Security white paper consultation (2)

1


GÉANT Security Whitepaper 2018 - 2022
Security Baselining
Standards, Frameworks, best practices, benchmarking
(Managed) Security Products & Services
DDOS mitigation, certificate services, crypto technologies
Legal Compliance
GDPR, NIS guideline, eIDAS, best practices
Management of Risk
Risk analysis, threat assessments, threat intelligence sharing
Training and Awareness
Develop new trainingmaterials, share best practices
Incident respons, Business continuity and crisis management

Security baseline

- CMM levels
- (Periodic) benchmark against ISO, etc
- Model for comparing baseline with management goals
- Nist 8xx-xx
- Upcoming European standards competing with ISO

Security Baseline

Security baseline ideas?

Policy templates/examples

"default" ISMS

A common mechanism for evaluating security posture - useful for benchmarking

Guide to apply the baseline for an NREN (e.g. where/how to start with ISMS)

Standards/frameworks in easy terms (explanations)

Developping an integrated European Standard considering IT Servicemanagement, Information Security-Standards like ISO20k, ISO27k, NIST, GDPR

Few standards selection and analysis for Policies creations

Benchmarking your NREN to others

Consider baselining for our clients (Universities) also (not sure if this is scope or just NRENs) - it would be equally of interest to NREN

Management of Risk

— Risk catalogue

— Risk assessment template/guidelines

— Risk management template/guidelines

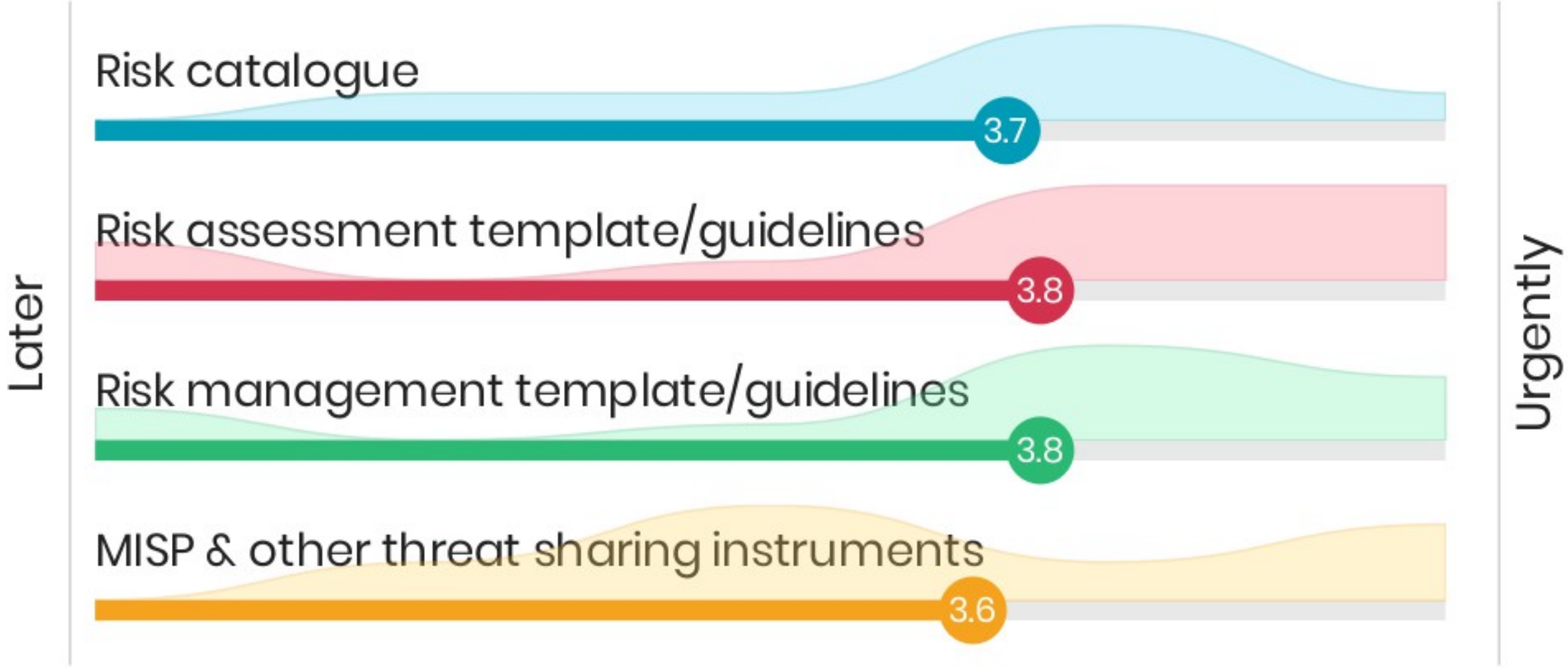
— MISP & other threat sharing instruments

— Risk management outside Europe

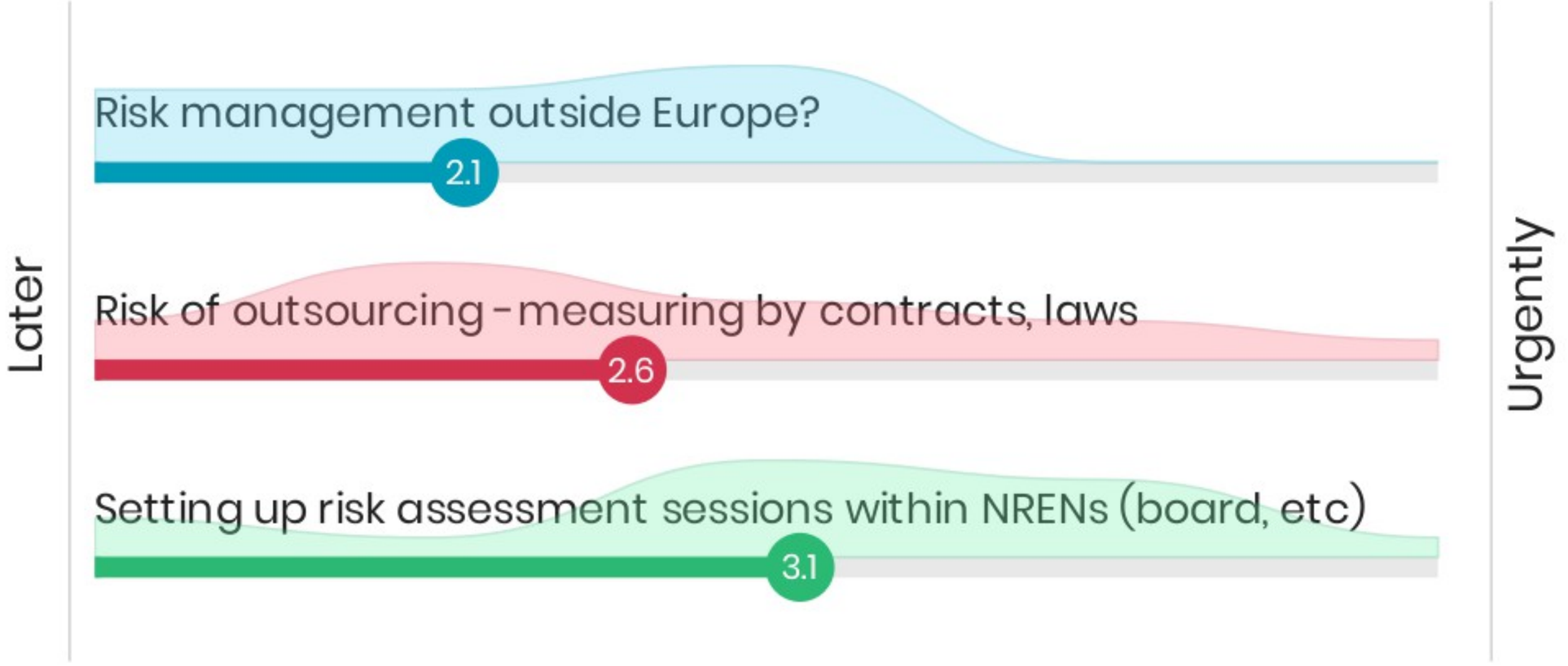
— Risk of outsourcing - measuring by contracts, laws

— Setting up risk assessment sessions within NRENs (board, etc)

Management of Risk



Management of Risk



Management of Risk ideas?

Identify and share best practices
Establish collaboration mechanism

templates for risk acceptance/temp authorized non-compliance

It could be part of the Information security Management but also on General risk Management -> ISO 31k

3

Legal compliance

— Non-legal compliance framework (Sirtfi, ISO, etc)

— Multiple contracts - same service

— Guidelines for big data tranfers

— Data register (art.30 GDPR)

— Security issues checklist GDPR

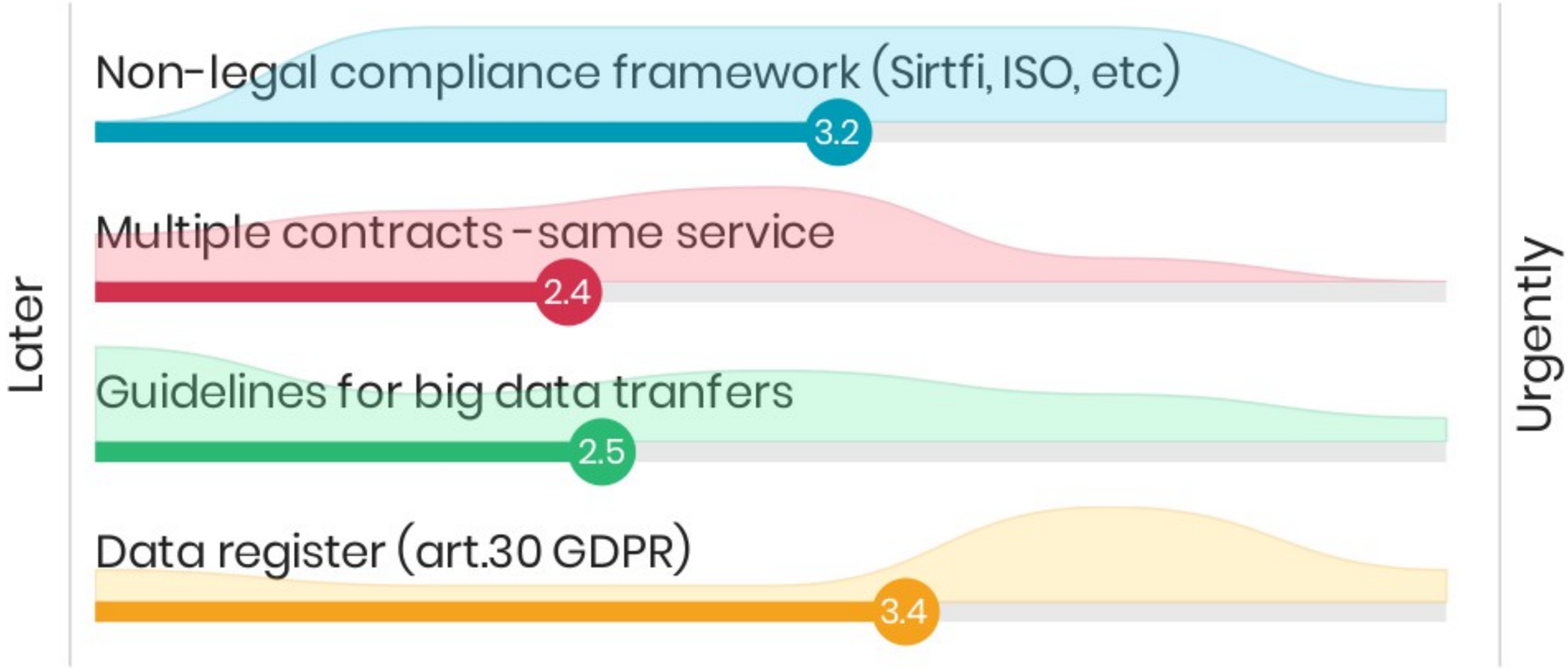
— Export restrictions (Malware exchange)

— ePrivacy Directive

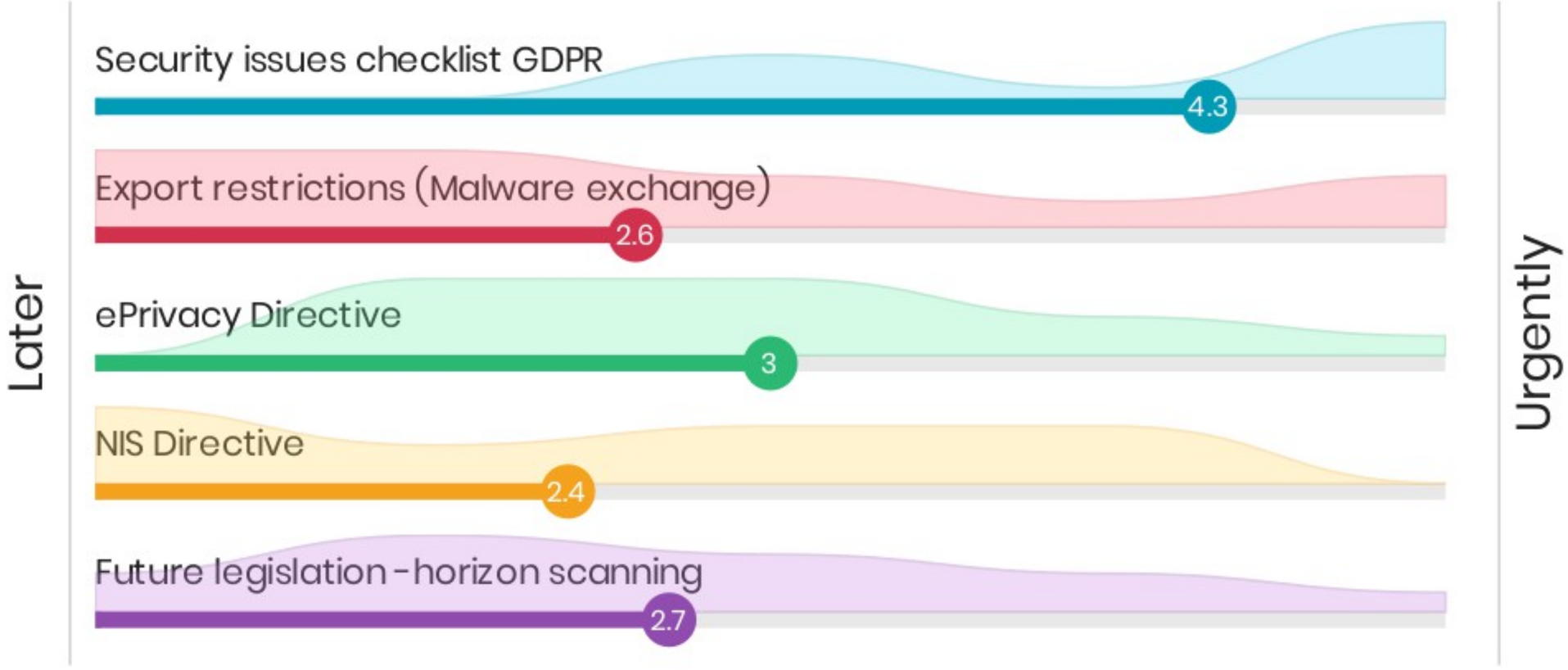
— NIS Directive

— Future legislation - horizon scanning

Legal Compliance



Legal compliance



Legal compliance ideas?

Look at influencing upcoming legislation

Make dedicated workshop on our posibilities of influencing future legislation

we should investigate the GDPR and security laws and their consequences regarding our operational processes and IT-Services -> check laws

Training and awareness

— Platform shared: awareness phishing

— Protecting personal data workshop

— Crisis management training/workshop

— Management/board training

— Setting up awareness tools catalogue

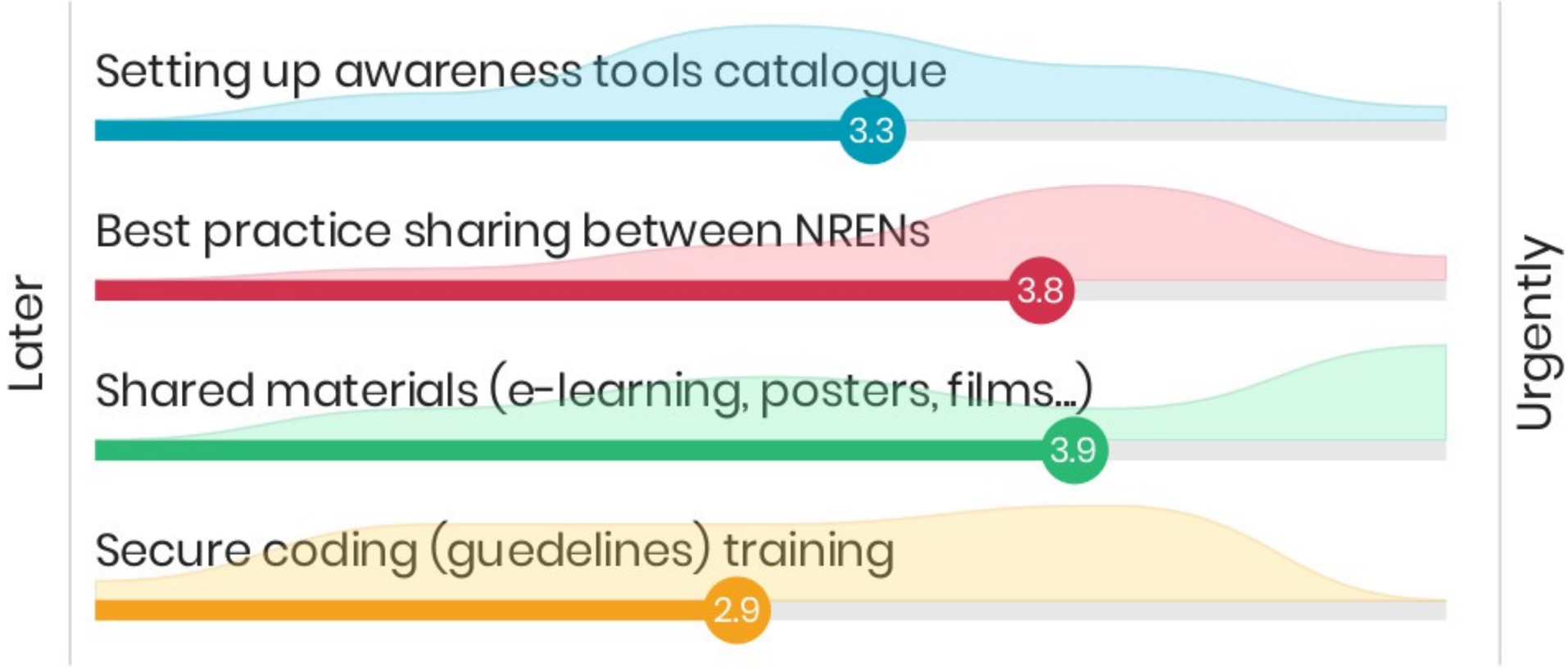
— Best practice sharing between NRENs

— Shared materials (e-learning, posters, films...)

— Secure coding (guedelines) training

Training and Awareness

Training and Awareness



Training and awareness ideas?

TRANSITS like training for management level (crisis management 101)

Framework for spheres, divided into sub-spheres, and examples of each

Developping the Secure Code Training and secure Code Audit to general Services for NRENs, universities etc.

Having a range of basic security awareness training courses would be useful - also completion stats/reporting would be valuable.

Collaboration with local (countries) CERT/CIRT agencies/teams doing join shared actions

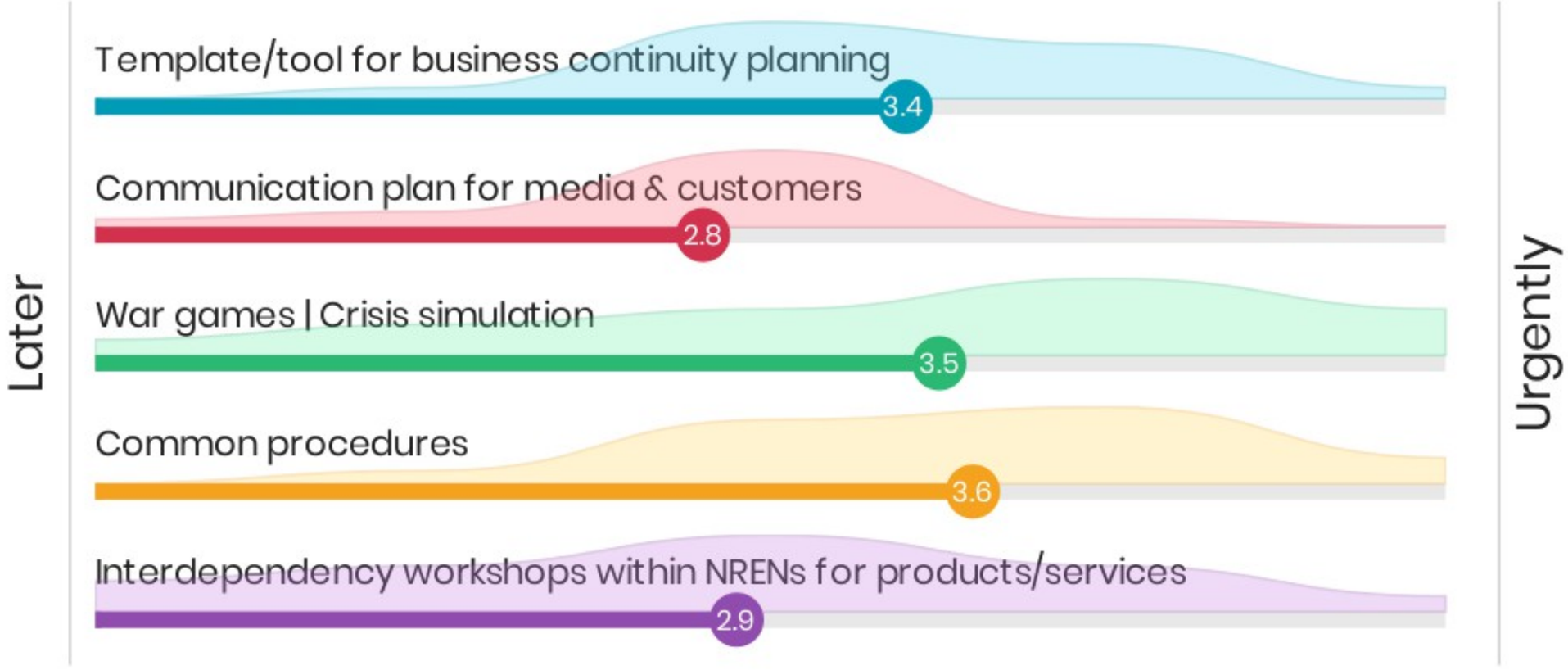
common tool, where you can meassure whether people read your policies

Incident response, business continuity, crisis management

- Template/tool for business continuity planning
- Communication plan for media & customers
- War games | Crisis simulation
- Common procedures
- Interdependency workshops within NRENs for products/services

Mentimeter

Incident response, business continuity, crisis management



Incident response, Business continuity, crisis management ideas ?

Working group on information sharing and tooling - discuss/collab on technical controls

Developping an integrated, harmonized incident Management process, combining the current different approaches and consideriing GDPR

2

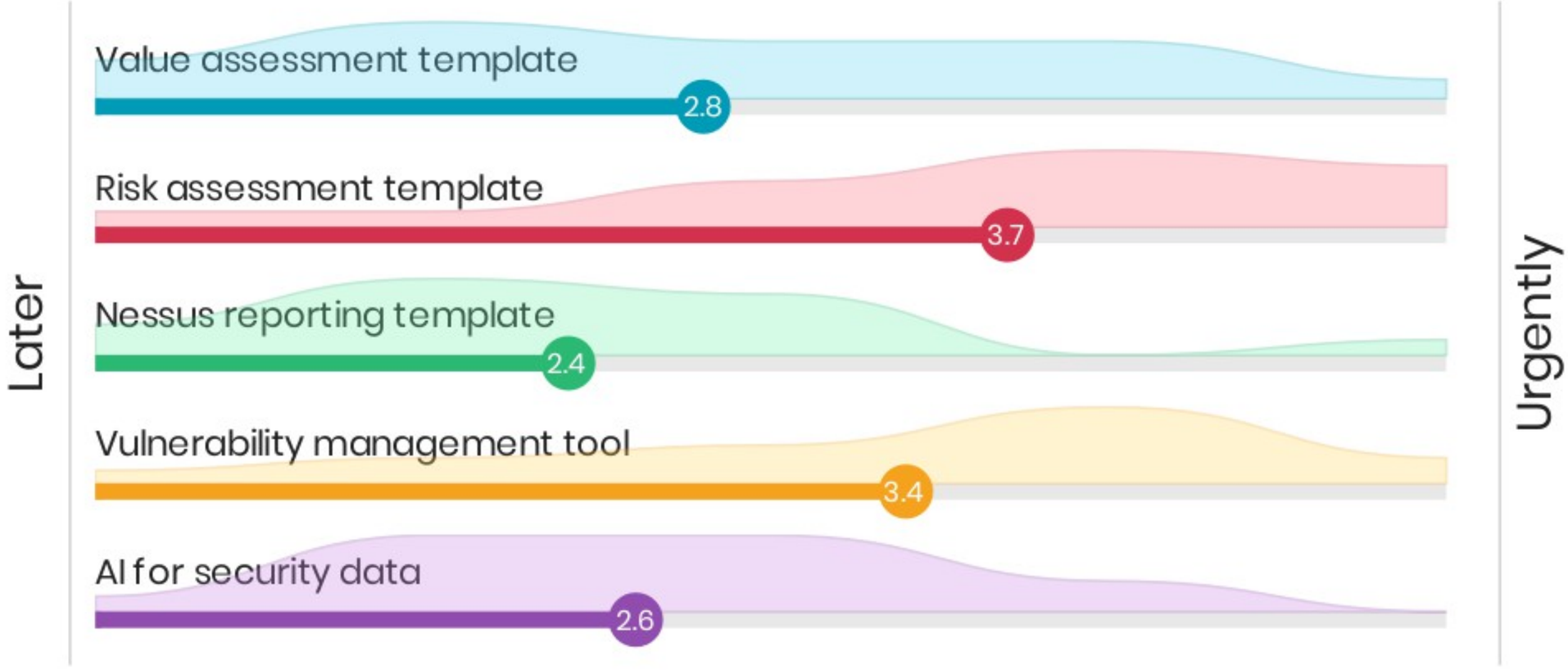
Products and Services

- Value assessment template
- Risk assessment template
- Nessus reporting template
- Vulnerability management tool
- AI for security data
- Shared/managed (community) SOC
- Blockchain

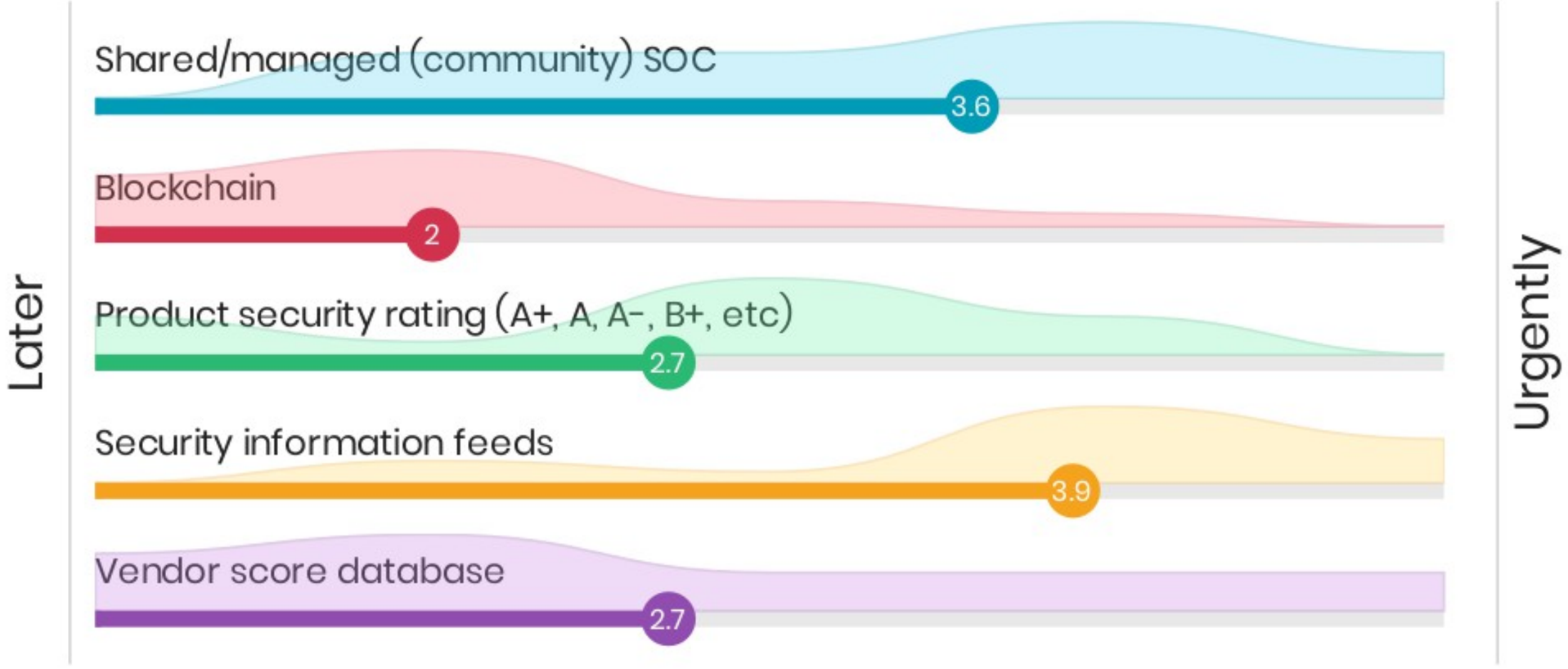
Products and Services

- Product security rating (A+, A, A−, B+, etc)
- Security information feeds
- Vendor score database
- Standards for procuring (networking) equipment
- European NRENs threat overview
- Network automation, SDN, virtualisation

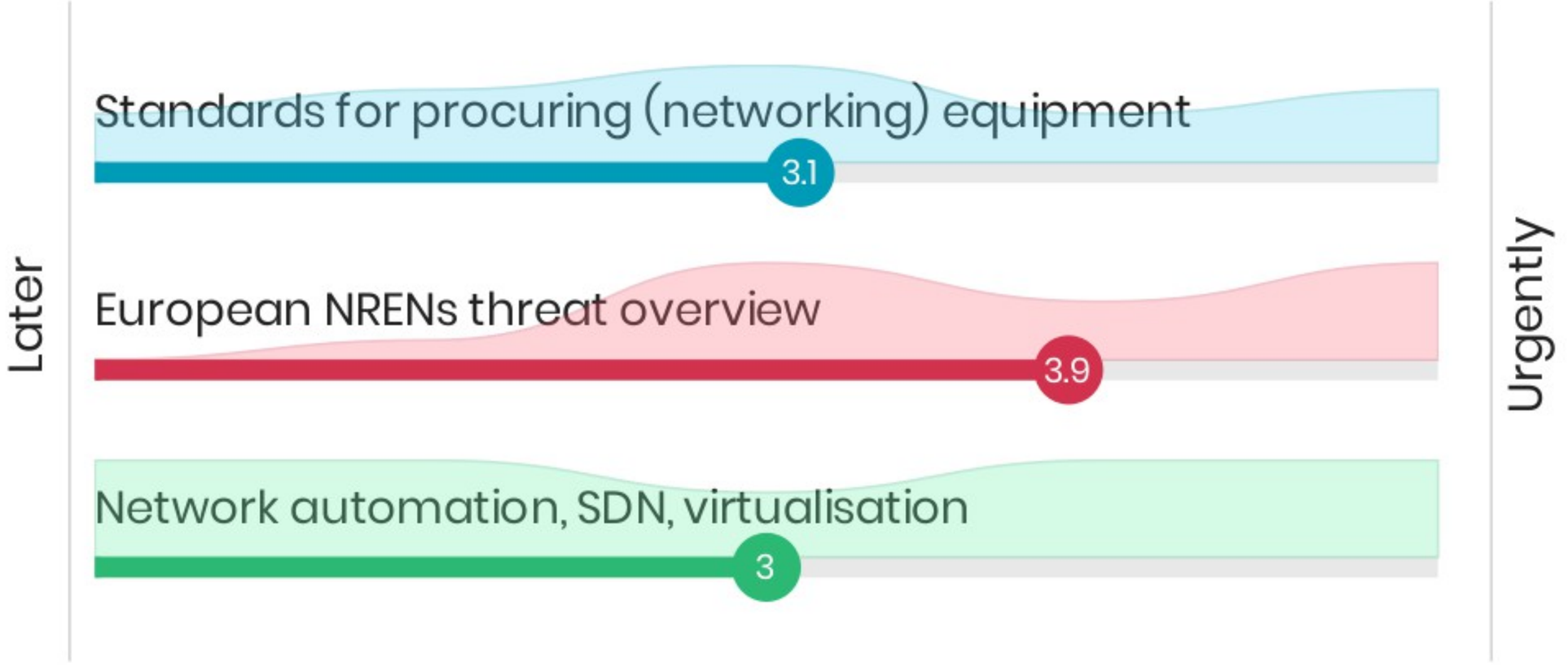
Products and Services



Products and Services



Products and Services



Products and Services ideas?

Generalized Multi-Domain FirewallOnDemand interface supporting further (non FlowSpec) DDoS mitigation technologies (washing machines, SDN/

EDU VPN: make VPN technology commonly available, by building better and more user-friendly tools (Secure and privacy preserving access fro

RepShield (correlated security events and reputation score for e.g. IP addresses) further development and distibution in Multi-Domain manner

Tools to pull threat info out of / process netflow data to indicate malicious activity

IoC detection and sharing at institutional level

Also: FirewallOnDemand as Multi-Domain interface for DDoS mitigation across multiple domains (GEANT, NRENs, institutions)

organizational and technical interop of NRENs and GEANTs ddos analsyis and mitigation platforms

-Evaluating pentesting as a service

Information sharing platform

Thank you!