OT Security

- **What is OT security?**

(ans): OT security as, “Practices and technologies used to (a) protect people, assets, and information, (b) monitor and/or control physical devices, processes and events, and (c) initiate state changes to enterprise OT systems.” OT security solutions include a wide range of security technologies from next-generation firewalls (NGFWs) to security information and event management (SIEM) systems to identity access and management, and much more.

- **Need for OT security.**

(ans): Operational technology (OT) security is designed to meet the unique security needs of OT environments. This includes protecting system availability, understanding OT-specific protocols, and blocking attacks targeting the legacy systems commonly used in OT environments.

- **Challenges of OT security.**

(ans): The Challenges of OT security are as follows:

1. Legacy Systems and Lack of Security by design.
2. Increasing connectivity and Convergence of OT/IT.
3. Evolving Threat Landscape.
4. Limited workspace and skilled force.

- **Reasons of evolving of challenges.**

(ans): The reasons are as follows:

1. Rapid adoption of Iot and IIot Devices.
2. Digital Transformation Initiatives.
3. Geopolitical Tensions.

- **Advantages of OT security.**

(ans): Advantages of OT security are as follows:

1. Cost Saving
2. Better performance
3. Improved flexibility
4. Increase operational standards
5. Enhanced security orchestration

- **Examples of Recent OT Cyber Security Attacks.**

(ans): The examples attacks are as follows:

1. **Colonial Pipeline Attack(2021):**

   A ransomware attack on the Colonial Pipeline, the largest fuel pipeline in the United States, disrupted fuel distribution for several days. This incident highlighted the vulnerabilities of critical infrastructure and the potential for severe economic impact.

2. **SolarWinds Orion Attack(2020):**

   The SolarWinds Orion breach allowed attackers to infiltrate multiple government agencies and private organizations, including those with OT systems. This supply chain attack demonstrated the potential for widespread consequences when critical software is compromised.

3. **Trition/Trisis(2017):**

   In 2017, a highly sophisticated malware named Triton/Trisis targeted safety instrumented systems (SIS) in a petrochemical facility in Saudi Arabia. The attack aimed to manipulate the facility's safety systems, potentially leading to catastrophic consequences.

4. **Ukraine Power Grid Attack(2015):**

   In 2015, hackers infiltrated the Ukraine power grid, causing widespread blackouts that affected more than 200,000 people. The attackers compromised both IT and OT systems, demonstrating the real-world consequences of cyber attacks on critical infrastructure.

5. **Stuxnet(2010):**

   Discovered in 2010, the Stuxnet worm targeted industrial control systems in Iran's nuclear facilities. It exploited vulnerabilities in Windows systems and Siemens PLCs, causing physical damage to the centrifuges used for uranium enrichment.

- **How to reduce the attack surface:**

(ans): We can here reduce the attack surface by following the below points:

1. Adopting a Risk-Based Approach.
2. Implementing Security by design.
3. Developing a skilled workforce.
4. Collaboration and Information sharing.

- **Difference between the IT and OT Security.**

(ans):

IT SECURITY	**OT SECURITY**
Enterprise	Industry
IT more focuses on Confidentiality.	OT more focuses on Safety.
Incident in IT are more frequent got occurred.	Incidents in OT are more destructive which can be not occurred not many times.
In IT the security strengthening process occurs every week.	In OT the security strengthening process occurs every ten years.

- **Features of OT Security:**

(ans): Features of OT Security are as follows:

1. Risk Assessment
2. Operations Protection
3. Operations Management
4. Device Security
5. Site Security
6. Network Segmentation

- **Benefits of our OT Security Solutions:**

(ans):

1. Help to identify, classify and prioritize various business assets based on their value.
2. OT security analyses traffic for potential threats and vulnerabilities and enforces access points.
3. OT security can secure both wired and wireless network access.
4. The solution of OT security help the client to discover the level of trust and monitoring behaviour of any device attached to OT network.
5. Multi-level authentication ensure that only authorized people can access it.
6. Continuous monitoring of OT network gather the data of unknown and new threats and than update the system and enhanced the OT network security.