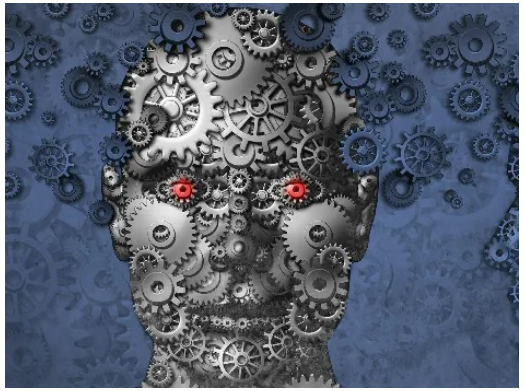
IT and OT Convergence: Risk, Reward, and Automated Response

MERIDIAN COOPERATIVE

THREAT LANDSCAPE



https://www.emsisoft.com/en/blog/29220/ransomware-as-a-service/
https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/
https://www.firstpost.com/tech/news-analysis/newbie-hackers-are-using-openais-chatgpt-generative-ai-bot-to-write-dangerous-malware-11951952.html

THREAT LANDSCAPE

- POTUS has called for sweeping changes in the critical infrastructure
- TSA regulatory requirements for airports, pipelines, and rail
- FERC has called for NERC CIP updates
- EPA will gain power to enforce cyber security requirements

Increased controls

- Continuous monitoring and detection of critical assets
- Prevent, detect, and respond to cyber threats
- Email protection
- Anomaly detection and response
- Log retention
- Network segmentation

D. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:

1. Capabilities to—

a. Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;

[10] This policy should be compliant with the most current version of the National Institute of Standards and Technology's Special Publication 800-63, Digital Identity Guidelines (available at https://csrc.nist.gov/publications/detail/sp/800-63/3/final).

b. Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;

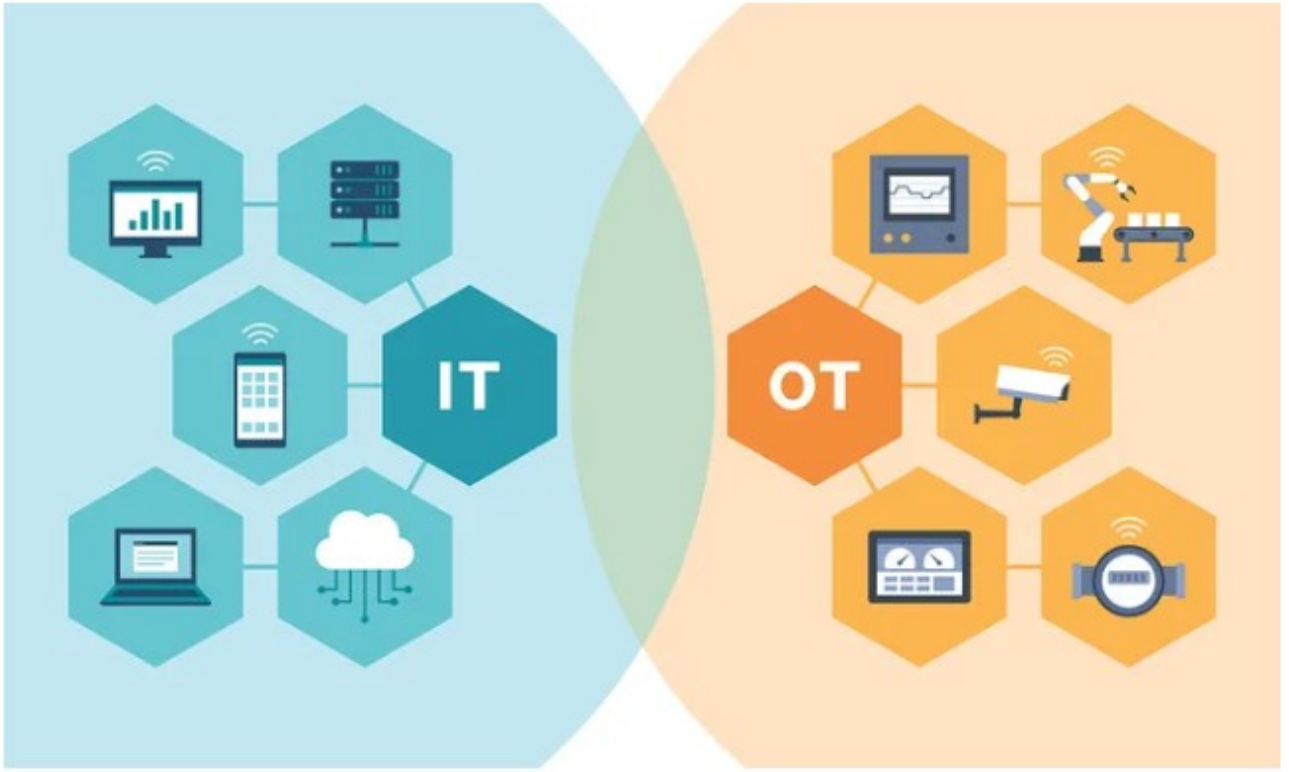
c. Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;

d. Block and prevent unauthorized code, including macro scripts, from executing; and

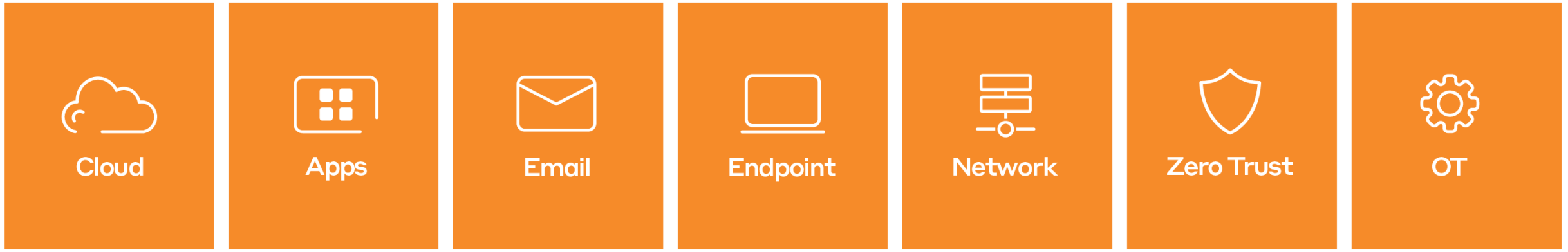
e. Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).

IT & OT Convergence

- Cloud-hosted Email
- Email remains a primary attack surface
- IT and OT networks have become porous
- Monitoring IT without OT and Email introduces visibility gaps



Visibility needs



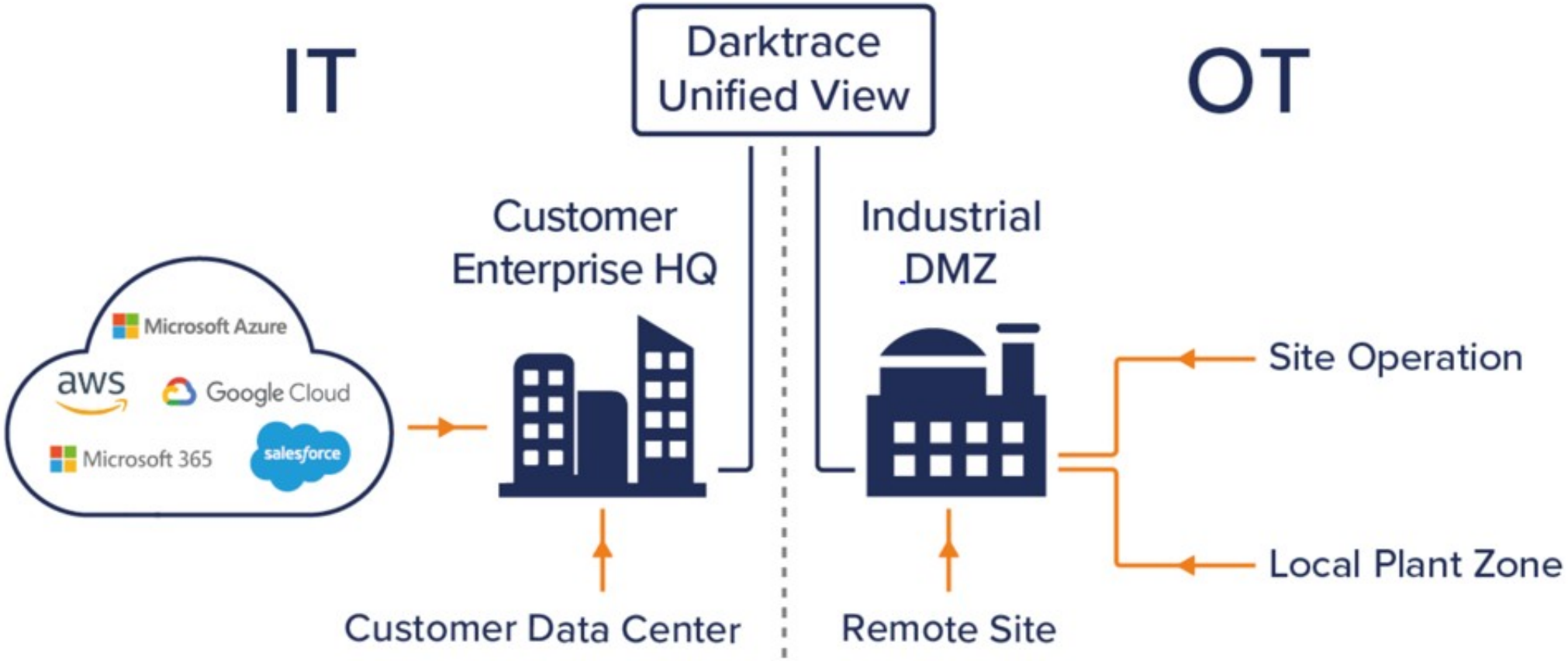
Google Cloud Dropbox slack zscaler The Cloud Security Company CROWDSTRIKE Office 365 box salesforce

aws okta DUO Microsoft Azure PAS Google Workspace CISCO SentinelOne

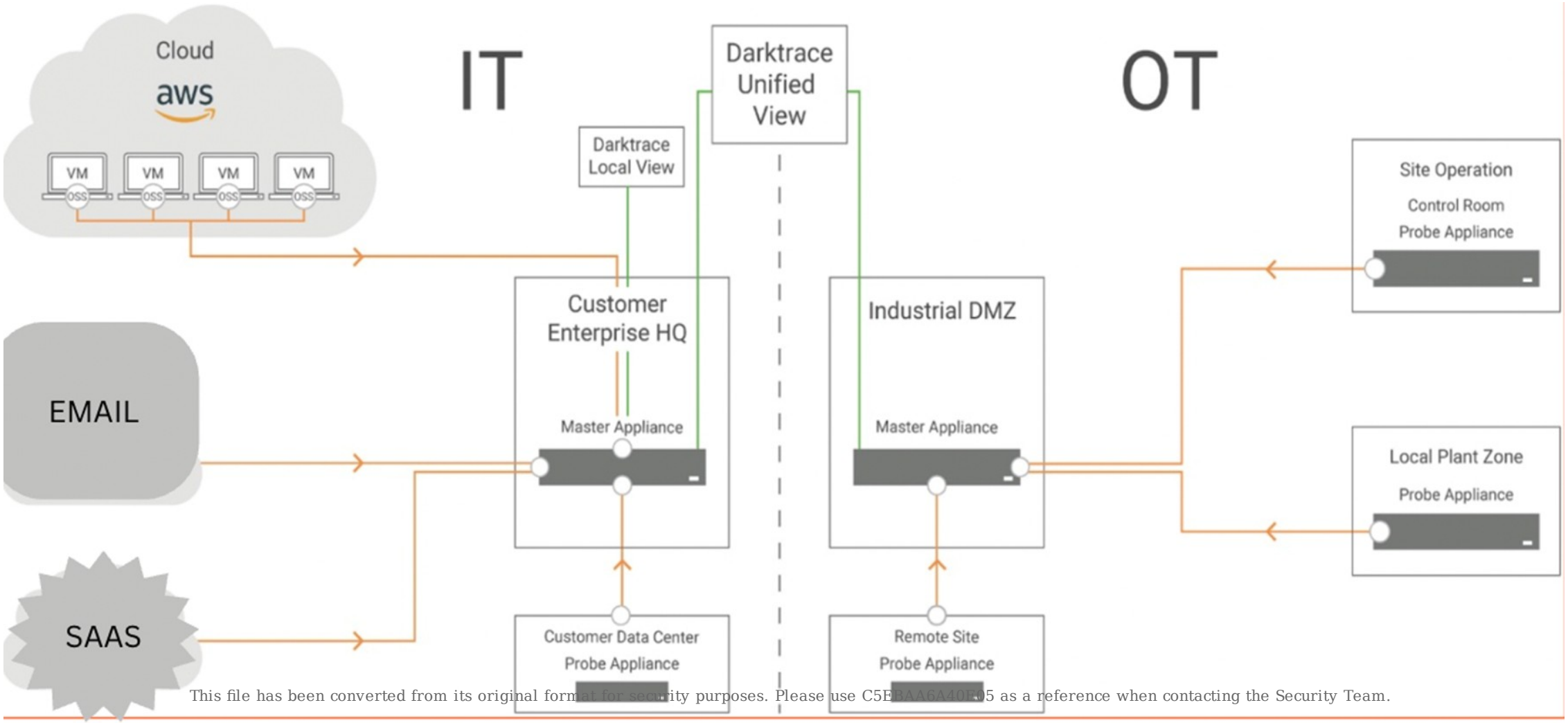
A shift in mindset and tooling is required

From	To
• Signatures	• Machine Leaning (ML) and Autonomous Response
• Rules	• Machine Leaning (ML) and Autonomous Response
• Lack of visibility or context	• Unified view across IT, OT, and Email
• Retrospective tooling	• Self Learning Artificial Intelligence (AI)

Unified View into IT, OT, and Email



Unified View into IT, OT, and Email

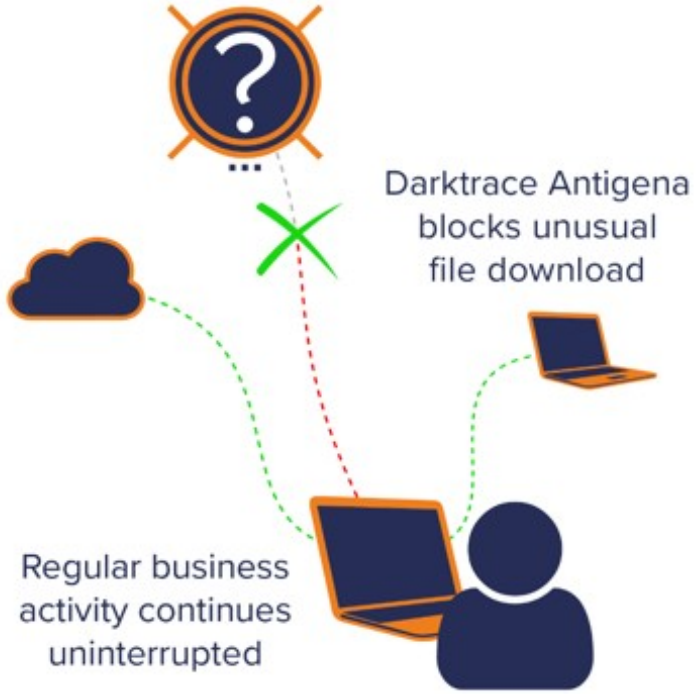


Cyber AI Analyst & Autonomous Response

- Autonomously investigates and prioritize security events
- Pulls together related events and behaviors into Incident Reports using natural language narrative
- Reduces triage time by up to 92%
- Neutralizes in-progress attacks
- Makes thousands of calculations at machine speed

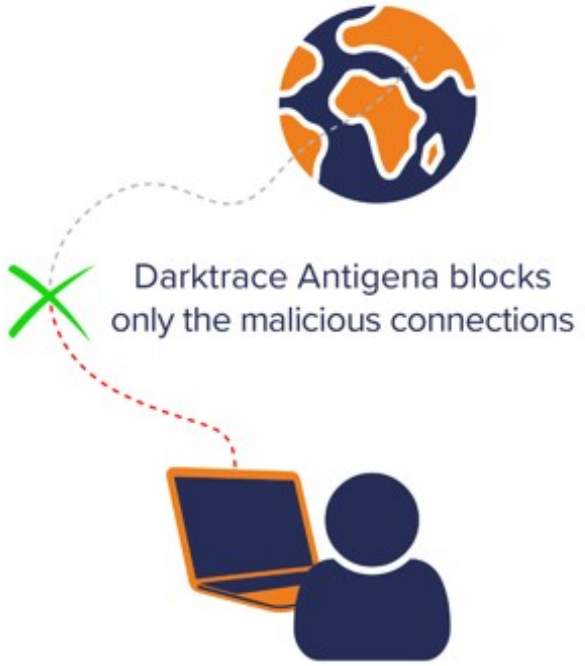
Stopping threats at multiple stages

1. Employee clicks on a link containing unknown malware



IF THE ATTACK CONTINUES...

2. Command and Control communication begins



IF THE ATTACK CONTINUES...

3. Endpoint attempts to upload sensitive documents onto OneDrive

Command and Control (C2) & beaconing

Initial Compromise

- Contractor initial entry point
- Long dwell time

Vulnerable HMI and ICS Historian

- Poorly segregated network
- Windows based VMs
- Running popular ICS software

Lateral Movement

- Living Off The Land
- Obtaining admin privileges
- Abuse of remote procedure calls
- SetupPrep.exe

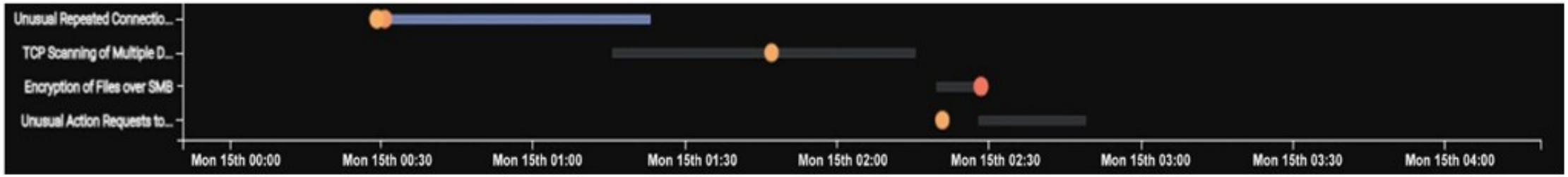
Conti Ransomware

Command and Control (C2)

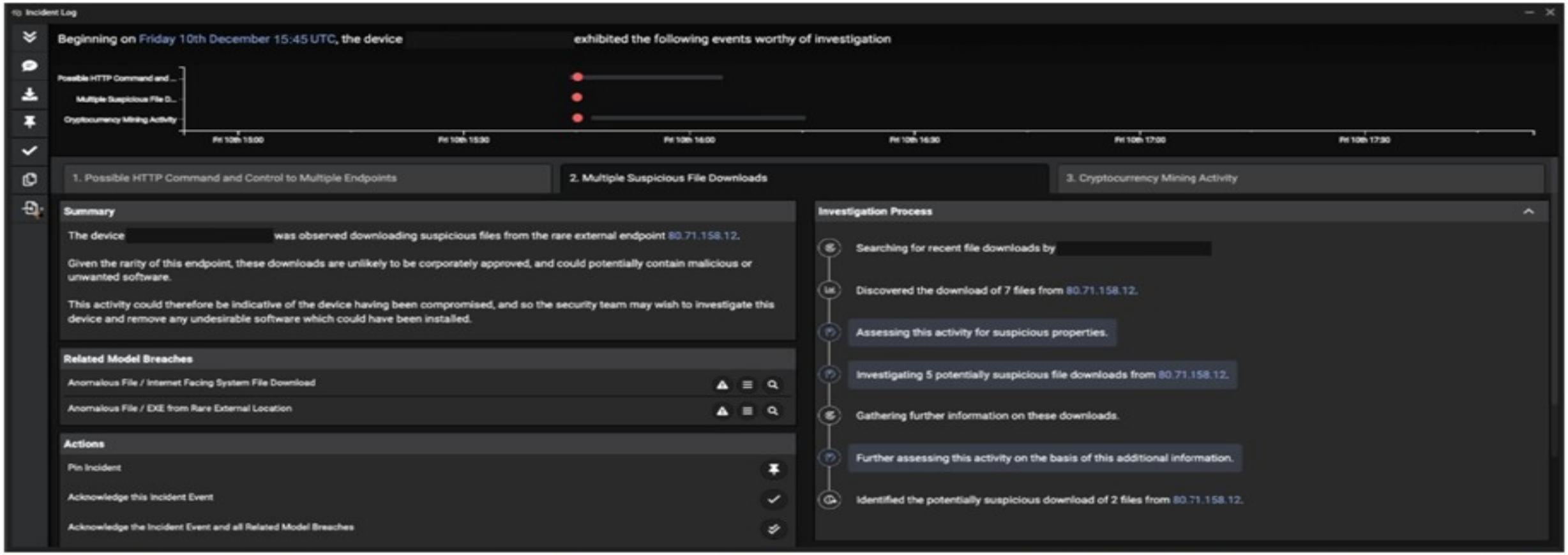
- Encrypted via SSL
- Ports 465, 995, 2222
- C2 Communications blocked

Encryption

- Compromised machine account
- Unusual SMB
- Unresponsive ICS device
- Ransomware note written



Conti Ransomware & Autonomous Response

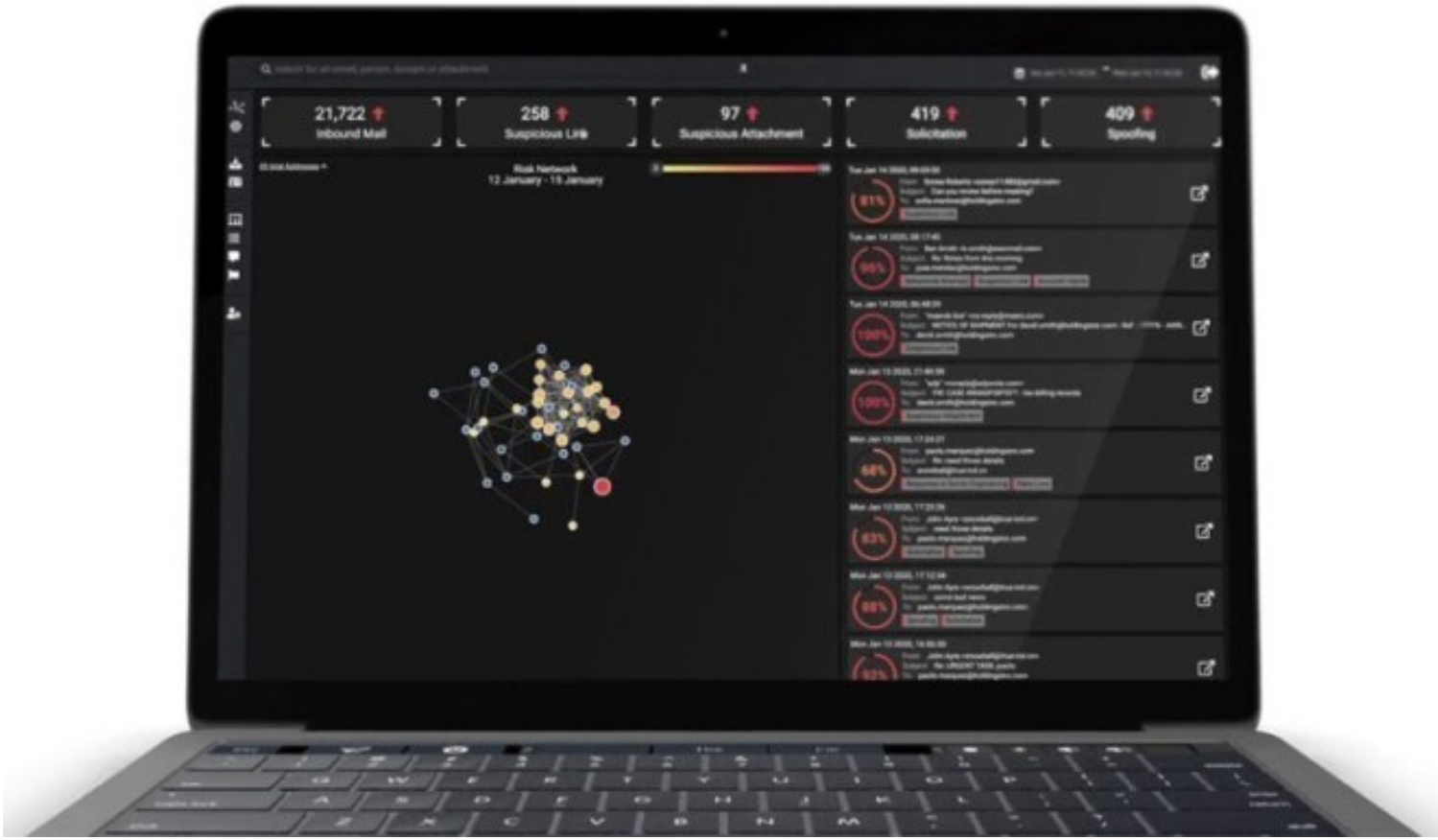


Example use cases in OT

- Unexpected IT/OT convergence and shadow devices
- APT and Zero Day exploits
- Contractors operating out of scope or with infected devices
- Supply Chain Compromise
- Physical Access granted through cyber attack
- Misconfigured / degraded PLC and other operational anomalies

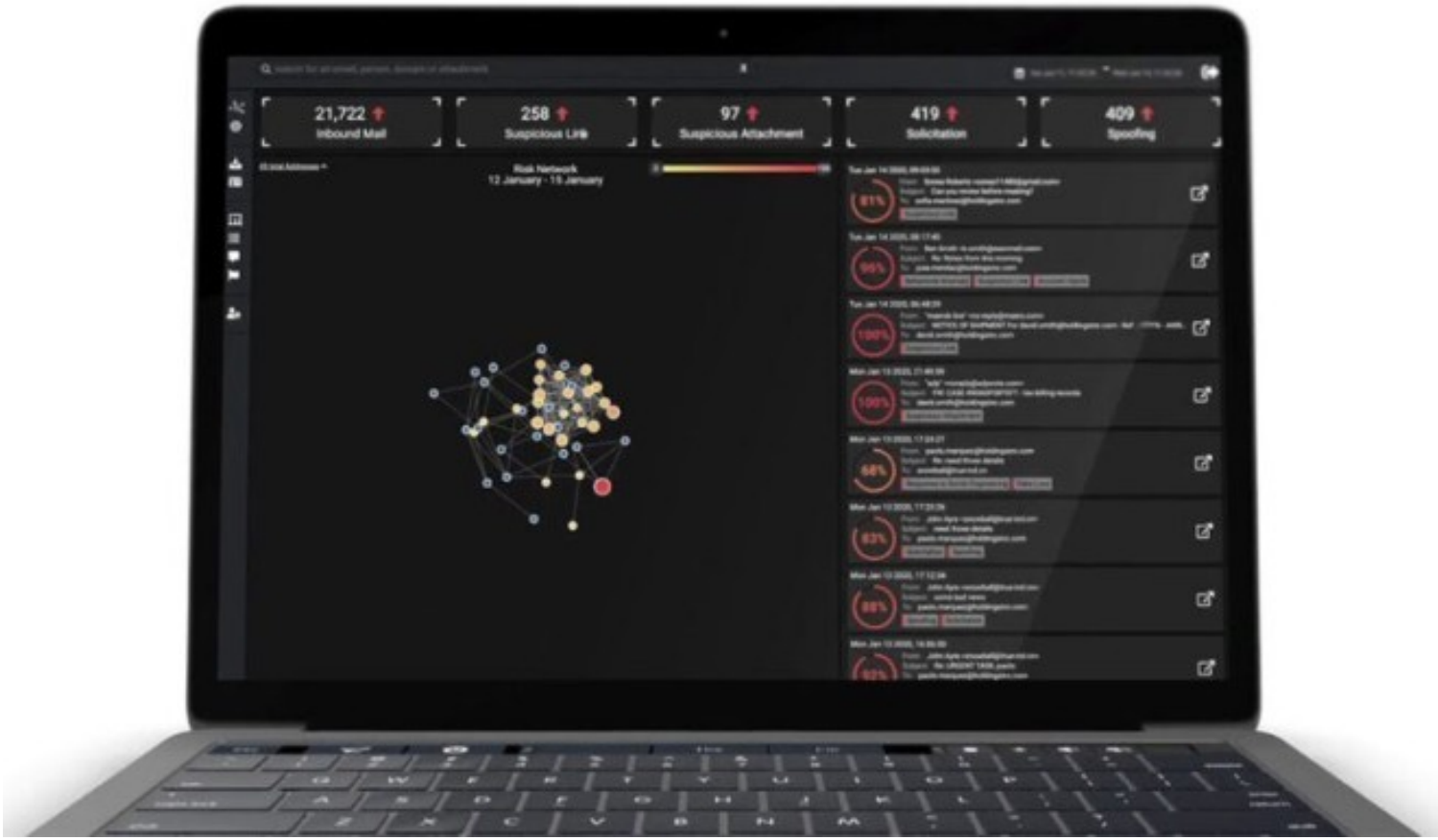
Email Protection + AI

- Creates behavioral profiles for every person
- Identifies relationships between senders and receivers
- Real-time determination of email legitimacy
- Configurable actions based on threat severity



Email Protection + AI

- Understands normal user behavior including account based behavior
- Meridian approved actions feed back into the AI, resulting in improved decision-making
- Autonomous response to lock attackers
- Includes impossible travel capabilities



Meridian + Darktrace better together

- Same great team, now with OT and email insight
- Accelerated by Artificial Intelligence (AI) and Machine Learning (ML)
- Increased visibility with IT, OT, and Email
- Meridian SOC informs and trains the ML algorithms
- Meridian audits recommended autonomous response

Meridian + Darktrace better together

- Batteries not included…
- Darktrace does not have their own Security Operations Center (SOC) – that's where we come in!
- Meridian to serve as a Managed Security Service Provider (MSSP) offering SOC capacities to Darktrace customers.
- 24/7, Excellent track record, US-based and deeply familiar with cooperatives

MERIDIAN

ENGAGE WITH US
ON SOCIAL MEDIA

@Meridian_Coop | @FuturaGIS

Meridian Cooperative | Futura Systems Inc.

Meridian Cooperative | FuturaGIS

@meridian_coop | @futurasystems

MeridianCoop | @futurasystemsinc

GREG GRAY

CIO

GregG@meridian.coop

QUOTATIONS:

techsales@meridian.coop

SCHEDULE A DEMO:

cri@meridian.coop