CYBER SECURITY IN A RAPIDLY EVOLVING SPACE INDUSTRY

—

Challenges in the modern space architectures

Presented by
George Tountas
Senior Manager,
Information Security Management

SES^

—
INTRODUCTION

Agenda

1. **INTRODUCTION TO SPACE / SES**

2. **EVOLVING BUSINESS AND THREAT LANDSCAPE**

3. **THREAT ACTORS**

4. **ATTACK TYPES / EXAMPLES**

5. **WHAT CAN WE DO ABOUT IT**

6. **Q&A**

Introduction

▲ Leader in global content connectivity solutions

▲ More than 30 years and 70 Satellites in 2 different orbits

▲ Our newest generation MEO fleet, O3b mPOWER

▲ Throughputs up to multiple gigabits per second per service.
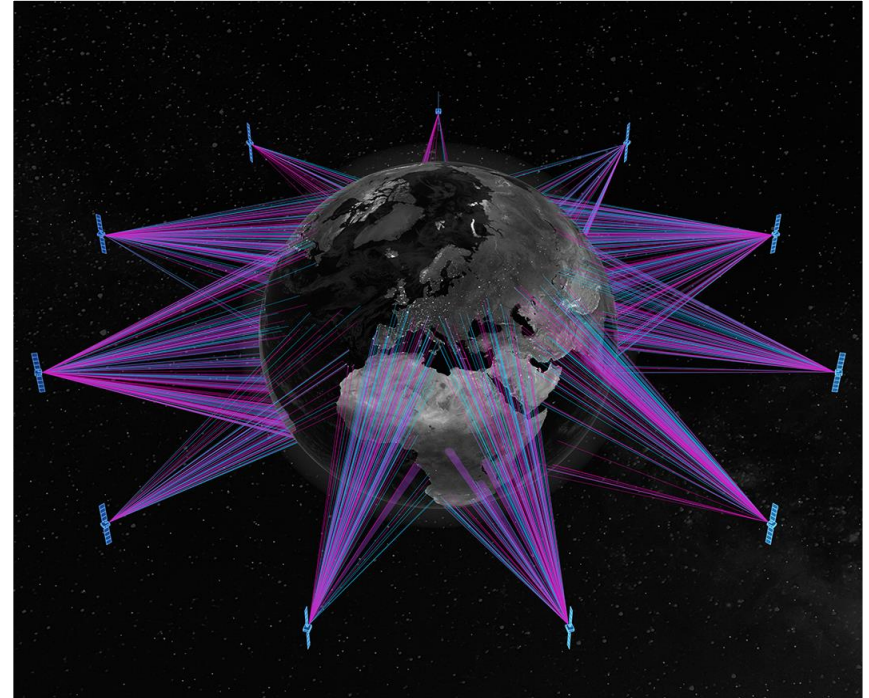
Evolving Business and Threat Landscape

- ▲ Traditional complexities are still driving Cyber Security Risks:
  - Extended use of proprietary systems
  - Long system lifetime
  - Availability is paramount
- ▲ Commercial Space is becoming a Critical Infrastructure and is utilized more and more by Governments and Defence customers
- ▲ Growing complexity and attack surface of Space infrastructures with multiple interdependencies

SES
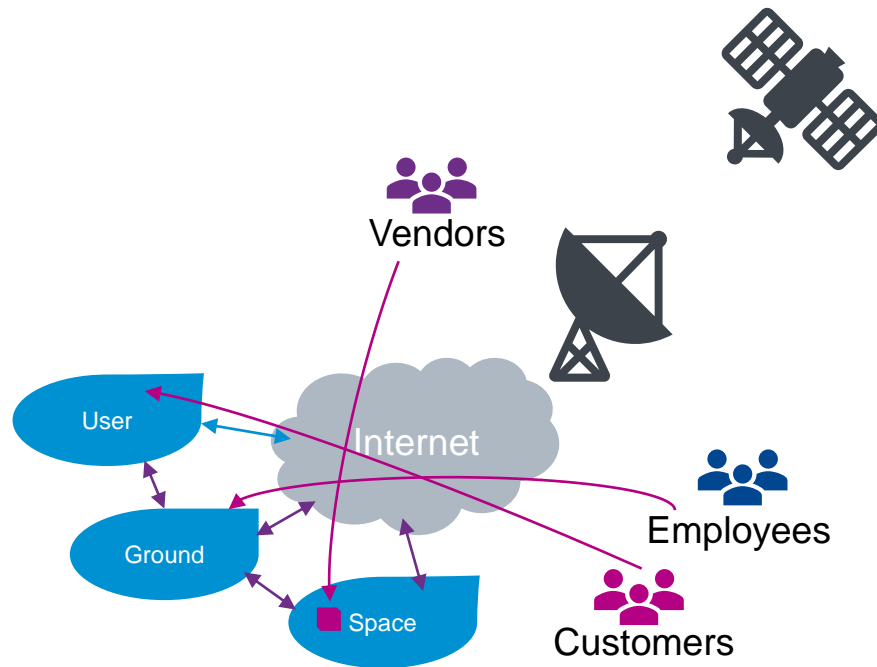
Threat Actors

Cyber Crime
- Opportunistic
- Medium Skills
- Financially Motivated
- Ransomware, Phishing

Hacktivists
- Targeted
- Low-Medium Skills
- Ideologically motivated
- Malware, Destructive

Nation State Actors
- Targeted
- Highly Skilled
- Geopolitical Interests
- Advanced Methods, Persistent / Warfare

Attack Types/Examples

Supply Chain Attacks

Hackers targeted **SolarWinds** by deploying malicious code into its Orion IT monitoring and management software used by thousands of enterprises and government agencies worldwide.
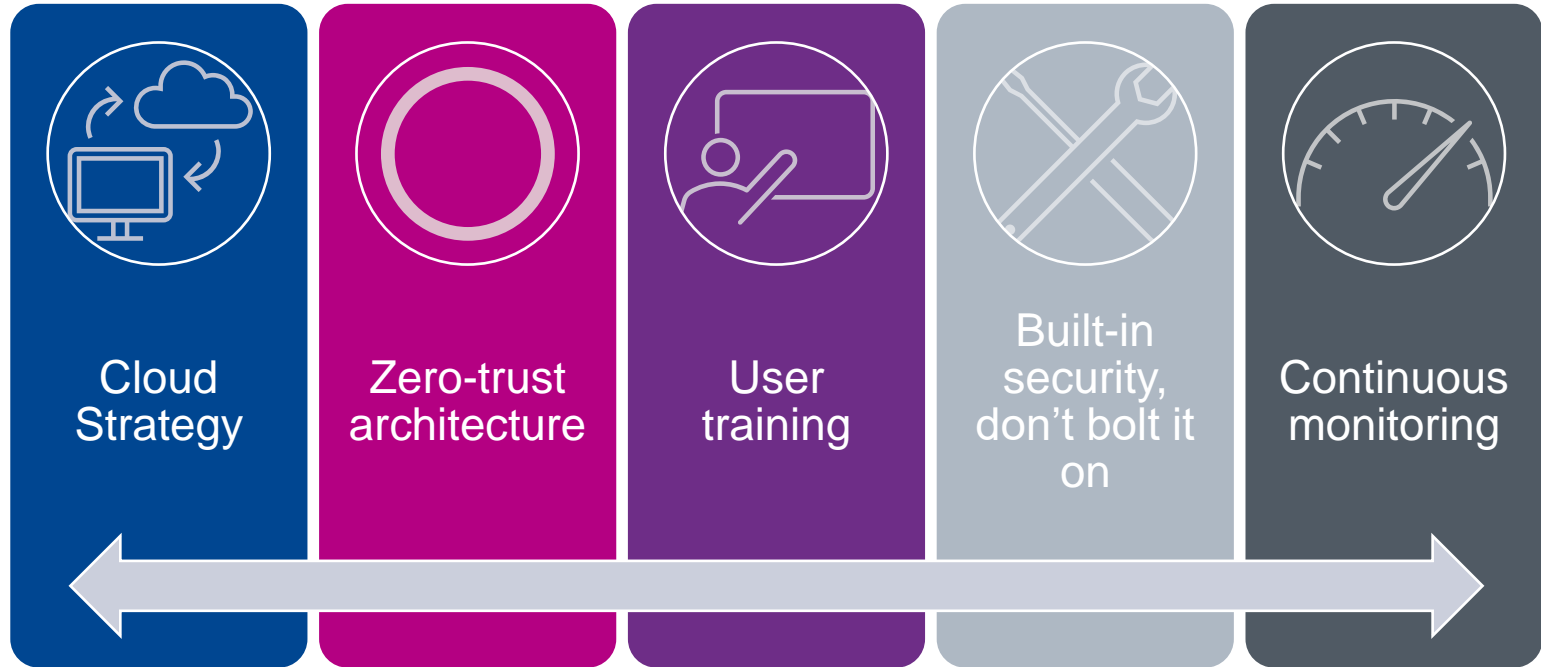
Ransomware

Hackers attacked **Maersk** by deploying ransomware via a Ukrainian tax software, which resulted in $300m cost

VIASAT Hack

In the **Viasat** case, the attackers compromised a virtual private network appliance to gain access to the trusted management part of the KA-SAT network. The attackers then issued commands to overwrite part of the flash memory in modems, resulting in them having to provision more than 30,000 terminals

SES▲

What can we do about it?

Cloud Strategy	Zero-trust architecture	User training	Built-in security, don't bolt it on	Continuous monitoring

SES▲

—
THANK YOU!
QUESTIONS?

SES

George Tountas

george.tountas@ses.com

———