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

GREG GRAY / CIO

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>

REGULATORY 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>).

Page 6 of 14

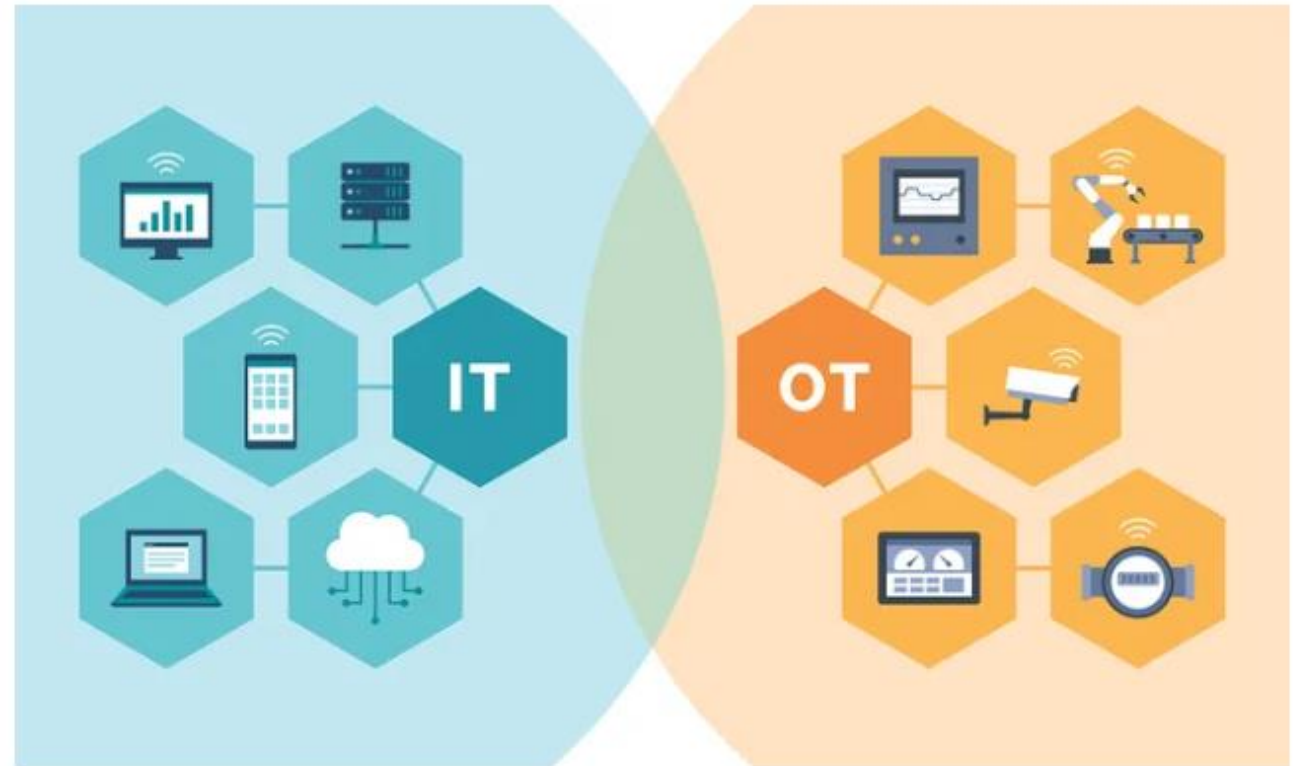
Security Directive

SD-1580/82-2022-01

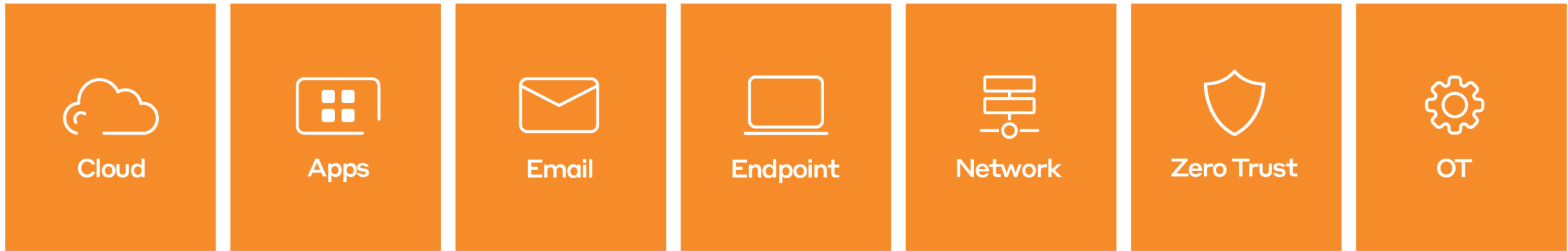
- b. Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;
- c. Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;
- d. Block and prevent unauthorized 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



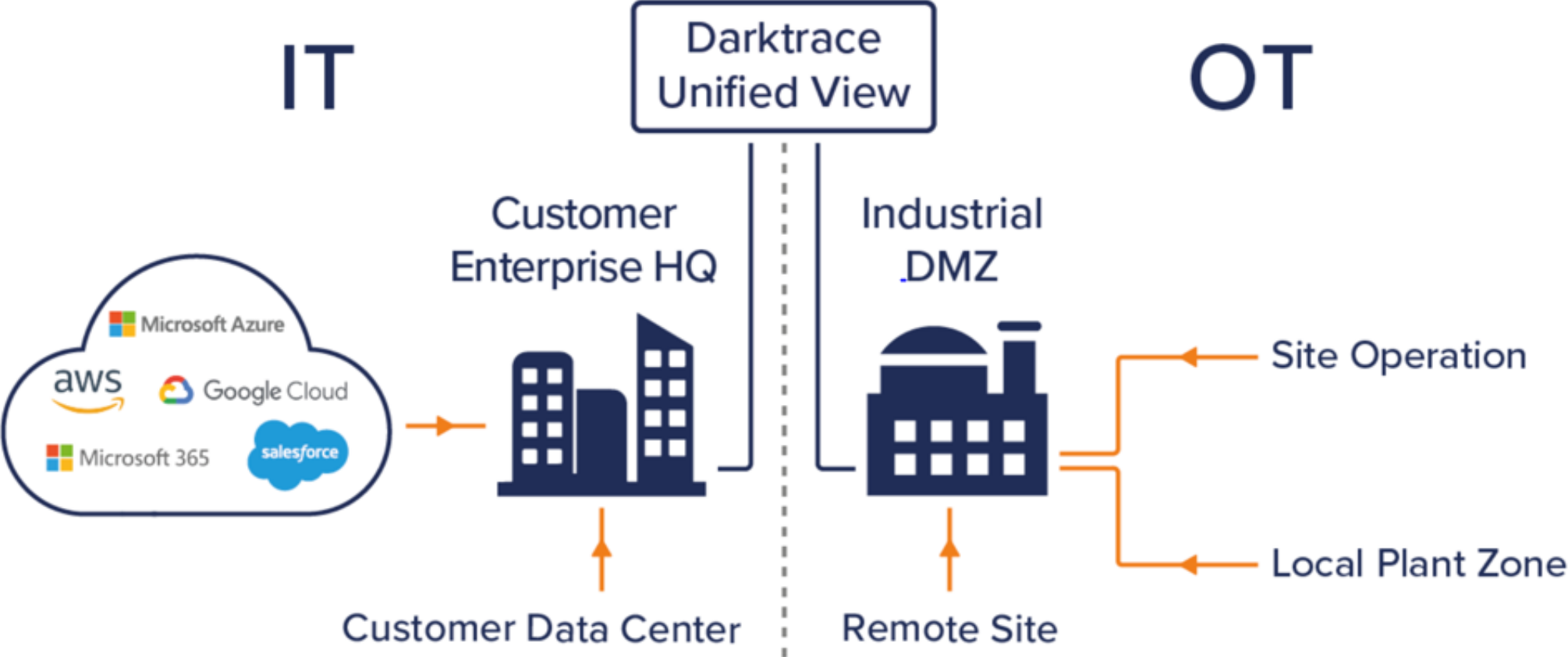
Visibility needs



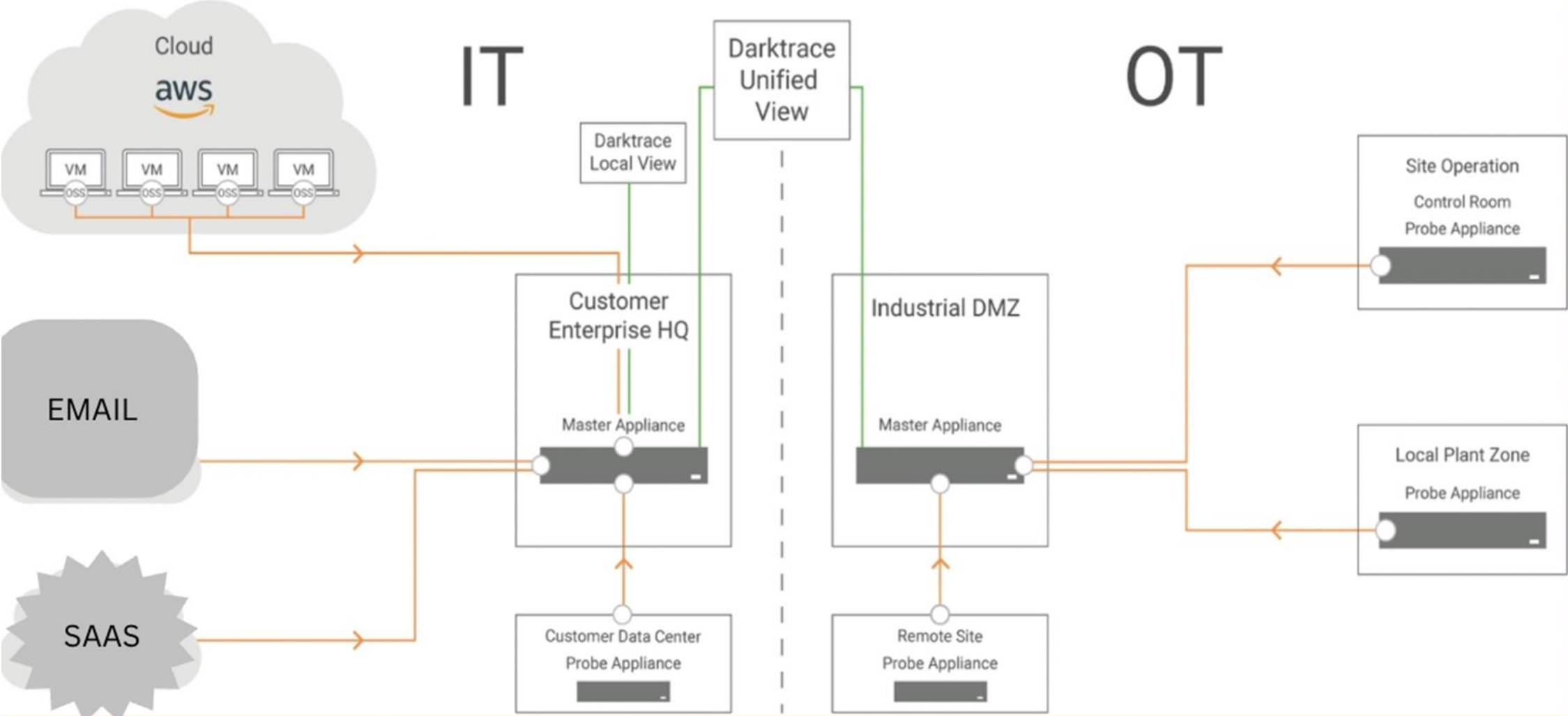
A shift in mindset and tooling is required

From	To
<ul style="list-style-type: none">• Signatures	<ul style="list-style-type: none">• Machine Learning (ML) and Autonomous Response
<ul style="list-style-type: none">• Rules	<ul style="list-style-type: none">• Machine Learning (ML) and Autonomous Response
<ul style="list-style-type: none">• Lack of visibility or context	<ul style="list-style-type: none">• Unified view across IT, OT, and Email
<ul style="list-style-type: none">• Retrospective tooling	<ul style="list-style-type: none">• 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



Cyber AI Analyst – IT Breach

Breach Log

Compliance / Possible Unencrypted Password File On Server

Description: A server is storing files that imply the presence of unencrypted passwords or other sensitive information. This model will breach once per week - a full list of possibly unencrypted password files accessed during the past week can be seen via Advanced Search.

Action: Review the files being accessed and if they contain passwords, the user who created the file should be reminded of password storage best practices.

Sun Feb 4, 00:00:00 to Tue Feb 6, 00:00:59 **Unacknowledged** All Acknowledged

Add model defeats

HOSTNAME **Launch RESPOND Action**

Compliance

4556 **SMB Read Success**

Mon Feb 5 06:56:10 Event message share= [redacted] \userfiles\$ file= [redacted] \documents [redacted] Passwords.xlsx version=smb2 account=[redacted]

Show less

Incoming traffic

Model Breach Event Log

Mon Feb 5 2024, 06:56:10 All Events

- Mon Feb 5, 06:56:00 [redacted] breached model Compliance / Possible Unencrypted Password File On Server
- Mon Feb 5, 06:55:59 [redacted] SMB Read Success — share=[redacted] \userfiles\$ file=[redacted] \Shortcut to UPN Reporting [redacted] lnk version=smb2 account=[redacted] [445]
- Mon Feb 5, 06:55:59 [redacted] SMB Read Success — share=[redacted] \userfiles\$ file=[redacted] Documents\Commercial Customers [redacted] Gifts.docx version=smb2 account=[redacted] [445]
- Mon Feb 5, 06:55:59 [redacted] SMB Read Success — share=[redacted] \userfiles\$ file=[redacted] \Documents\Commercial Customers [redacted] [redacted].doc version=smb2 account=[redacted] [445]
- Mon Feb 5, 06:55:59 [redacted] SMB Read Success — share=[redacted] \userfiles\$ file=[redacted] \Documents\Commercial Customers [redacted] [redacted].xlsx version=smb2 account=[redacted] [445]
- Mon Feb 5, 06:55:59 [redacted] SMB Read Success — share=[redacted] \userfiles\$ file=[redacted] \Documents\Commercial Customers [redacted] [redacted].doc version=smb2 account=[redacted] [445]
- Mon Feb 5, 06:55:59 [redacted] SMB Read Success — share=[redacted] \userfiles\$ file=dcarden\Documents\Commercial Customers [redacted] pdf version=smb2 account=[redacted] [445]

Cyber AI Analyst – OT Breach

Incident Log

Beginning on Monday 29th January 14:31 EST, the device [redacted] exhibited the following events worthy of investigation

1. Unusual Write Requests to OT Endpoint ✓ 2. Possible SSL Command and Control

SUMMARY

The device [redacted] **Source Host** was observed making multiple OT write requests to 10.31.101.93.

This behaviour did not match the previous pattern of requests observed from this device.

Consequently, though this activity could be due to a legitimate change in behaviour, it could also be a sign of this device attempting to compromise or gather information on another OT endpoint in the network.

The security team may therefore wish to investigate these requests, and ensure they were expected.

Lateral Movement

RELATED MODEL BREACHES

ICS / Multiple New Write Commands

INVESTIGATION PROCESS

- Searching for recent OT requests from [redacted] **Source host**
- Discovered 10 write requests to 10.31.101.93 .

ACTIONS

- Incident Event Acknowledged
- Unacknowledge this Incident Event

SOURCE OF REQUESTS

Source Device: [redacted] **Source Host** 10.33.4.40

- Antigena All
- Domain Authenticated
- MODBUS Device
- High Risk
- Microsoft Windows
- ICS Device

Username Observed Prior To Activity: [redacted] **AD User**

Source Of Username: Kerberos TGS request

Time Observed: 29th Jan 2024 14:26:12 EST

Event UID: CXytPh3h1H0ziPbRle00

Conti Ransomware



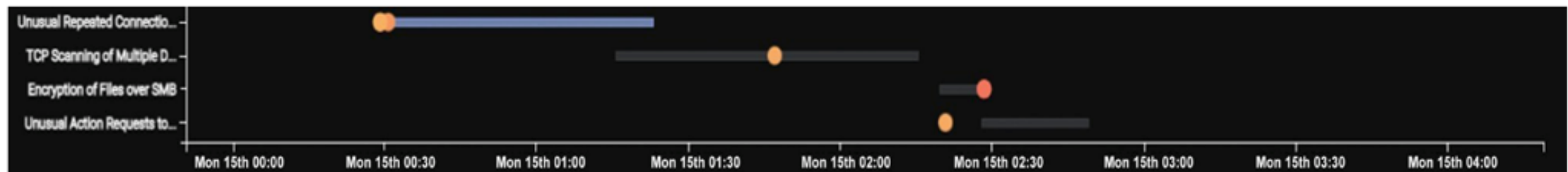
Command and Control (C2)

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



Encryption

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



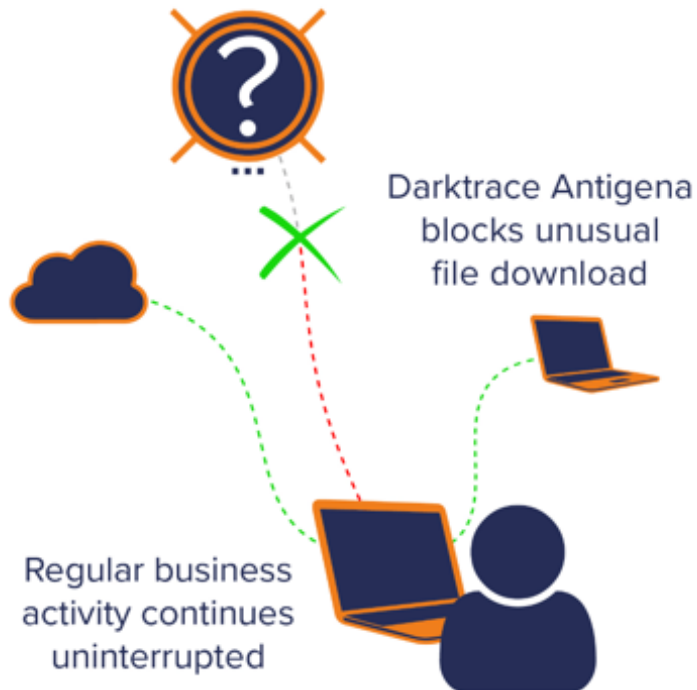
Conti Ransomware & Autonomous Response

The screenshot displays an 'Incident Log' window with a dark theme. At the top, a summary states: 'Beginning on Friday 10th December 15:45 UTC, the device [redacted] exhibited the following events worthy of investigation'. Below this is a timeline from 15:00 to 17:30 on Friday, 10th December, with three red dots indicating events. The main content area is divided into three tabs: '1. Possible HTTP Command and Control to Multiple Endpoints', '2. Multiple Suspicious File Downloads', and '3. Cryptocurrency Mining Activity'. The '2. Multiple Suspicious File Downloads' tab is active, showing a 'Summary' section with text: 'The device [redacted] was observed downloading suspicious files from the rare external endpoint 80.71.158.12. Given the rarity of this endpoint, these downloads are unlikely to be corporately approved, and could potentially contain malicious or unwanted software. This activity could therefore be indicative of the device having been compromised, and so the security team may wish to investigate this device and remove any undesirable software which could have been installed.' Below the summary is a 'Related Model Breaches' section with two entries: 'Anomalous File / Internet Facing System File Download' and 'Anomalous File / EXE from Rare External Location'. At the bottom of the tab is an 'Actions' section with three options: 'Pin Incident', 'Acknowledge this Incident Event', and 'Acknowledge the Incident Event and all Related Model Breaches'. To the right of the summary is an 'Investigation Process' section with a vertical flow of steps: 'Searching for recent file downloads by [redacted]', 'Discovered the download of 7 files from 80.71.158.12.', 'Assessing this activity for suspicious properties.', 'Investigating 5 potentially suspicious file downloads from 80.71.158.12.', 'Gathering further information on these downloads.', 'Further assessing this activity on the basis of this additional information.', and 'Identified the potentially suspicious download of 2 files from 80.71.158.12.'

Sun Dec 12, 16:18:10 ▼ ⓘ Antigena Response — Block connections to 164.52.212.196 port 88 for 2 hours [88]
Sun Dec 12, 16:18:08 ▼ → [redacted] connected to [redacted] 164.52.212.196 [88]
A rare port for the HTTP protocol. A new connection externally on port 88

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



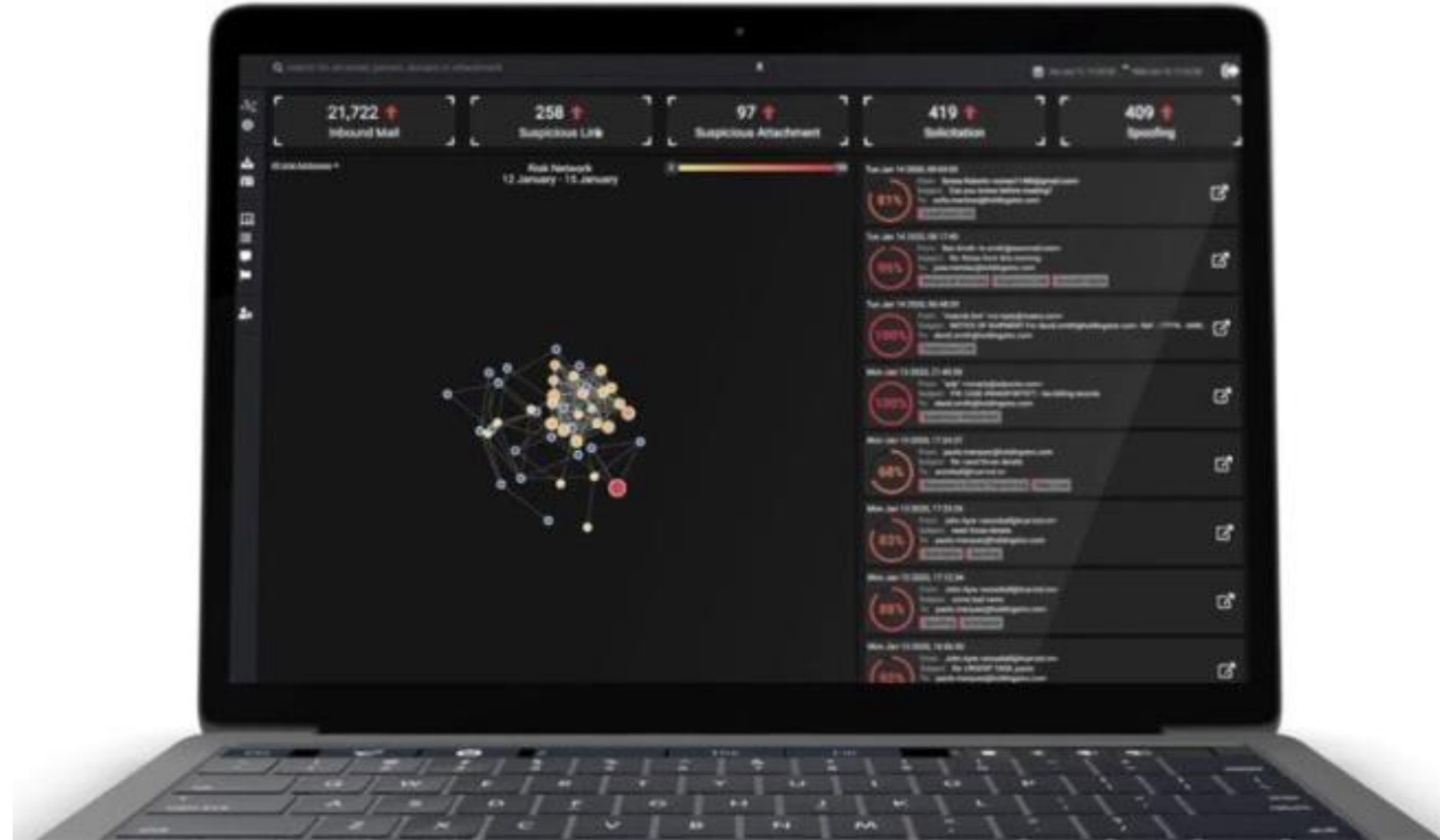
Example use cases in OT

- 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 (continued)

- 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



CEO Targeted Phishing Email



Meridian: Password System Reminder

"Meridian IT Service - (No Reply)" <support@reudatur.com>

To: chrish@meridian.coop

100%

WED FEB 7 2024, 18:18:20

Held

- Credential Harvesting
- Internal IT Impersonation
- Phishing Link
- User Impersonation
- Low Mailing History
- No Association
- Spoofing Indicators
- Unknown Correspondent
- VIP

Hold message

ANOMALY INDICATORS

The sender appears to be impersonating an internal service by referencing **meridian** in their **display name**. This tactic allows attacks to avoid any validation checks which apply to this domain.

The email contains a highly suspicious link to a host **webemail.constructoin.best**. The host has a **100%** rarity score based on references in internal traffic. The link was **hidden** from the user and masked by text reading **Keep retktfMY Passvart1dword**.

HISTORY 0 Users 0 Days

ASSOCIATION 0 Users Never

VALIDATION SPF .ll DKIM .ll DMARC .ll

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 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



DARKTRACE

MERIDIAN CYBERSECURITY PARTNERS

ENDPOINT DETECTION & RESPONSE



24/7 MONITORING

DARKTRACE

MULTIFACTOR AUTHENTICATION



NEXT GENERATION FIREWALL

FORTINET

VULNERABILITY SCANNING



PENTESTING-AS-A-SERVICE (PTaaS)



CYBER AWARENESS EDUCATION



PATCH MANAGEMENT

ninjaOne

SIEM & HOST INTRUSION DETECTION SYSTEM

wazuh.



CONNECT WITH US

GREG GRAY

CIO

GregG@meridian.coop

770-414-8400 ext. 2618

ENGAGE WITH US ON SOCIAL MEDIA

 @Meridian_Coop | @FuturaGIS

 Meridian Cooperative | Futura Systems Inc.

 Meridian Cooperative | FuturaGIS

 @meridian_coop | @furasystems

 MeridianCoop | @furasystemsinc