Multi-cloud Security - Issue #2314

As cloud infrastructures become a key element in the telecommunication operator ecosystem, particularly with the 5G rollout becoming a critical business necessity, cloud-focused threats and associated adversarial behaviours, methods, tools, and strategies that cyber threat actors use to plan and execute are part of the attack surface landscape.

In an ecosystem comprised of different network domains, products and business partnerships, the responsibility for managing these different cloud environments necessary to support 5G use cases falls to different organisations, creating a new level of complexities and a new range of security risks. In such an environment, there are additional security principles to be considered. These principles, see Table 2 below, drawn from the collaboration with GSMA FASG [E], intend to address typical cloud associated attacker behaviours, as identified in the widely accepted MITRE ATT&CK® Framework [A],. This framework provides a systematic approach to capture adversarial behaviour targeting cloud environments. Examples of such adversarial behaviours are listed in the Table 1 below.

Attacker behaviour	**Description**
Initial Access	Compromising user administration accounts that are not protected by multi-factor authentication
Evasion	Modifying cloud compute instances in the production environment by modifying virtual instances for attack staging
Discovery	Using open-source tools to discover what cloud services are operating and then disabling them in a later stage to avoid detection
Data Exfiltration	Moving data from the customer's production databases to the hacker's cloud service account or transferring the data out of the Communi cation Service Provider (CSP) to the attacker's private network
Service Impact	Creating denial-of-service availability issues by modifying Web Application Firewall (WAF) rules and compromising APIs and web-based GUIs

Table 1. Cloud attacker behaviours

Multi-cloud Security Principle	**Description**
Policy synchronization	Consistency in applying the right security policies across environments, services, interfaces, and configured resources
Visibility	A common data model approach to capture events and behaviours across all the key compute, storage, network, and applications resources, environments, virtualised platforms, containers and interfaces
Monitoring	Centralisation, correlation, and visualisation of security information across the different cloud environments to provide an end-to-end view and enable timely response to attacks
Automation	Automation of critical activities including cloud security posture management, continuous security assessments, compliance monitoring, detection of misconfigurations and identification and remediation of risks
Access Management	Organisation of a wide range of users including administrators, testers, DevOps, and developers and customers should be organise d into security groups with privileges appropriate to different resources and environments
Security Operations Model	Augmentation of security services provided by cloud service providers with the vetted third-party and/or open-source tools and services, all incorporated into the established overall security operations model

Table 2. Multi-cloud security principles

If telecommunication operators decide to run some of their public telecom network functions in a multi-cloud environment, and specifically in public clouds, the industry will need a set of new standards and new security tools able to regulate the interactions between participating parties. For instance, it seems to be sensible to eliminate access to some restricted areas altogether rather than merely prohibit it. The ETSI standard TS 103 457 "Interface to offload sensitive functions to a trusted domain" [B] provides extra security requirements for public clouds to offer telecommunication operators the option of running public telecom network functions in public clouds.

TS 103 457 introduces a concept of an LTD (Less Trusted Domain) and an MTD (More Trusted Domain) and specifies the TCDI (Trusted Cross-Domain Interface) to standardise secure interactions between them. The standard defined the following elementary functions of TCDI:

- Connection and session management
- Data and value management

- Transferring cryptography functionality
    - Entropy request
    - Encryption keys request
    - Trusted timestamping
    - Secure archive
    - Secure storage
- Search capabilities

As described in Sec. 1 (Scope) of TS 103 457 it "… specifies a high-level service-oriented interface, as an application layer with a set of mandatory functions, to access secured services provided by, and executed in a More Trusted Domain. The transport layer is out of scope and left to the architecture implementation ". The standard provides extra security for sensitive functions down to individual Virtual Machines or Containers. As such, it is recommended that the relevant components of reference models, reference architecture, reference implementations and reference compliance take notice of this standard and ensure their compatibility, wherever possible.

On the Container side, the NIST Internal Report (NISTIR) 8320A "Hardware-Enabled Security: Container Platform Security Prototype" [D] explains an approach based on hardware-enabled security techniques and technologies for safeguarding container deployments in multi-tenant cloud environments. It also describes a proof-of-concept implementation of the approach – a prototype – that is intended to be a blueprint or template for the general security community.

REFERENCES

[A]	MITRE ATT&CK® Framework	MITRE ATT&CK: Design and Philosophy, MITRE, March 2020
[B]	ETSI TS 103 457	CYBER; Trusted Cross-Domain Interface: Interface to offload sensitive functions to a trusted domain
[C]	HardenStance Briefing No. 22, 28th March 2019	"ETSI Secures Public Clouds for Telcos"
[D]	Draft NISTIR 8320A	Hardware-Enabled Security: Container Platform Security Prototype
[E]	GSMA FS.40 2.0	FS.40 CR1002 CR to Reflect 3GPP R16 Developments