume, SMB, Enterprise, VLE, Service Provider, government...
- Threat researcher, Threat operation team, ERS, WRS, FRS, Vulnerability researcher, Exploit researcher,
Connected Organization for securing connected world