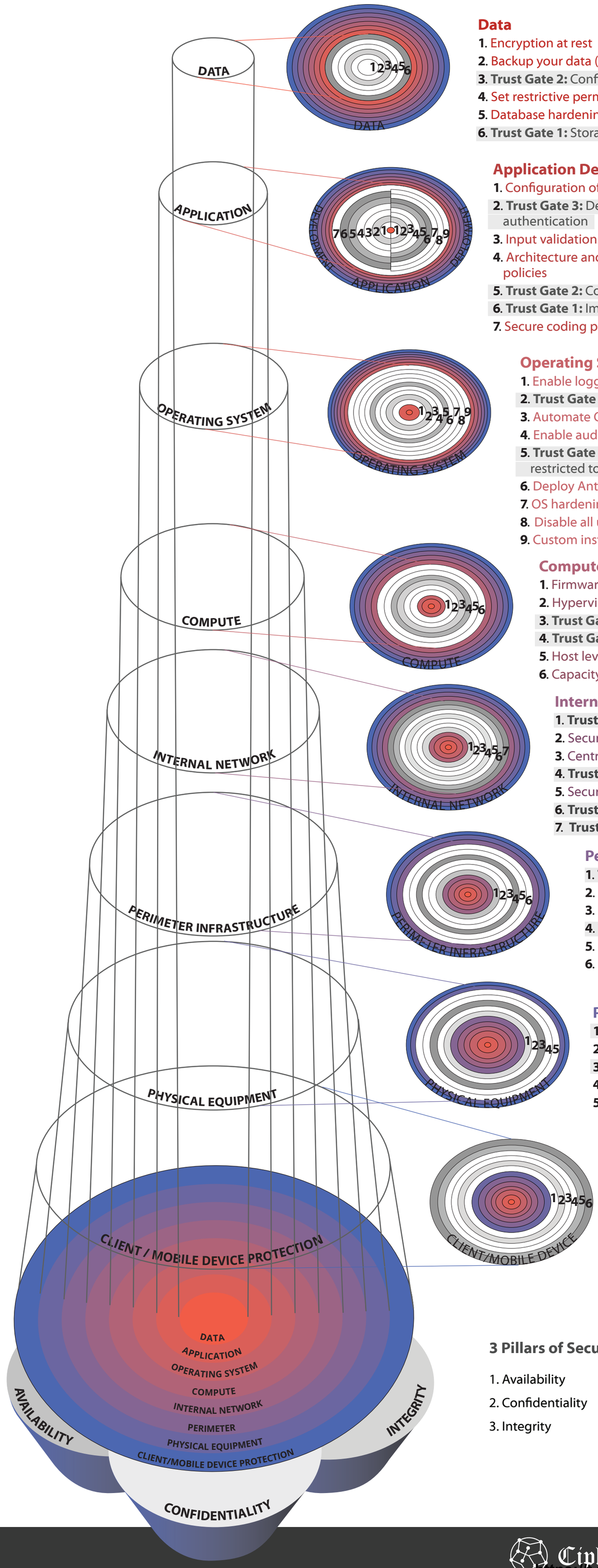
Zero Trust security: Multi-layered protection against cyber-threats



Data

1. Encryption at rest
2. Backup your data (and test your backups)
3. **Trust Gate 2:** Configure data access rights
4. Set restrictive permissions (at field level)
5. Database hardening – using best practices guidelines
6. **Trust Gate 1:** Storage infrastructure access

Application Development

1. Configuration of application level logging
2. **Trust Gate 3:** Design to support and enforce multi-factor authentication
3. Input validations & error handling framework
4. Architecture and design level alignment with applicable security policies
5. **Trust Gate 2:** Code for identity and access management policies
6. **Trust Gate 1:** Implement API Authentication
7. Secure coding practices

Application Deployment

1. Include security testing in deployment pipeline
2. **Trust Gate 3:** Practice principle of Least Privileges
3. Care for and configure to protect privacy
4. Configure for a purpose - discard default configurations
5. **Trust Gate 2:** Encrypt identities and secrets
6. **Trust Gate 1:** Enable SSO / multifactor authentication
7. Application level patch update schedule
8. Monitor for security outliers
9. Deploy Web Application Firewall

Operating System

1. Enable logging and auditing
2. **Trust Gate 2:** Restrict processes runing with privileged rights
3. Automate OS patching
4. Enable auditing for all critical OS resources – files / directories / processes
5. **Trust Gate 1:** Layered Privileges access - secure, logged, monitored, restricted to necessary and sufficient to perform defined tasks
6. Deploy Anti-malware
7. OS hardening using CIS (or equivalent) benchmarks
8. Disable all unwanted services
9. Custom installation of OS

Compute

1. Firmware update policies
2. Hypervisor, orchestration platform and Host OS patching management
3. **Trust Gate 2:** RBAC – for underlying IaaS, PaaS
4. **Trust Gate 1:** Use ACLs for limiting host access
5. Host level IDS
6. Capacity utilization monitoring

Internal Network

1. **Trust Gate 4:** Intra-network ACLs
2. Securely configure of routing / switching and VLAN
3. Centralized logging
4. **Trust Gate 3:** Design for role-based network segmentation
5. Security fixes for networking OS
6. **Trust Gate 2:** Deny by default - Network Security Groups and ACLs
7. **Trust Gate 1:** Configure network ACLs and monitor for unauthorized access

Perimeter Infrastructure

1. **Trust Gate 2:** VPN for inbound access
2. DDoS protection
3. Network IDS
4. **Trust Gate 1:** Network level firewall
5. Secure DNS configuration
6. Monitor for intrusion, DDoS and DNS attacks

Physical Euipment

1. **Trust Gate 2:** Locked and restricted access to server cages and racks
2. Surveillance via security cameras and biometrics readers
3. **Trust Gate 1:** Biometric access with visual verification
4. 24 x 7 Guarded physical access
5. Monitor for unauthorized access

Client / Mobile Device Protection

1. Encryption of data stored in mobile
2. **Trust Gate 3:** Enable App level passwords for Enterprise Mobile Apps
3. Client level anti-malware
4. Auto-patch apps and client OS
5. **Trust Gate 2:** Deploy supervised mobile devices
6. **Trust Gate 1:** Restrict device access via password / fingerprint / face recognition

3 Pillars of Security

1. Availability
2. Confidentiality
3. Integrity

Zero Trust Security is the NextGen Security model to protect against the growing sophistication of cyber threats. In this era of speed, 24 x 7 work 'on-the-go,' and an equally sudden and jolting halt to global mobility amid the global COVID-19 pandemic, IT security models must be able to quickly adapt to the demands of extreme situations with minimal disruption to 'business-as-usual.'

https://t.me/learningnets