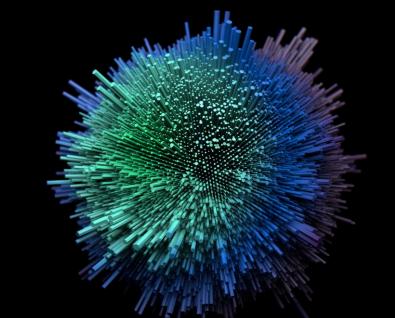
Deloitte.

Shedding light on Shadow OT What is Shadow OT and how does

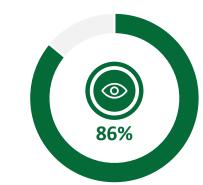
it impact Industrial Organizations?



Industrial organizations are facing new challenges with the convergence of Operational Technology (OT) with Information Technology (IT), such as **network blind spots** caused by **not knowing the data flows** or by **unknown devices** that are placed between these networks, increasing the likelihood of a **cyber incident** in these environments.



OT Organizations that experienced at least one intrusion in the past 12 months. 78% had more than three [1]



Organizations that have limited or no visibility into their OT environment [2] a 4% increase since 2017 [4]



Organizations that are ineffective at discovering and maintaining an inventory of all OT devices throughout the asset lifecycle [3]



Having reduced visibility of the operational systems and a poor network device inventory, can make activities such as network assessment and hardening of network devices more complex, and lead organizations to face a phenomenon known as Shadow OT.

Sources: [1] Fortinet (2022), [2] Dragos (2021), [3] Ponemon Institute (2021), [4] Forrester (2017)

Shadow OT refers to unidentified and unmonitored assets inside an organizations' network and can be caused by the lack of complete visibility into the network and operational systems, inappropriate asset management and no OT discovering tools.

Examples of Affected Devices



Unmanaged sensors



Unmanaged **VPN** connections



Personal devices



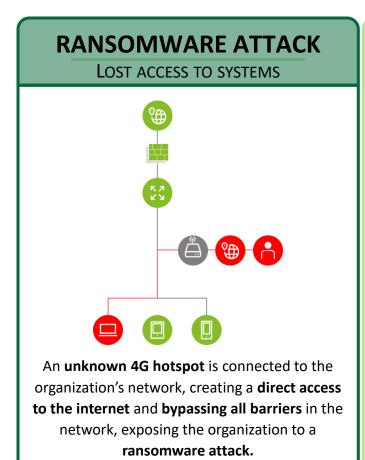
extensions



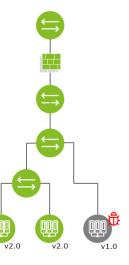


There are several examples of situations in which shadow devices endangered organizations' networks, by allowing cyber incidents such as Ransomware, SQL injection and IoT attacks to happen.

Examples of Attacks on Organizations





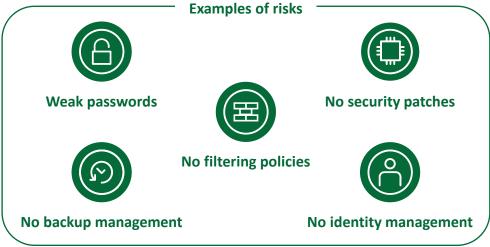


An **unpatched server** is connected to the organization's network, allowing a SQL injection attack caused by an exploited vulnerability, which allowed hackers to gain access to confidential data from the internal network.

STOLEN CONFIDENTIAL DATA

An **unmanaged IoT sensor** is connected to the organization's network, serving as an entry point to hackers, who then moved laterally to other places within the network, and were able to steal confidential data.

Unidentified devices present several technical and business risks that can impact organizations at different levels, so being able to identify them is crucial to define a security strategy capable of mitigating these vulnerabilities.





To mitigate Shadow OT different actions are required, and they can be structured in a four-step approach:



- Ensure clear visibility over people, processes and technology
- Identify network and security requirements
- Identify network blind spots



- Define a governance model Design a network
- security strategy
- Identify tools to eliminate blind spots



- strategy and discovery tools
- Monitor network traffic and analyse logs
- Automate OT data collection and define identity-based network access



- Raise awareness and educate employees
- Create documentation for all network changes
- Perform physical and logical audits

How can Deloitte help?

Our technology and engineering expertise and business strategic skills allows us to be a trust-worthy advisor for every step of the journey.

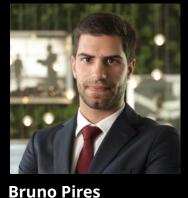
and a proven track record in network and tech transformation.

Wide experience in OT/ICS environments, with a proven methodology from assessment to design until implementation in several industries. Global Telecom CoE with unique technology and engineering knowledge,

Multidisciplinary specialized teams, which combine the high technical expertise with business and strategic consulting teams.

Contacts

Experts



Telecom Engineering

brunpires@deloitte.pt

Excellence

Manager



Excellence

Senior Consultant

davandrade@deloitte.pt

Sponsor



Telecom Engineering Excellence Partner petavares@deloitte.pt



Telecom Engineering Excellence Partner labreu@deloitte.pt

"Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities and, therefore, do not bind each other for all intents and purposes. Accordingly, each entity is only liable for its own acts and omissions and cannot be held liable for the acts and omissions of the other. Furthermore, DTTL does not provide services to clients. To learn more, please consult www.deloitte.com/about Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune

"Deloitte," "us," "we" and "our" refer to one or more of Deloitte Touche Tohmatsu Limited ("DTTL") member firms, and their related entities (collectively, the

Global 500° among thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. To learn how Deloitte's 415,000 people worldwide make an impact that matters please consult www.deloitte.com.

This communication contains general information only, and neither Deloitte Touche Tohmatsu Limited ("DTTL") nor its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Accordingly, before deciding or taking any action that may affect your finances or your business, on the basis of this communication you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and therefore neither the issuer, nor DTTL or its network of member firms, related entities, employees or agents may be held liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

