E2E NFV Security

Why automating desired results is the big challenge
Topics of Discussion

- Security results: Desired state
- Security automation unique to NFV
- Threat landscape dynamics
- Continuous threat intelligence
- Lifecycle NFV security automation
- Action plan for automating security
- Resources
Desired NFV Security State

- Automating the **secured provisioning and maintenance** of dynamic network services throughout the NFV lifecycle
- Minimizing downtime and preventing data loss **through actionable threat intelligence tied to infrastructure threat profiles**
- Supporting a mix of **cloud-aware/stateless and state-dependent applications** across multiple tenants and providers
- Seamless, **highly available application acceleration and load balancing services** supporting multiple locations
- **Automated compliance across security and performance SLAs**
Automate to Hyperscale

**Traditional Telco Environment**
- Configure appliances
- Siloed, fragmented automation
- Hardware-defined
- Scale up
- Avoid failures
- Manage configs

**Hyperscale Cloud Environment**
- Program the system
- Fully automated
- Software-defined
- Scale out
- Assume failure
- Manage relationships
DevOps Automation

Automate-first mindset applied to everything
Every change is scripted
Management shift: from operations organization to engineering organization

Development and operations are run as an engineering process
Uniquely NFV

Automate security through:

- API’s and DevOps
- Attestation of enclaves
- Topology validation
- Hypervisor introspection
- Workload orchestration
- Control/data plane isolation
- Multi-provider management
Threat Dynamics

• Threats are the most dynamic force in NFV security!
• Threat Landscape spans from open-source to COTS to proprietary technologies and processes
• *Continuous Threat Intelligence* must be operator, subscriber and technology adapted
• Administrative threat is now multi-party
• Internet of Things (IoT) will further escalate threats!
Trusted Control and Data automation expressed and enforced by policy across technologies and processes:

- Distributed storage
- Availability zones
- Compute Clusters
- Routing and Flows
- Load Balancing
- API’s
- ...

*Due to substantial complexity, trust must be automated*
NFV Security Lifecycle

Workflow processes:
- Operational
- Administrative
- Audit / Compliance
- Subscribers
- Devices / Things
- Ecosystem

Contextual and Dynamic
Action Plan

**Automation Services**
- Programmable network controls
- Interoperability through APIs
- Scripting from proactive to reactive
- Orchestrated workflow lifecycles
- Service chaining of dependencies
- Fault domain management
- Enclaves for crypto/certs/keys
- Reliability, resiliency, redundancy!
- Analytics-driven innovations

**Validation and Attestation**
- Predictive threat intelligence
- Pentesting of network services
- Required security always active
- Prohibited functions denied
- Identity and anonymity balanced
- Isolation of multiple admin domains
- Jurisdictional boundaries maintained
- Data sovereignty maintained
- Telemetry proves business value
Resources

ETSI NFV
- Security Problem Statement
- Security and Trust Guidance

OpenDaylight
- a major foundational element for NFV

OPNFV
- an open platform to accelerate NFV

Whitepaper
- Best practices for multi-zone and multi-region cloud integration
Thanks!

Kurt Roemer
Chief Security Strategist
Citrix

kurt.roemer@citrix.com

Citrix works with partners in a wide range of specializations, including network security, network visibility, mobile device management, identity management and web content security, to deliver best in-class software-defined networking solutions. The result is a dynamic network architecture that supports virtualization and cloud strategies to increase agility, simplify operations and reduce costs.