CSA SINGAPORE | SG Passion Made Possible

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

Deceive by Design: How to Use Deception Technology to Protect OT Networks

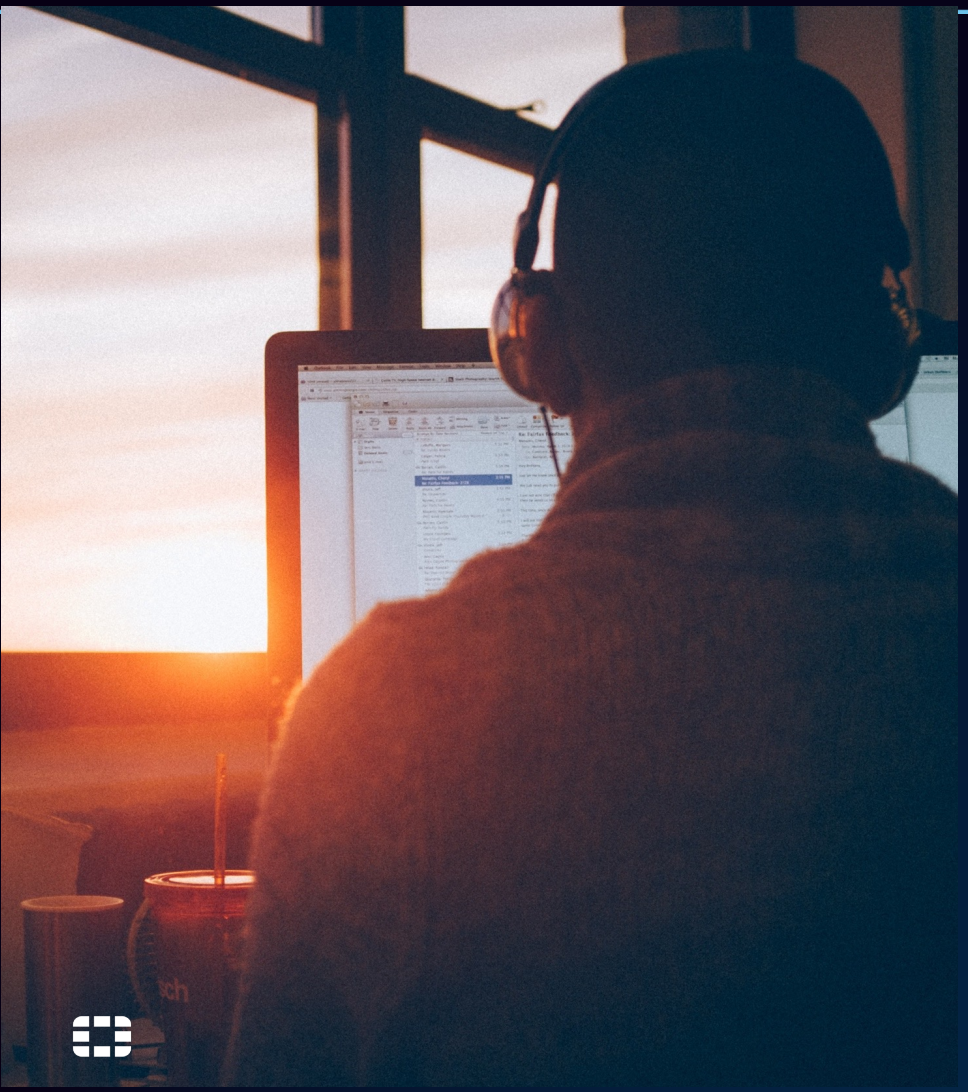
What is Deception?

Honeypots vs Deception

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

What is Deception?

What is Deception?



Diverting attackers to fake assets to protect enterprise's real assets

Decoys
Fake assets, fake network devices, fake applications

Lures
Fake Applications/services of the honeypots/decoys

Network traffic
Fake network traffic beaconing (SMB,CDP, UPnP, and more)

Breadcrumbs (tokens)
Fake resources placed on real IT assets and point to the fake systems

Prioritize alerts from the deception — High-fidelity alerts that require your immediate attention

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Honeypots vs Deception

	Traditional Honeypots	Deception Technology
Authenticity		●
Ease of deployment and operation		●
Scalability	○	●
Interaction		●
Capture Lateral Movement	○	●
Automated Threat Response	○	●

Why Use Deception Technology for OT Environments?

Critical assets are unpatched or unmonitored

- ICSs/IoTs lack security by design and are brittle to change
- Maintenance windows are costly and measured in months/years
- Diverse, multi-vendor assets (legacy OSs, non-standard devices and protocols)

Air gaps between IT and OT are decreasing

- ICSs are no longer isolated from corporate or other networks

Security teams are stretched

- High rate of false positive alerts

< 5% are investigated

- Cybersecurity skill gap

Challenges Facing Security Teams

Detecting attackers is challenging

- On average, global dwell time is 21 days
- Unable to detect lateral movements

Security teams are stretched

- High rate of false positive alerts, < 5% are investigated

Securing legacy/unmanaged systems (OT, IoT, IoMT)

- Air-gap protection diminishes
- Assets do not provide their own telemetry (e.g., IoMT/OT/IoT)
- Unpatched/unmonitored critical devices

Break out of the darkness and quickly detect in-network threat activity across all attack surfaces

Securing High-Value Assets and Confidential Unclassified Information

NIST

SP 800-172

SP 800-82 Rev. 3

SP 800-172

Enhanced Security Requirements for Protecting Controlled Unclassified Information

Published: February 2021

Key elements essential to addressing the APT:

"**Using deception to confuse and mislead adversaries** regarding the information they use for decision-making, the value and authenticity of the information they attempt to exfiltrate, or the environment in which they are operating."

SP 800-82 Rev. 3

Guide to Operational Technology (OT) Security

Published: April 26, 2022

"…Because decoys **do not actively interact with other network components**, deception technologies can support malicious activity monitoring and detection **without jeopardizing the controlled process.**" (E.2.7)

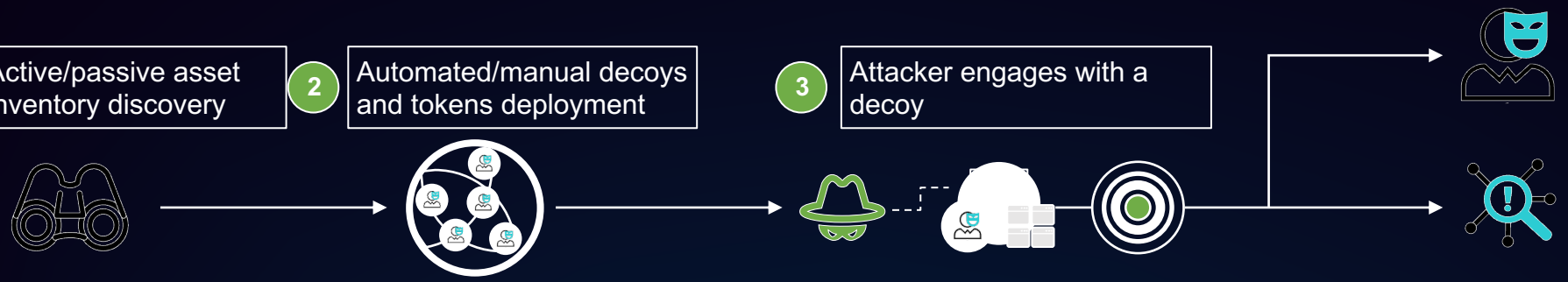
How Does Deception Work?

Deception Topology & Deployment

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

How Deception Works - DEPLOYMENT

1. Active/passive asset inventory discovery
2. Automated/manual decoys and tokens deployment
3. Attacker engages with a decoy
4. Attack is automatically blocked



Automated Quarantine, Actionable Intelligence

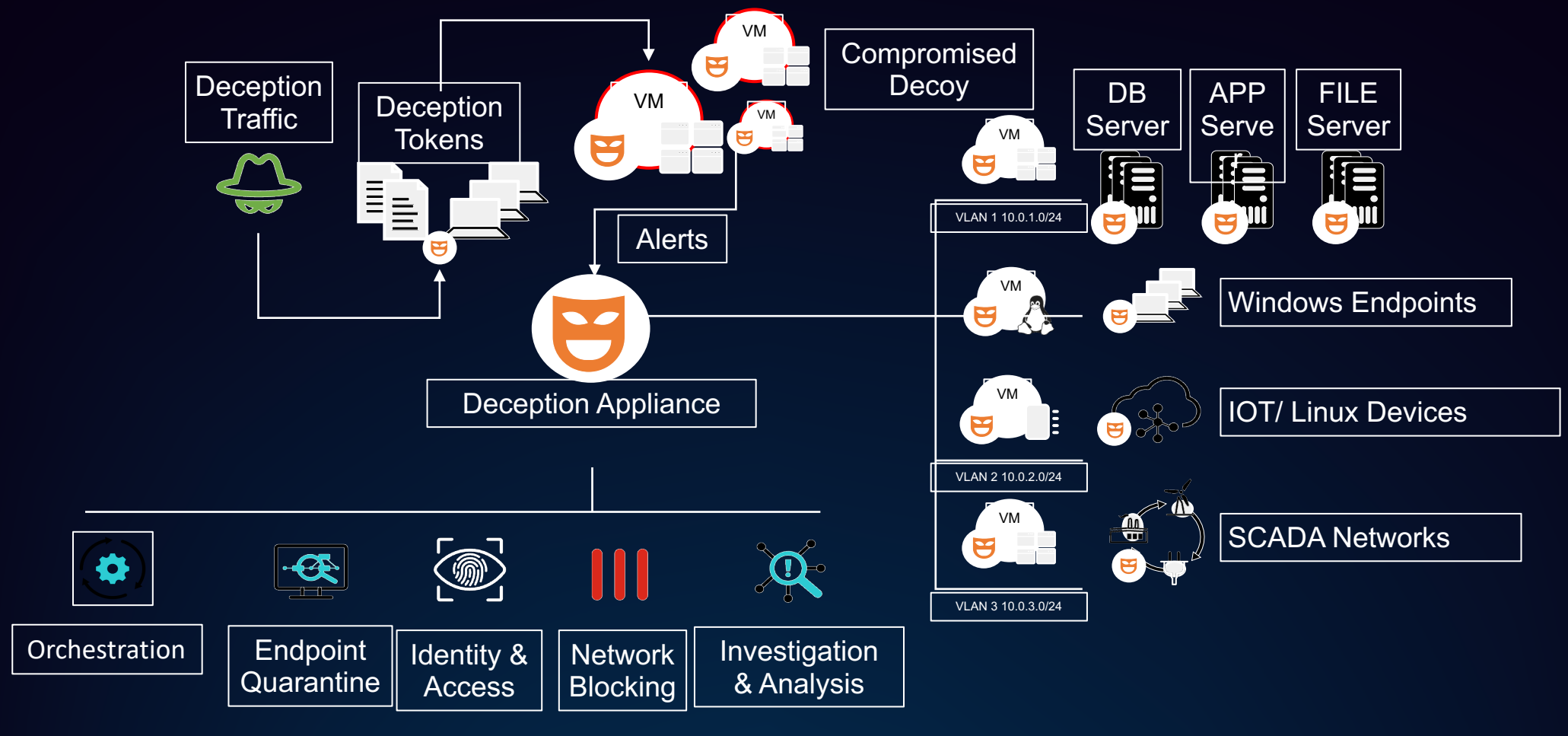
Automated Decoy Generation & Placement Optimization

Real-Time Detection & Threat intelligence

Comprehensive detection, closing visibility gaps, diverts attackers from sensitive assets to shift the balance to defender's advantage

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

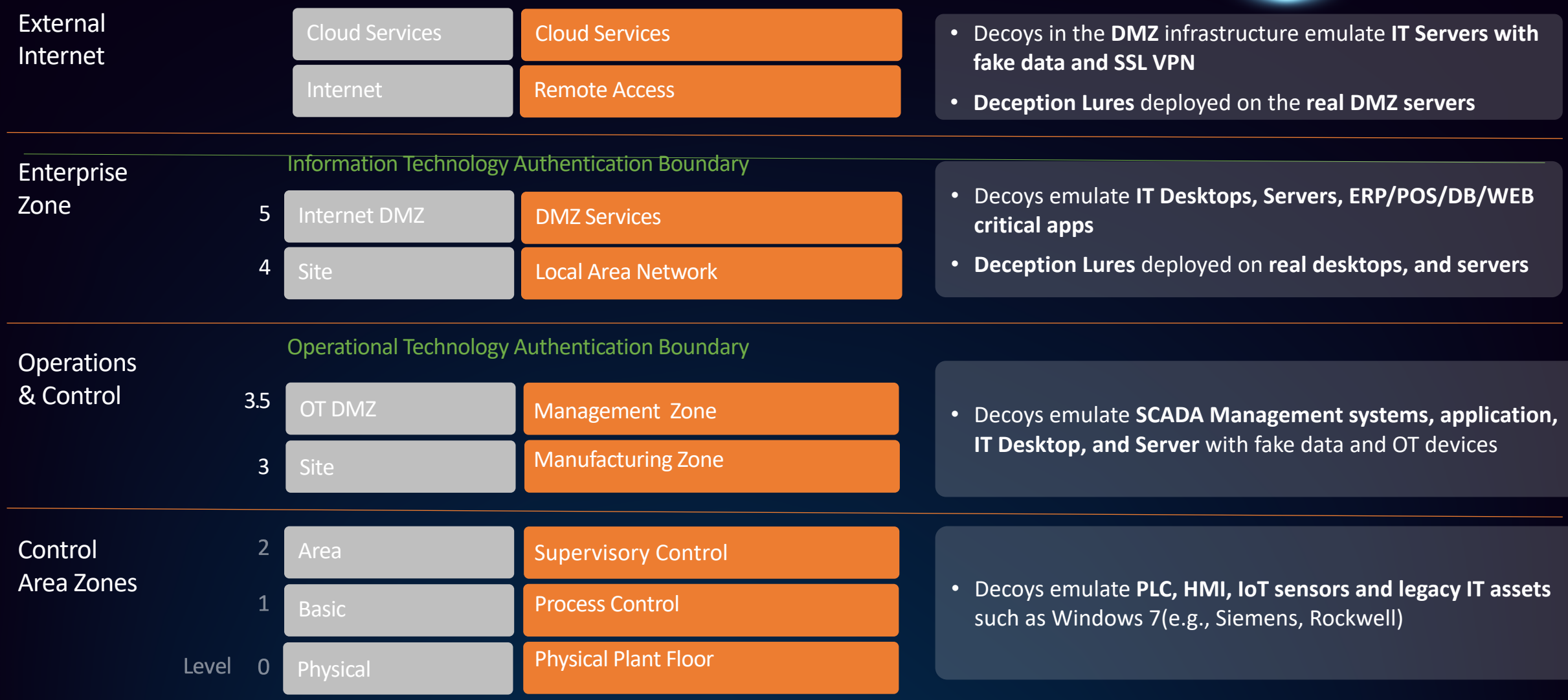
How Deception Works - TOPOLOGY



Deception Use Cases

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Protecting OT – Based on the Purdue Model



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Most Common Use Cases: How Deception can help

OT

- Network visibility and breach detection via passive footprint
- Detects threats to assets that cannot provide their own telemetry

Ransomware Mitigation

- Early detection, alert and response to Ransomware – Decoys 'feed' the malware with fake data, divert, and contain the attack
- Keeps malware from encrypting 'real' data and spreading

Lateral Movement

- Detects lateral movements as opposed to detecting threats on egress/ingress
- Last-resort security control ("detect when all other controls fail")
- Provides a defense-in-depth and active defense strategies

Threat Hunting

- Enables less noisy in-network threat detection, empower your SOC team
- Leverages deception lures to track attack origin
- Learns about attacker TTPs by observing attackers in highly-monitored environments

Deception Case Studies

Case Study
Leading Energy Provider Protects Critical Remote Assets

Pain Points

Concerned about compromised remote sites

Increased attack surface

Siloed visibility and control across IT/OT

Results and Benefits

Active deception layer across IT/OT environments covering all crown-jewel segments

- Decoys include pump decoys, automated tank gauges (ATGs), cameras, ERP systems, and “golden image” apps
- Use “golden images” to create decoys
- Use industrially-hardened, rugged devices

Close SOC visibility gap

- Provides in-progress attack intel and detailed forensics captured by the attacker’s activities

Use deception as a compensating control

- Use decoys and fake tokens to protect critical assets where patching isn’t possible, and uptime is critical

Enhance visibility and accelerates incident response

- Integrates with Fortinet Security and third-party security controls

Reduce false positive alerts

- Provides correlation and forensics

Case Study

Leading HealthCare provider Protects Critical Medical Devices

Pain Points

- Concerned about compromised Medical Devices
- Increased attack surface
- Siloed visibility and control across Medical IoT/IT

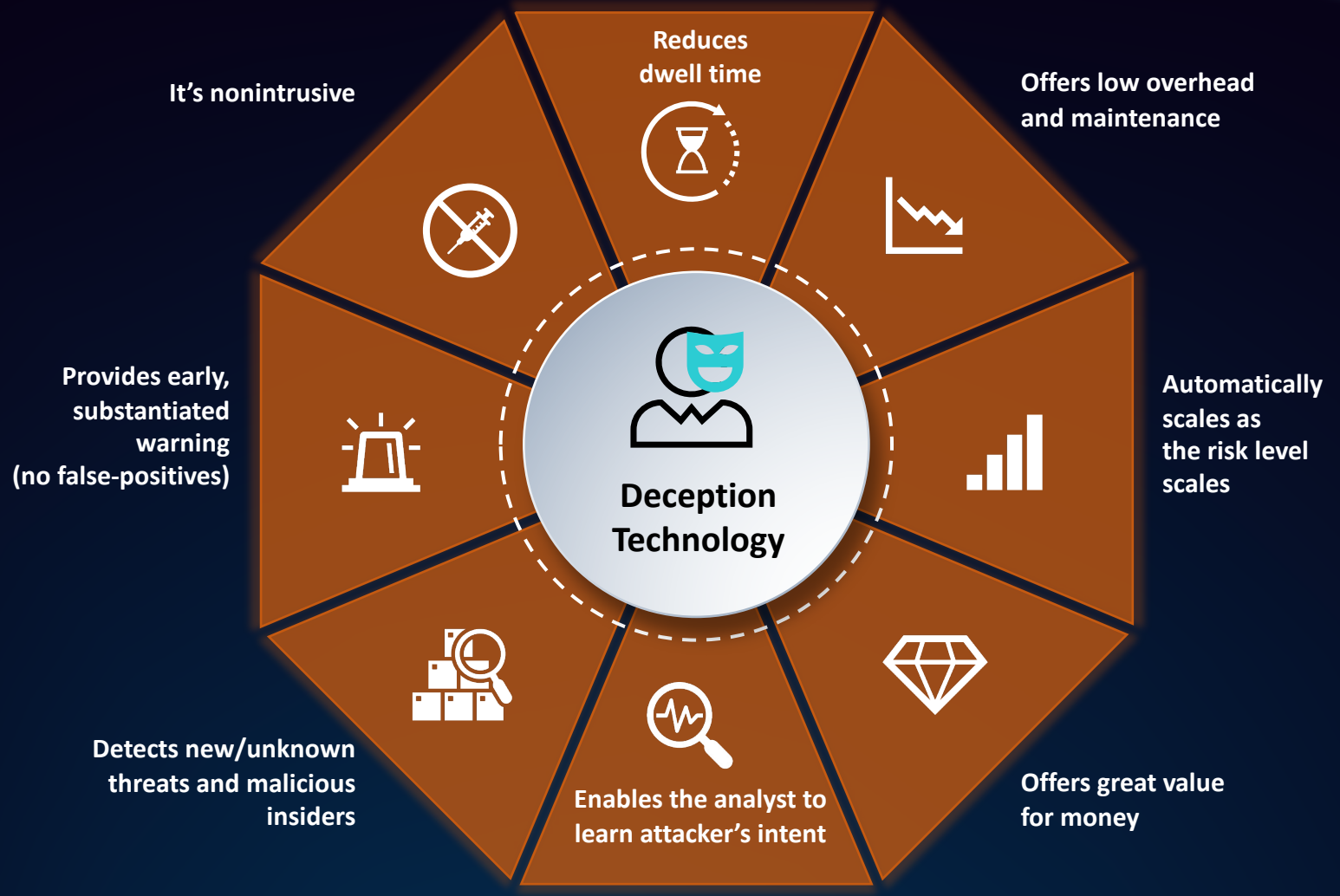
Results and Benefits

- Active deception layer across Medical IoT devices and IT environments covering all crown-jewel segments
  - Decoys include Infusion pump decoys, PACS servers, cameras, ERP systems, and “golden image” apps
  - Use FortiDeceptor HW appliance
- Use Deception for early breach detection in medical segments
- Use deception as a compensating control
- Enhance visibility and accelerates incident response
- Reduce false positive alerts
- Provides correlation and forensics


OTCEP
2023
OPERATIONAL TECHNOLOGY
CYBERSECURITY EXPERT PANEL FORUM 2023

Summary

Why Should Everyone Use Deception?



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Why Deception?

How else would you know **if attackers are inside your network**? How fast can you detect them?

How do you protect devices that **cannot provide their own telemetry** or cannot be protected using monitoring agents or security patching?

How do you plan to **reduce false-positive rates**? Are you looking to **reduce the time spent** on reviewing alerts?

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

What to look for in a Deception OT solution?

1 **Decoys for both OT and IT**

- Aligns with Purdue Model
- SCADA/ICS profile e.g. Rockwell Ethernet/IP, Siemens S7, Bacnet, IPMI, Modbus and etc.
- Windows and Linux with Git, VPN, SMB, SQL, etc. applications, and honeytokens

2 **Simple and Easy**

- Automated discovery of network and assets
- AI-based recommended deployment

3 **Holistic Response Strategy**

- Open integration with existing security infrastructure
- Automated threat response, and threat hunting

In Summary

- What Is Deception
- How Does it Work
- Use Cases
- Deception Use Cases

Thank you Very Much!

Stay In touch, Save my Contact

Stay Informed, Ask Questions