“Assume Breach”

A Network Security Engineer Perspective

Rabih Itani
Cybernetics Partners
May 2024

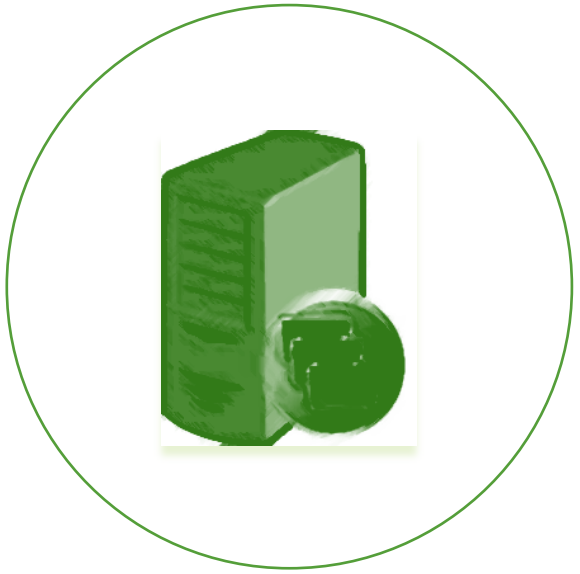
Cybernetics Partners

Network Security Pre-Digital Transformation

Clear and Clean-cut Segmentation

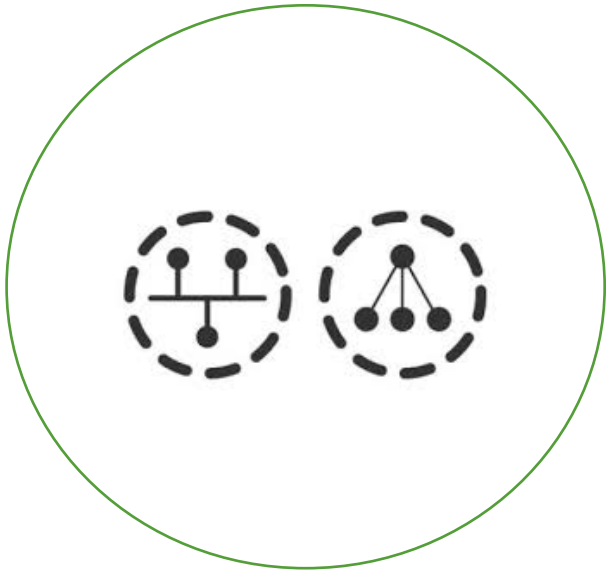
Perimeter Firewalls

Simple Zoning: Trust-Untrust-DMZ



Simple Application Patterns

Monolithic or Layered (typically 3) App. Architecture



VLAN based Segmentation

Inter-VLAN static Layer 3 or 4 based Policies

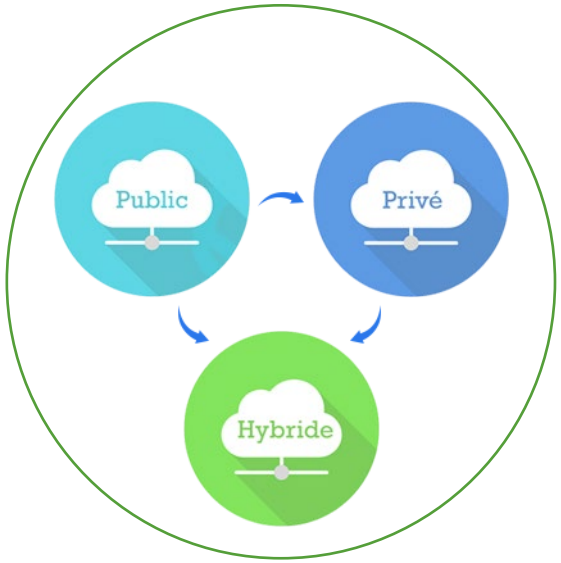
Cybernetics Partners

Network Security Today

Where, How, and When to Segment?

The Perimeter Vanished.

Trust is lost



The World is Hybrid.

Crown Jewels Everywhere

Microservices & APIs Exploded.

Open Communication

Cybernetics Partners

Protection against persistent attackers is

Not Enough

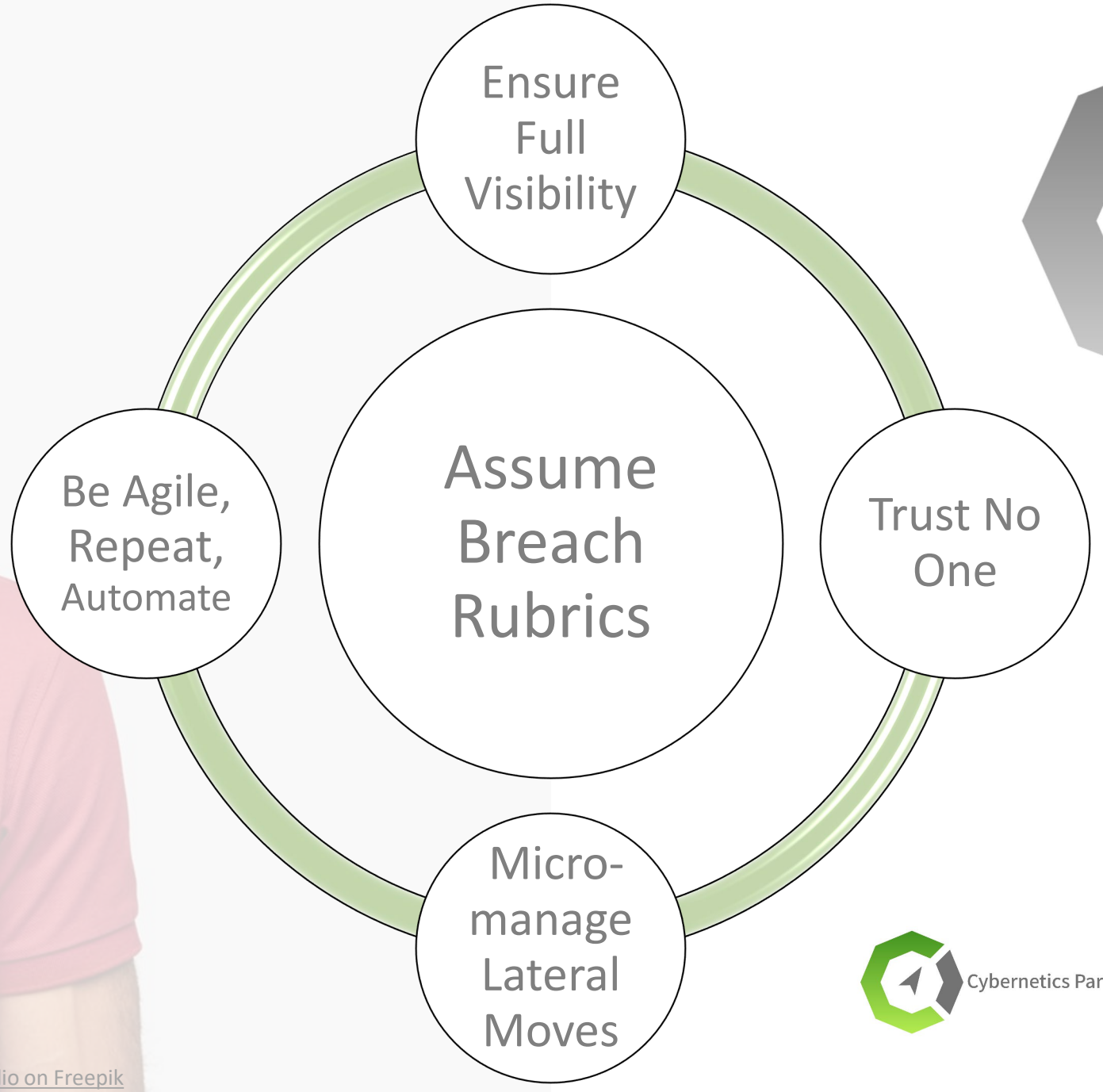
Detection of sophisticated attacks is

Tough

Assume Breach Mindset

Cybernetics Partners

Image by wayhomestudio on Freepik



Cybernetics Partners

Apply Full Visibility

Cover of all attack surfaces and environments

(Bare metal, Virtual, Containers, IoT, OT)

Tap all traffic directions

East-West (lateral) is a Must

Discover all Workloads, Repeat (Forever)

Context Based Identification and Flow Mapping

Cybernetics Partners

Trust No One

Image by DC Studio on Freepik

Isolate, Segment

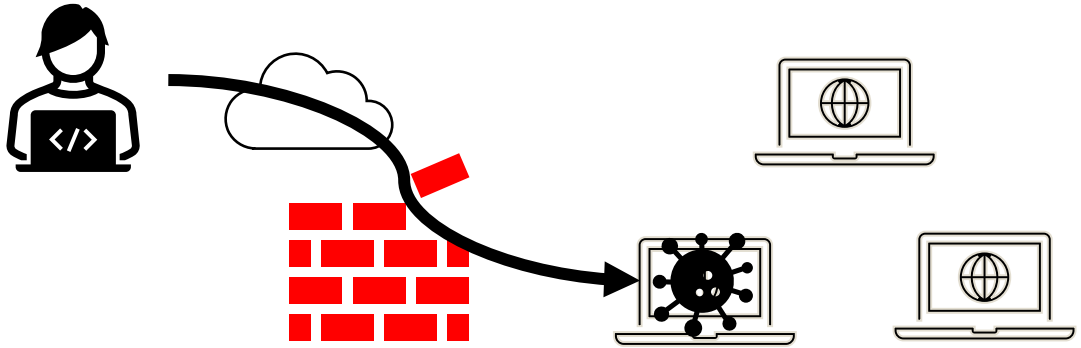
Default to an implicit Deny

Practice Zero tolerance for IP address or TCP/UDP based access only policies.

Demand Identity and more Context to enforce fine-grained policies at Workload and Application level

Cybernetics Partners

Micromanage Lateral Moves



Attackers already inside

Perimeter protection already bypassed

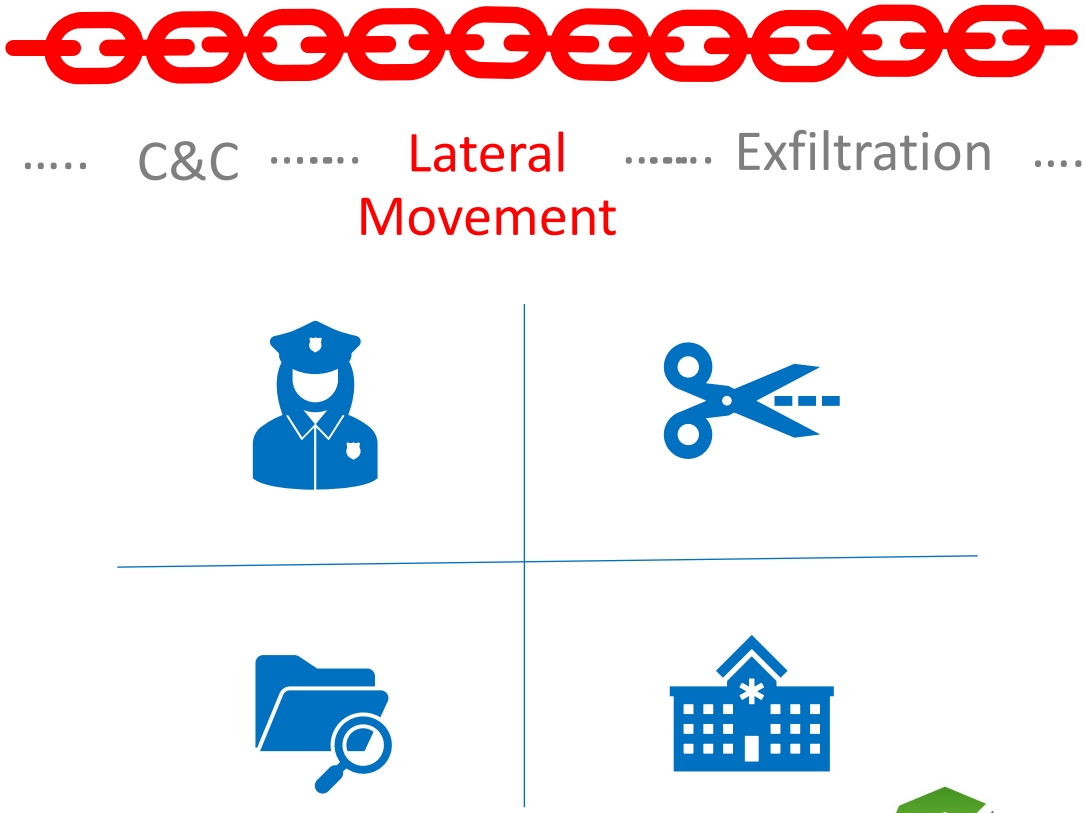
Now attackers moves are mainly lateral trying to reach the crown jewels

Cybernetics Partners

Micromanage Lateral Moves

Isolate and Microsegment with the objective to:

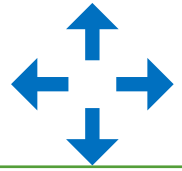
- Break the kill chain or at least slow down attackers
- Contain the Breach
- Enable more focused investigation
- Allow for Faster Remediation



Cybernetics Partners

Be Agile, Repeat, Automate

Practice Agility



Adapt the continuous change of today's DevOps environment

Repeat Processes (forever)

Continuous Discovery, Deployment, Policy Identification & Enforcement

Automate to Enable Scale

Automate discovery, policy recommendation, and possibly policy enforcement

Cybernetics Partners

Available Technology

Zero Trust Micro Segmentation (ZTMS)

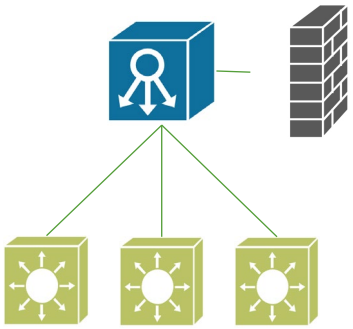
Cybernetics Partners

What to Look for in a ZTMS Solution?

Coverage of all attack surfaces and environments	 Tapping on all traffic directions	 Continuous Workload Discovery and Flow Mapping
 Recommendation and Enforcement of Fine-grained Context based policies	 Automation to Scale all Continuous Processes	 Integration with Ecosystem (Cloud, Identity, Firewalls, SIEM, Threat Feeds)

Cybernetics Partners

What are ZTMS Deployment Options?



Network Overlay

(taps onto Network controls)

Agent Based

Cloud Native (Provided by AWS, Azure, Google…)

API Based with Cloud Providers

Cybernetics Partners

Recommendations

Adopt Zero Trust Micro Segmentation as integral part of your Zero Trust Strategy and Architecture

Micro segmentation is not a hype or a panic response but an evolved long-awaited architecture

Identify Your Organization Use Cases

Flow mapping, Isolation, or Breach containment

Select the Best Fit Solution

Tightly integrates with your enterprise architecture & workload environment and provides the granular identification & policy control needed

Cybernetics Partners

Final Recommendations

Two words:

“Assume Breach”