Securing Critical Infrastructure With Zero-Trust Security Model

stc Kuwait cyber security department
November , 2021

Agenda

01. What is Zero Trust?
02. Zero-trust security Model importance for Critical Infrastructure
03. Zero Trust Access Control Strategy
04. Sample Attack Approach with Zero Trust Model
05. The Time of AI & ML based cyber security systems for critical infrastructures
06. References

01

What is Zero Trust?

Trust No One

All access must be authenticated authorized and VERIFIED ALL THE TIME

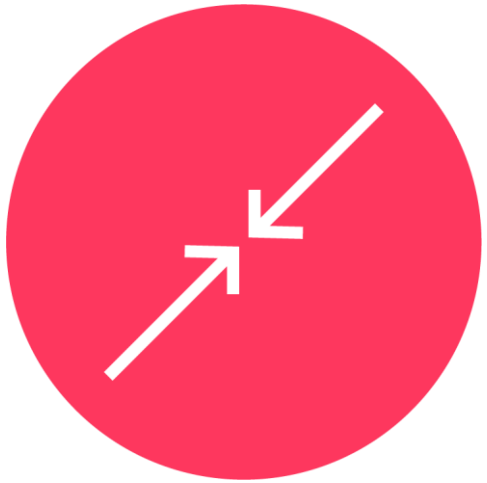
stc

IT/OT environment evolving

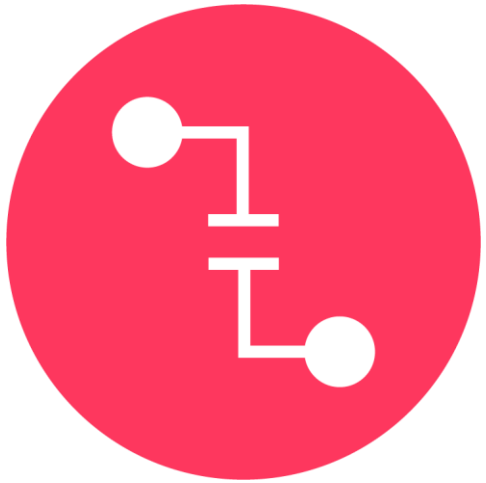
Users are ~~employees, contractors~~	→	Employees, contractors, partners customers
~~Corporate managed devices~~	→	Bring your own devices and IoT
~~On-premises apps~~	→	Explosion of cloud apps (Azure, Blockchain, E-Government integration…)
~~Corp network and firewall~~	→	Expanding Perimeters
~~Local packet tracking and logs~~	→	Multi sources of signal

Zero Trust Core principles

Verify explicitly



Use least privilege access



Assume breach

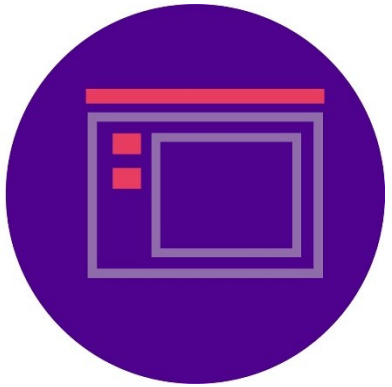
ZERO TRUST

stc

Zero Trust across the digital estate

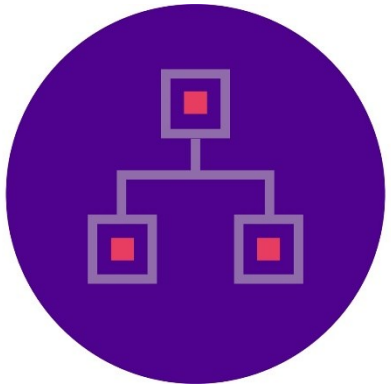
Identity

Devices

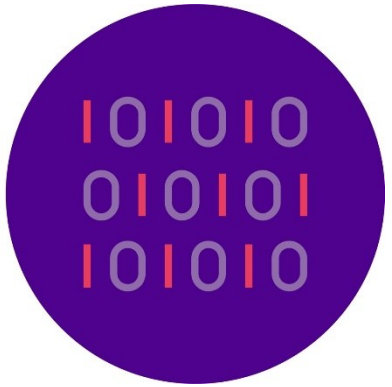


Apps

Infrastructure



Networking



Data

Identities

Zero Trust Objective:

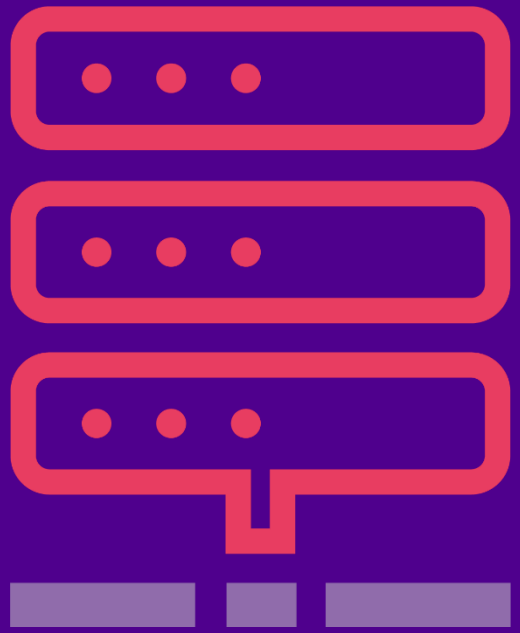
Verify and secure every identity with strong authentication and keep an eye on users during the session.

Devices

Zero Trust Objective:

Allow only compliant and trusted apps and devices to access data, and keep device under monitoring while connected to the network

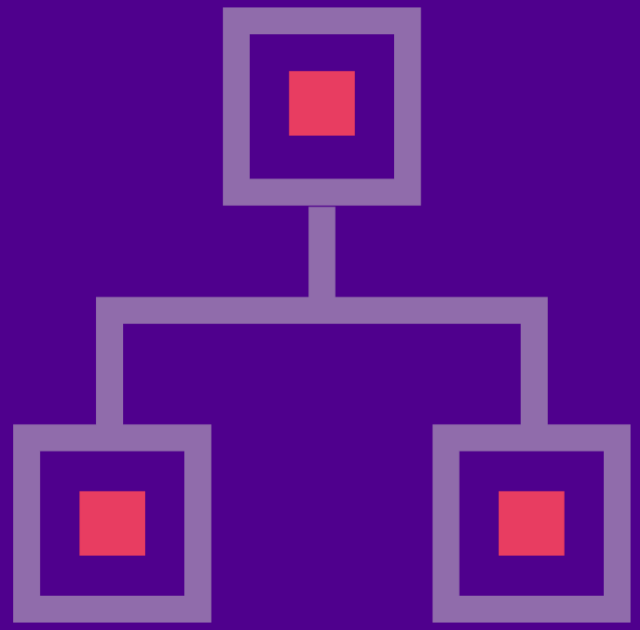
stc



Infrastructure

Zero Trust Objective:

Harden defenses and detect and respond to threats in real time.



Network

Zero Trust Objective:

Move beyond traditional network security approaches, Utilize AI and ML traffic analysis.

stc

Zero Trust Security Model Definition

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries.

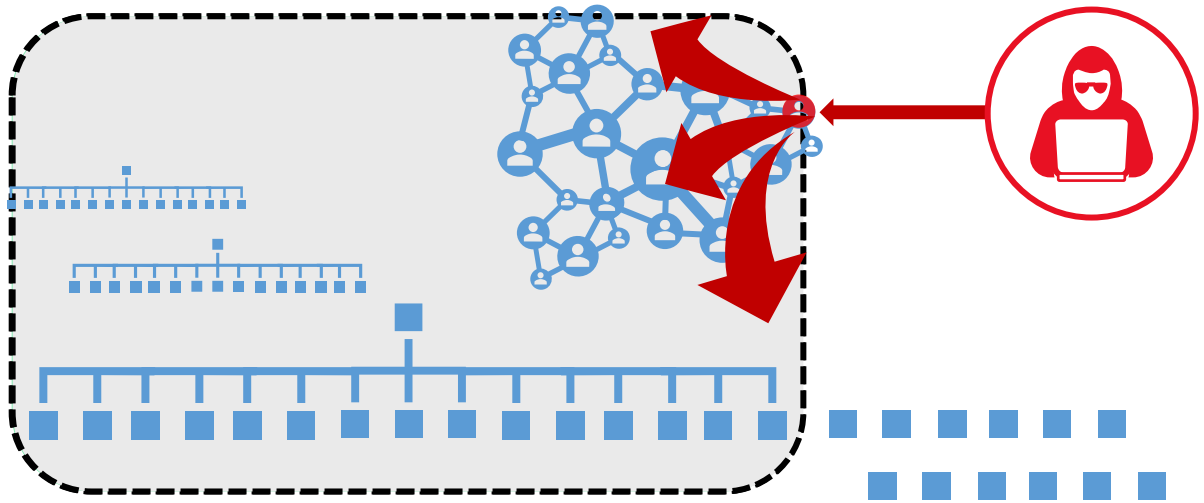
Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).

References: - NSA - National Security Agency - PP-21-0191 | February 2021 Ver. 1.0
- NIST - National Institute of standards & Technology SP 800-207, Zero Trust Architecture

02

Why Zero-trust security Model important for Critical Infrastructure?

Why Zero-trust security Model important for Critical Infrastructure?

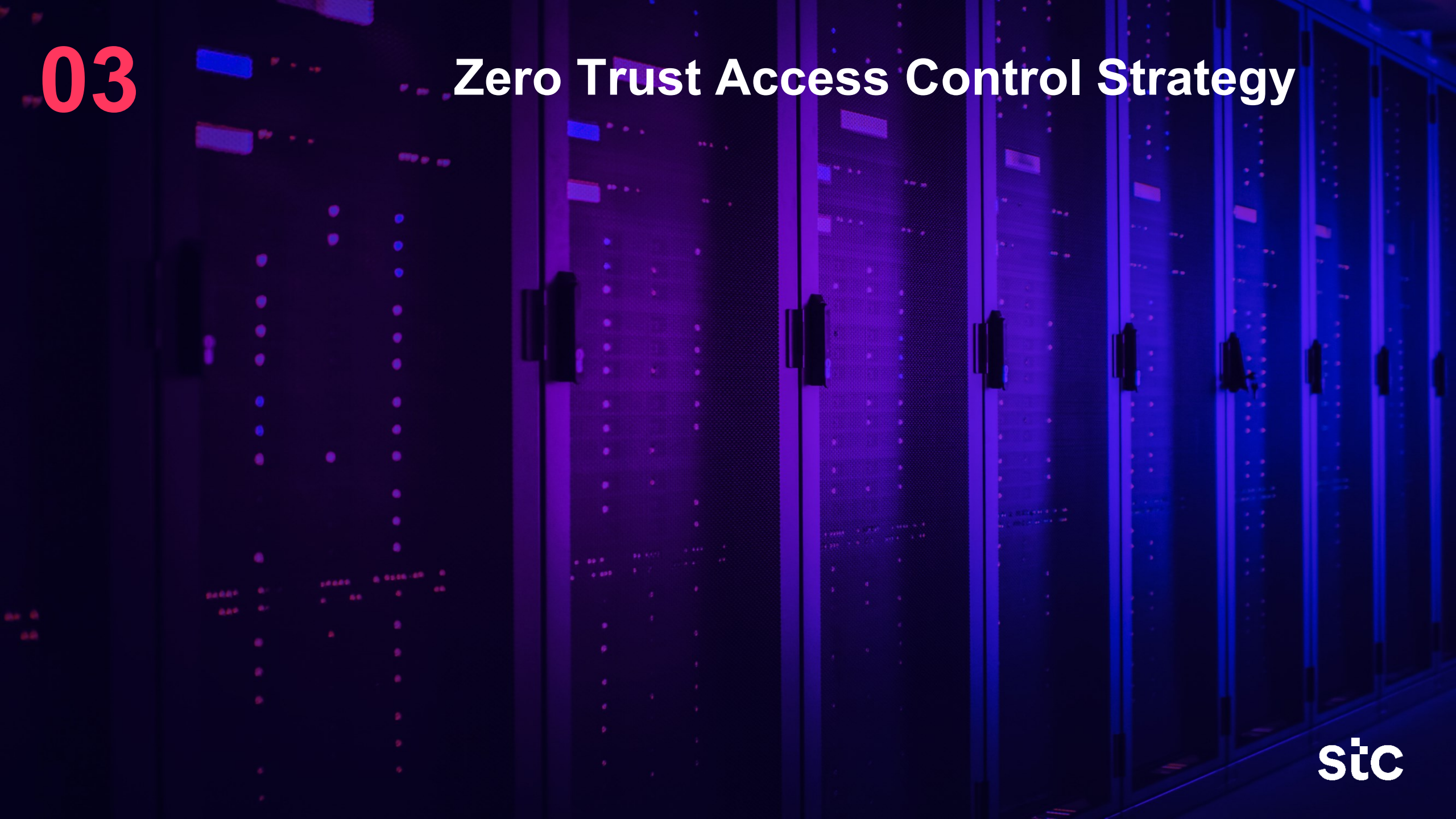


1. **Environment Security became Complex**
   - Many Devices, Users, & Connections
2. **No More "Trusted network" security strategy**
   - Initial attacks were network based, now it target everything including users identities.
3. **Assets increasingly leave network**
   - BYOD, SaaS, Contractors & 3rd Parties
4. **Attackers shift to identity attacks**
   - Phishing and credential theft

stc

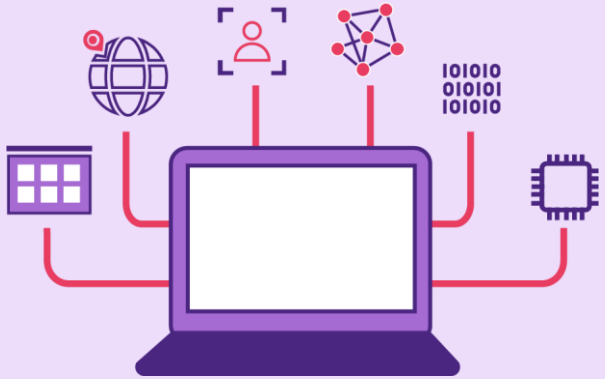
Why Zero-trust security Model important for Critical Infrastructure?

- Increased visibility
- Faster detection of internal attacker/compromised accounts
- Reduces lateral movement after attack
- Reduces alerting time once an attack has occurred
- Limit post attack damage



03 Zero Trust Access Control Strategy

Never Trust. Always verify.

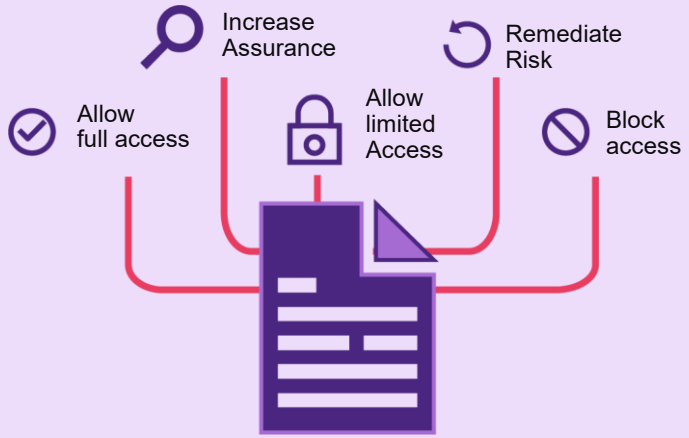


Signal

to make an informed decision

Device Risk
Device Management
Threat Detection
and more…

User Risk
2FA Authentication
Behavior Analytics
and more…



Decision

based on organization's policy

Apply to inbound requests
Re-evaluate during session

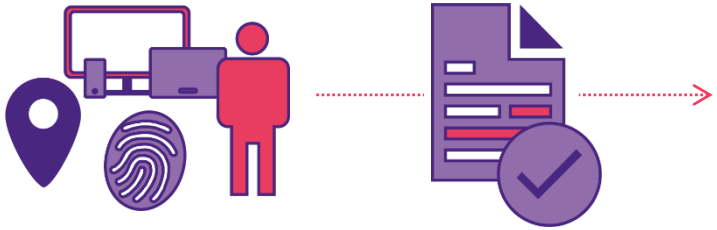
Enforcement

of policy across resources

Based on session monitoring and evaluation

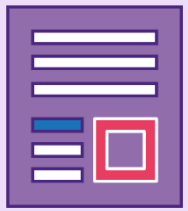
Zero Trust Extend policy enforcement into the session level

Continuous policy assessment and enforcement

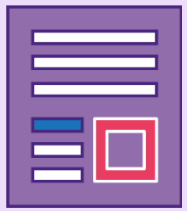


In-session monitoring and policy enforcement

Access Data



Edit files



Run Commands/ Process

User Risk

User Risk

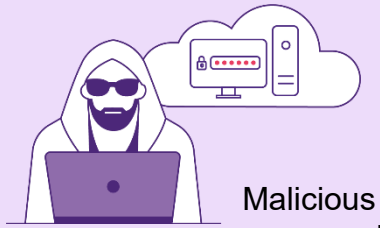
Update user's session risk through additional evaluation

User behavior analyzed against session policy

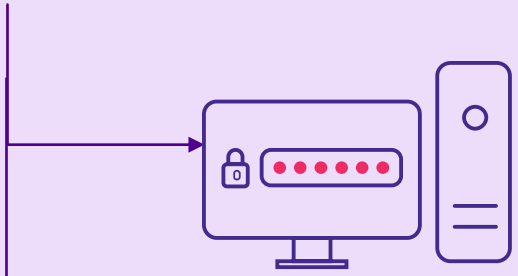
Risky user behavior logged for future analysis and Investigation

Sample Zero Trust remote exploitation scenarios where most attempts would have been successful in non-Zero Trust environments.

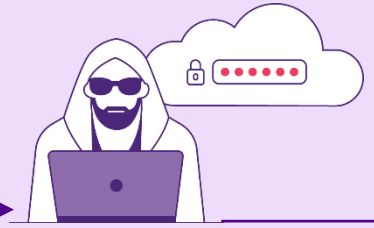
Access Method



Malicious actor compromises user's device and credentials

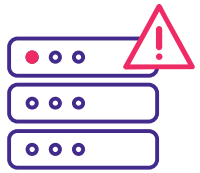


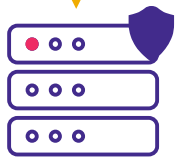
Access via user's device

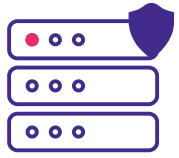


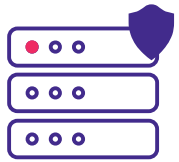
Access via malicious actor's device using user's stolen credentials

Attempts to Access Network Repositories (Servers & Software)









Allowed: User role and device are authorized to access specific data based on policy and context

Blocked: Lateral movement prevented by segmentation and default-deny policy

Blocked: Blocked: User role is not authorized access

Limited: Access to application or service is limited based on least privilege

Blocked: Dynamic analytics detect suspicious activity by user account and block access

Blocked: Device is not authorized

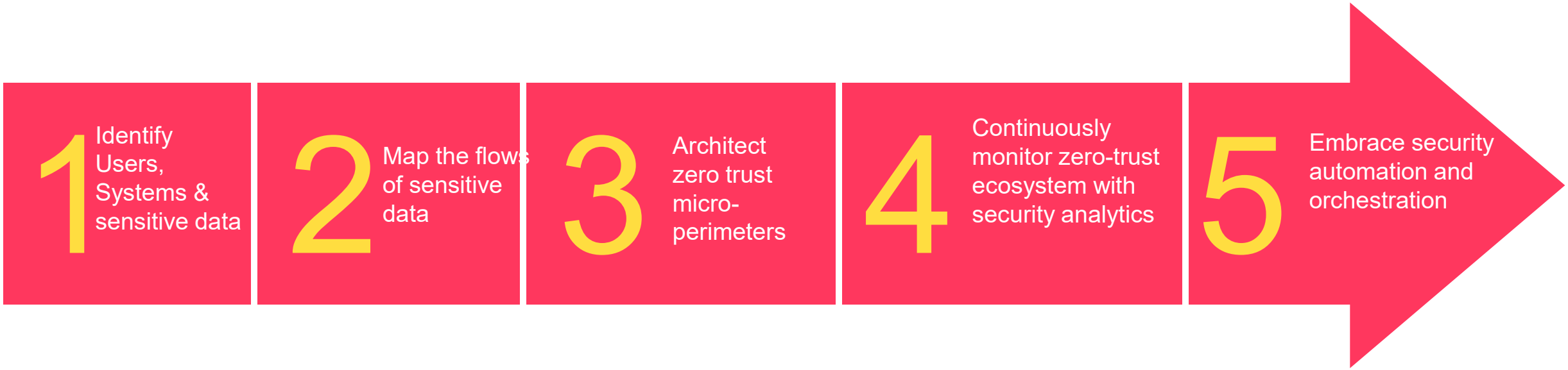
Visibility Analytics

Logged analysis detects attempts

04 Zero Trust Model Adoption Approach

Forrester’s Five Steps to adopt Zero Trust

As per Forrester Zero trust adoption strategy, the below five mile stones to be translated into initiatives:



05

The Time of AI & ML based cyber security systems for critical infrastructures

Why AI & ML based Cyber security systems?

There are five core use cases that Artificial Intelligence support to improve the cyber hygiene and operational excellence:

Incident Analysis

AI able to perform the incident analysis to provide in-depth information on the incident impact, who the threat actors are and provide the attack kill chain and root cause.

Incident Triage

AI will minimize false positives by augmenting rules-based detection systems.

Always Hunting

AI never sleeps, keeps learning & enhancing detection accuracy, and as a result will be able to continuously monitor & discover anomalous behaviors as they occur

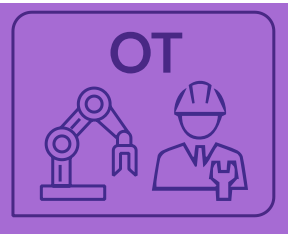
Threat Prediction

AI will pull threat intelligence from internal and external sources and provide predictive services for upcoming threats.

Incident Response

AI will apply case-based reasoning and create and/or run existing playbooks to perform an incident response either fully automated or with a human analyst monitoring it.

AI Cyber Security systems nowadays available for both IT & OT critical infrastructures



References

1. Department of Defense (2019), DoD Digital Modernization Strategy.
2. NSA - Operational Test and Evaluation (2021), FY 2020 Annual Report. Available at:
3. National Institute of Standards and Technology (2020), Special Publication 800-207: Zero Trust Architecture
4. Institute for Defense Analysis In-Use and Emerging Disruptive Technology Trends.
5. NIST Special Publication 800-207 - Zero Trust Architecture

Shukran!

شُكراً