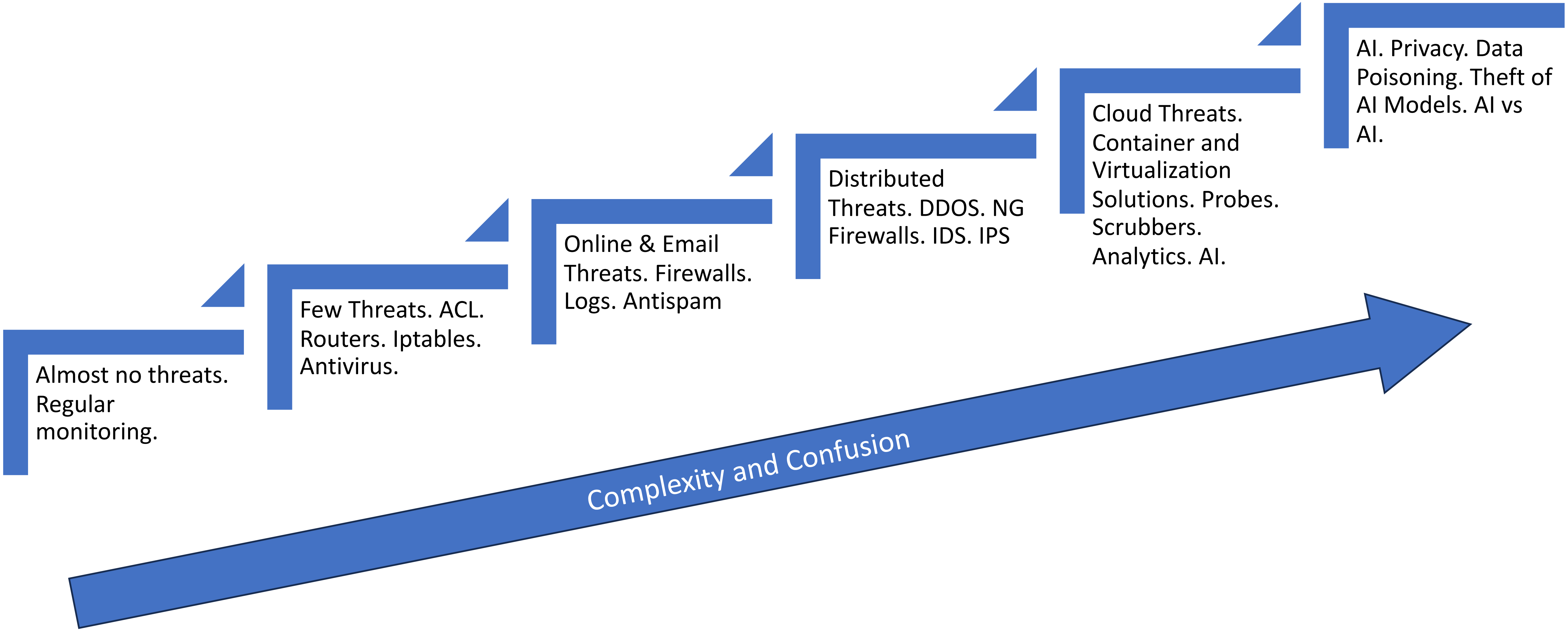
The Security Conundrum

The Ever-increasing Confusion for Network Operators

From WEF

Fundamentally, complexity in cybersecurity means a lack of visibility. The sheer number of components and point products in many modern networks makes identifying vulnerabilities, let alone remediating them, challenging.

Complexity is the attackers' friend. It creates vulnerabilities for them to exploit and simultaneously obscures defenders from confronting the problem before it's too late.



Almost no threats. Regular monitoring.

Few Threats. ACL. Routers. Iptables. Antivirus.

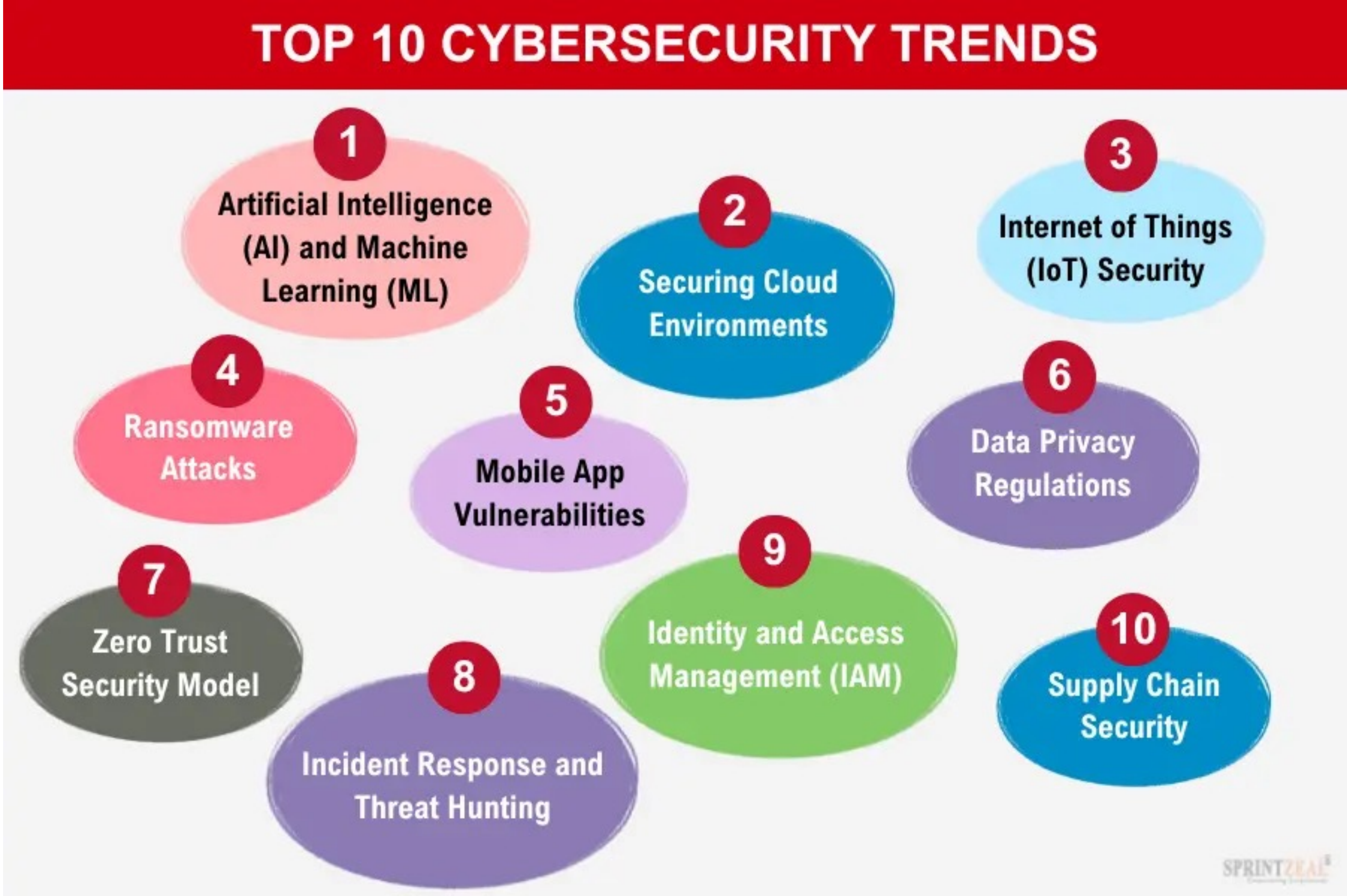
Online & Email Threats. Firewalls. Logs. Antispam

Distributed Threats. DDOS. NG Firewalls. IDS. IPS

Cloud Threats. Container and Virtualization Solutions. Probes. Scrubbers. Analytics. AI.

AI. Privacy. Data Poisoning. Theft of AI Models. AI vs AI.

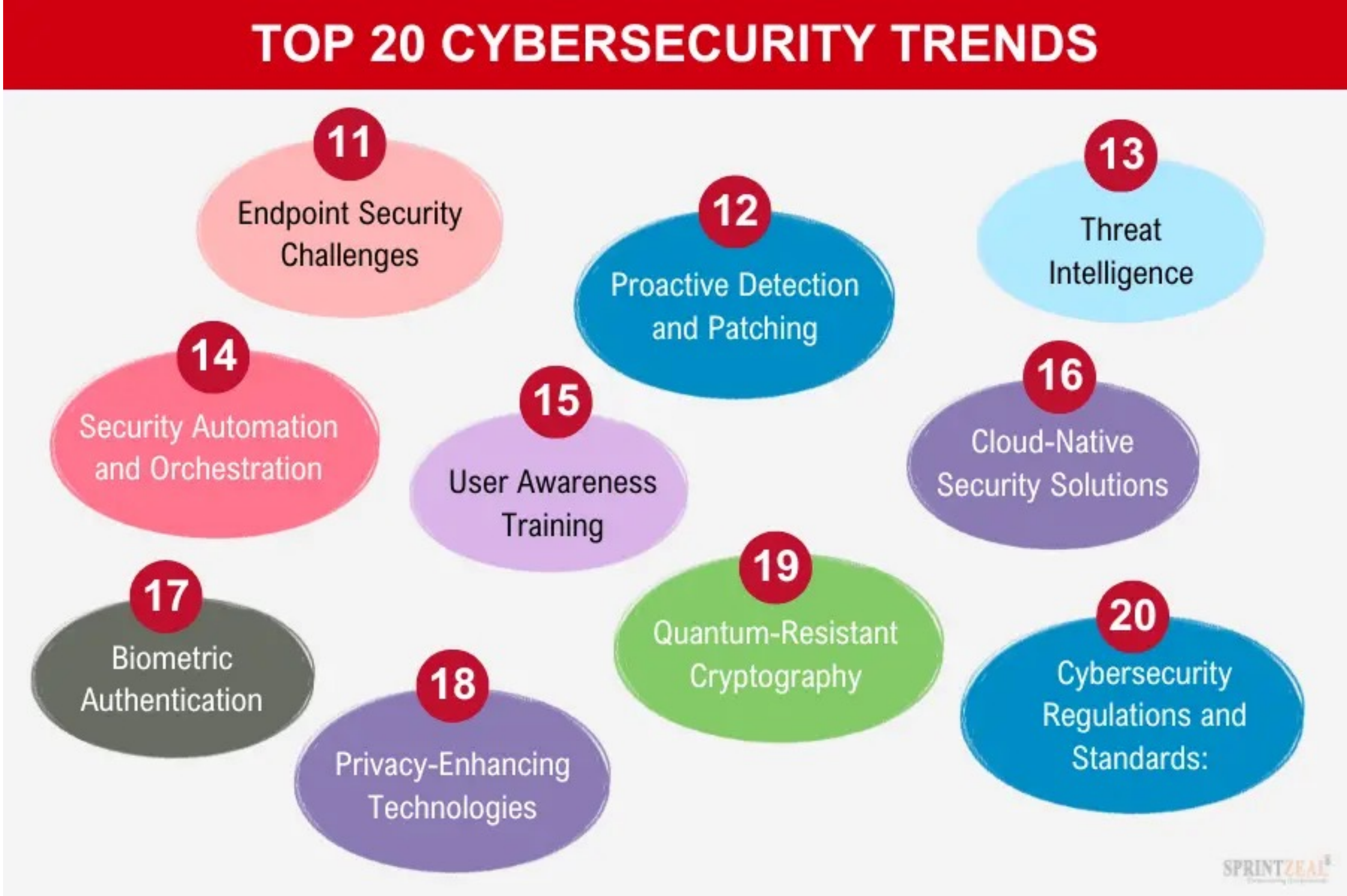
Sprintzeal.com



TOP 10 CYBERSECURITY TRENDS

1. Artificial Intelligence (AI) and Machine Learning (ML)
2. Securing Cloud Environments
3. Internet of Things (IoT) Security
4. Ransomware Attacks
5. Mobile App Vulnerabilities
6. Data Privacy Regulations
7. Zero Trust Security Model
8. Incident Response and Threat Hunting
9. Identity and Access Management (IAM)
10. Supply Chain Security

sprintzeal.com



TOP 20 CYBERSECURITY TRENDS

11 Endpoint Security Challenges

12 Proactive Detection and Patching

13 Threat Intelligence

14 Security Automation and Orchestration

15 User Awareness Training

16 Cloud-Native Security Solutions

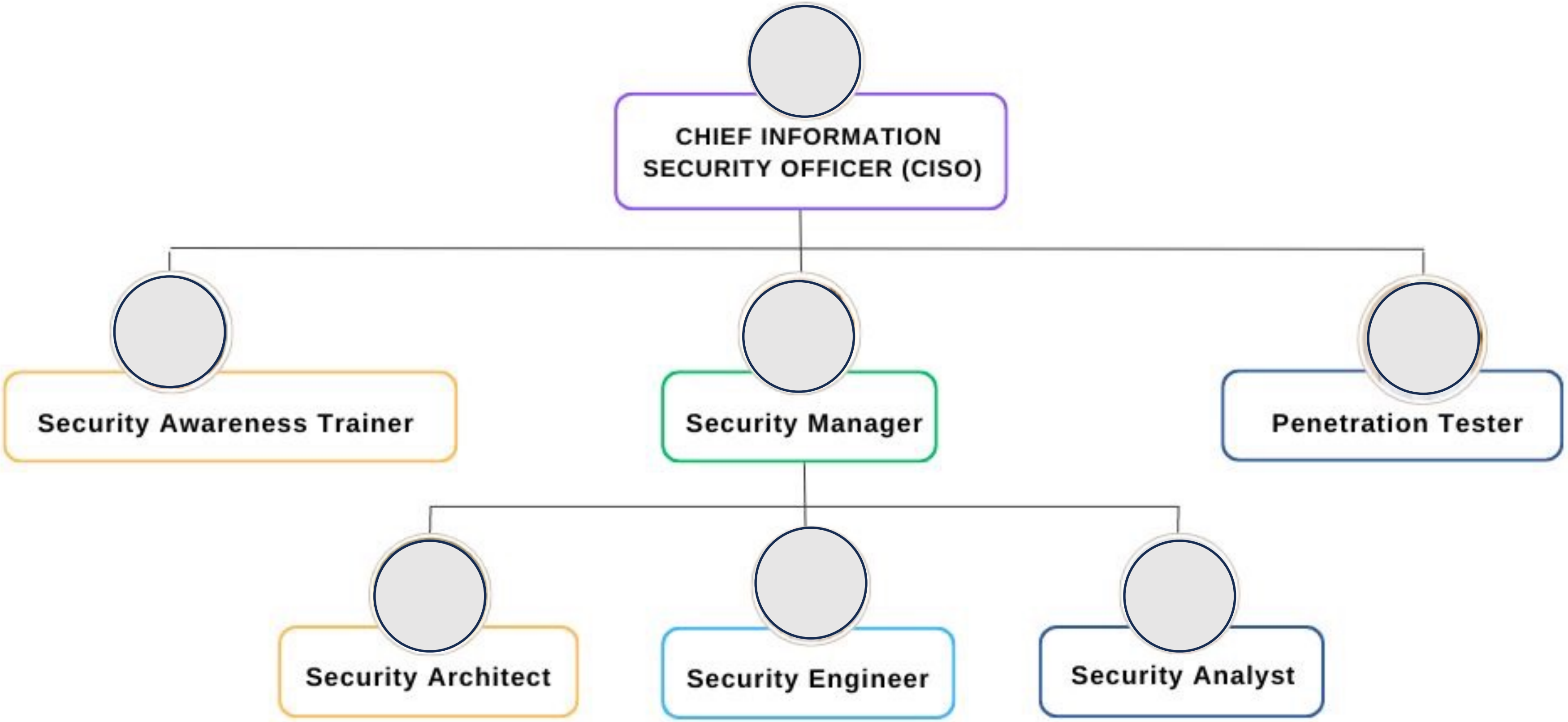
17 Biometric Authentication

18 Privacy-Enhancing Technologies

19 Quantum-Resistant Cryptography

20 Cybersecurity Regulations and Standards:

CYBER SECURITY TEAM ORGANIZATION CHART



CHIEF INFORMATION SECURITY OFFICER (CISO)

Security Awareness Trainer

Security Manager

Penetration Tester

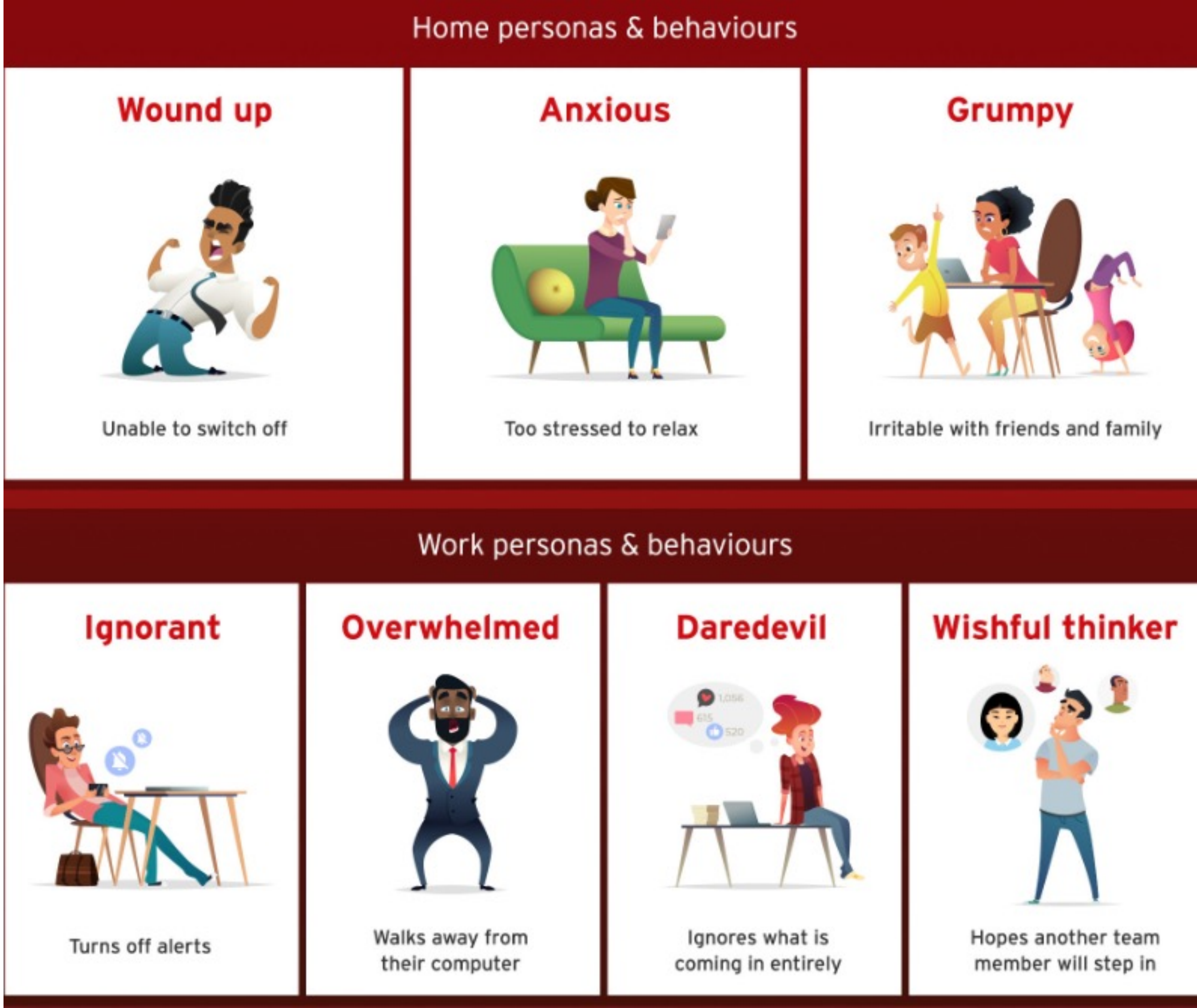
Security Architect

Security Engineer

Security Analyst

SoC Personas

(ref.: trend micro)



Home personas & behaviours

Wound up

Unable to switch off

Anxious

Too stressed to relax

Grumpy

Irritable with friends and family

Work personas & behaviours

Ignorant

Turns off alerts

Overwhelmed

Walks away from their computer

Daredevil

Ignores what is coming in entirely

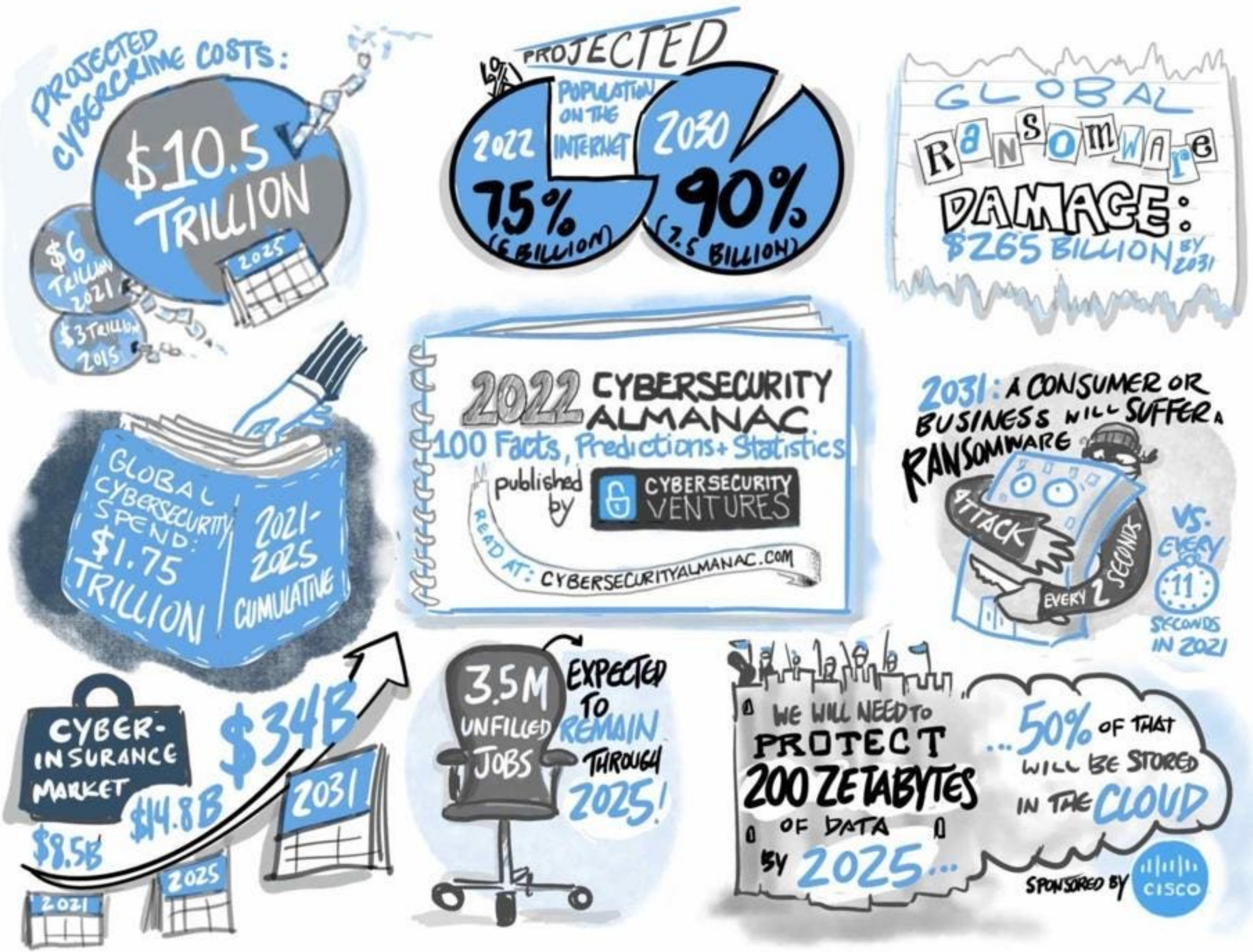
Wishful thinker

Hopes another team member will step in

It’s about money.

A lot of it.

(ref.: forbes.com)

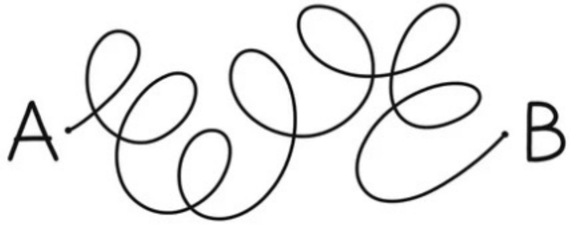

PROJECTED CYBERCRIME COSTS:
$10.5 TRILLION
2025
$6 TRILLION 2021
$3 TRILLION 2015
PROJECTED
POPULATION ON THE INTERNET
2022
75%
(5 BILLION)
2030
90%
(7.5 BILLION)
GLOBAL
RANSOMWARE
DAMAGE:
$265 BILLION BY 2031
GLOBAL CYBERSECURITY SPEND: $1.75 TRILLION
2021-2025 CUMULATIVE
2022 CYBERSECURITY ALMANAC
100 Facts, Predictions + Statistics
published by
CYBERSECURITY VENTURES
READ AT: CYBERSECURITYALMANAC.COM
2031: A CONSUMER OR BUSINESS WILL SUFFER A RANSOMWARE
ATTACK
EVERY 2 SECONDS
VS. EVERY 11 SECONDS IN 2021
CYBER-INSURANCE MARKET
$8.5B
2021
$14.8B
2025
$34B
2031
3.5M UNFILLED JOBS
EXPECTED TO REMAIN THROUGH 2025!
WE WILL NEED TO PROTECT 200 ZETABYTES OF DATA BY 2025...
...50% OF THAT WILL BE STORED IN THE CLOUD
SPONSORED BY CISCO

Those Days

- ACLs
- Iptables
- Initial firewalls
- Simple antivirus
- Limited antispam
- RBAC
- Scripts
- A lot of monitoring and logs

Now - Too Many Variations

- End point security and app security
- Cloud security
- Single sign-on & Privilege access management
- Network access control & Intrusion detection
- DDoS
- BYOD
- IoT related threats
- Social media security and protection of minors
- Online gaming security …



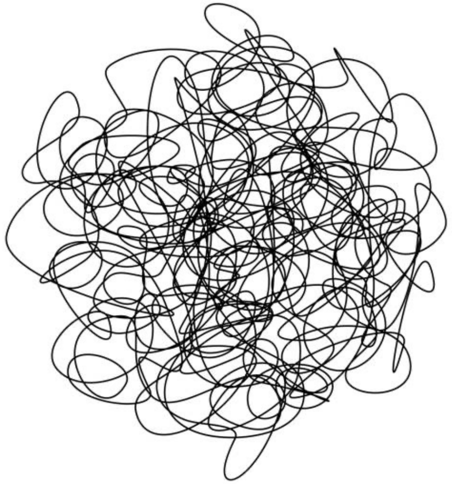
Too Many Areas

- Infrastructure
  - Cloud
  - Network
  - Application
  - API
  - Data loss prevention
  - Access management
  - IoT
- Logging / Audit / Response
  - SIEM, SOAR, VA-PT, IS Audit …

- End Point
  - Antivirus
  - Protection from malware
  - Social media
  - Identity theft

Configuration Drifts
Misconfigurations
Evolving Attacks

Cloud Induced Complexities



- Intangible assets
- Undefined and unclear perimeter
- High abstraction and hard to define the threat boundaries
- Continuous Integration and Continuous Deployment (CI/CD) challenges
- Security specific to services and containers
- Unclear regulations and operations across jurisdictions

IoT

- Too many devices
- Encrypt data
- Small devices
- Vulnerability to the very edge
- Over-dependence on cloud and central processing
- Need to maintain end-user affordability while ensuring security

Securing IOT

- Devices
- Privacy
- Connectivity
- Hubs
- Information flow
- Data store
- Apps and data presentation

Everything As a Service

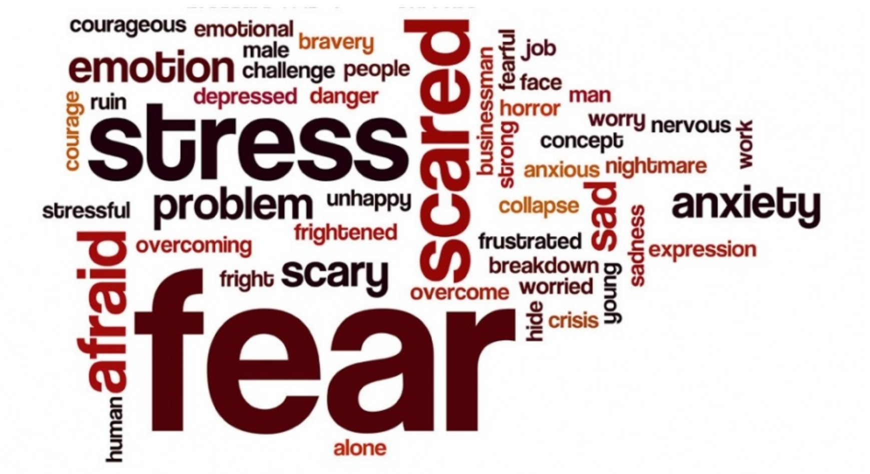
- Software and cloud driven
- Based on licenses
- Recurring subscriptions – rate hikes, every small thing costing a bit more
- Almost no control in the hands of the local team
- Over-exposure
- Provider-locking

Baseline Practices (CISA, IC3…)

- Implement a centralized management solution
- Implement network segmentation
- Implement Security Orchestration, Automation, and Response (SOAR)
- Develop, maintain, update, and regularly drill IT and OT cybersecurity incident response plans
- Automate and validate vulnerability scans on all public-facing enterprise assets.
- Use well-tested, high-performing cybersecurity solutions
- Integrate an incident detection system
- Have annual trainings on basic security concepts
- Implement a strong identity and access management solution

Industry of Fear

- Nobody wants to live in fear
- Will have to do something to alleviate
- One cause patched, another props up
- Fear is amplified by external advices
- Fear creates market
    - Leads to new products, careers, fields of expertise
- Leads to talks like this



FOMO

- Am I doing enough?
- Are my equipment and systems properly safeguarded?
- Are our clients safe?
- Is our service credibility affected due to security?
- Can there by a threat from my network to others?
- Is my company considered backward or not serious?

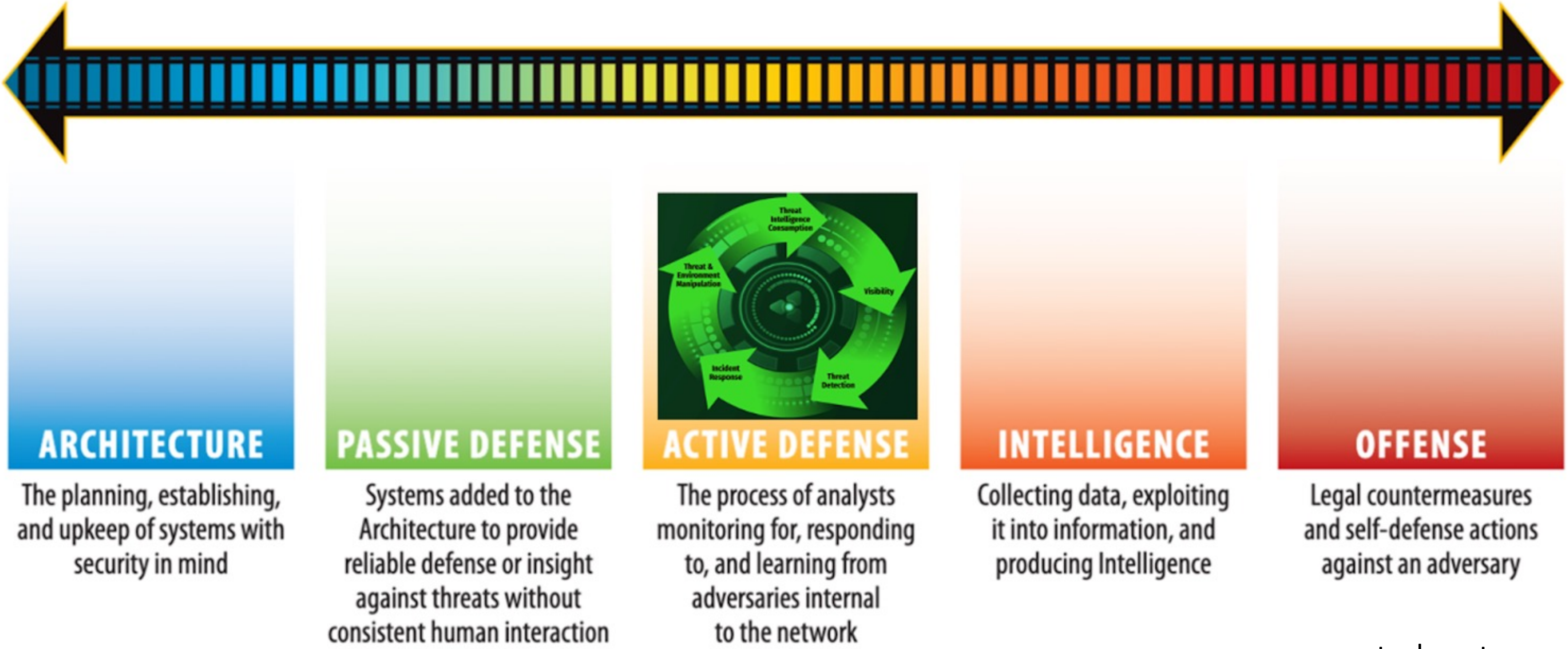
Whom to Look Up To

- Experts
- Consultants
- Bounty Hunters
- Ethical Hackers
- Auditors
- Security Architects
- Forensic Investigator
- Vulnerability Assessor

- Penetration Tester
- Incident Manager

Certifications
Qualifications
Accreditations

Trying to Resolve the Conundrum?


Threat Intelligence Consumption
Visibility
Threat Detection
Incident Response
Threat & Environment Manipulation

ARCHITECTURE

The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE

Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE

The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

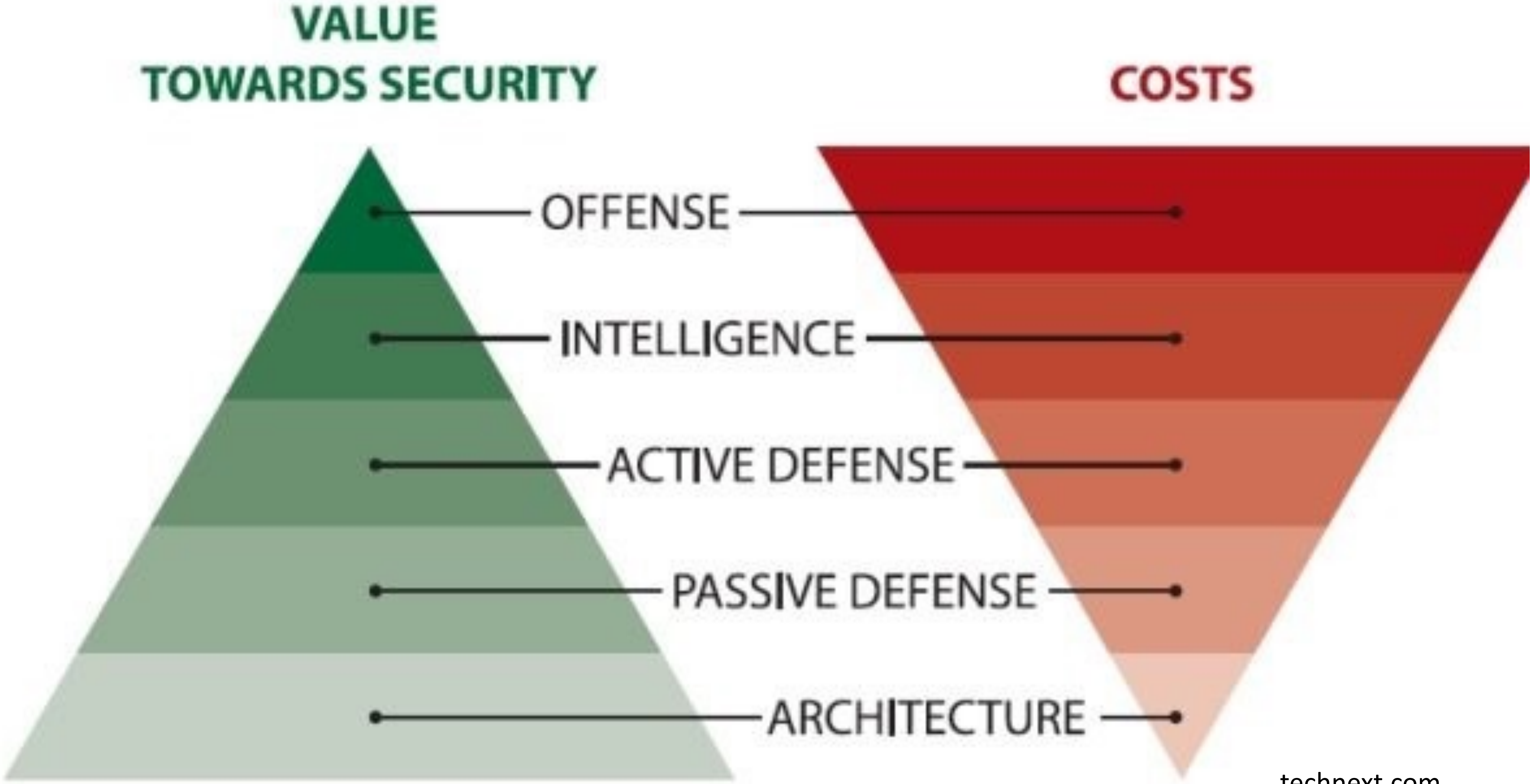
INTELLIGENCE

Collecting data, exploiting it into information, and producing Intelligence

OFFENSE

Legal countermeasures and self-defense actions against an adversary

technext.com



VALUE
TOWARDS SECURITY

COSTS

OFFENSE

INTELLIGENCE

ACTIVE DEFENSE

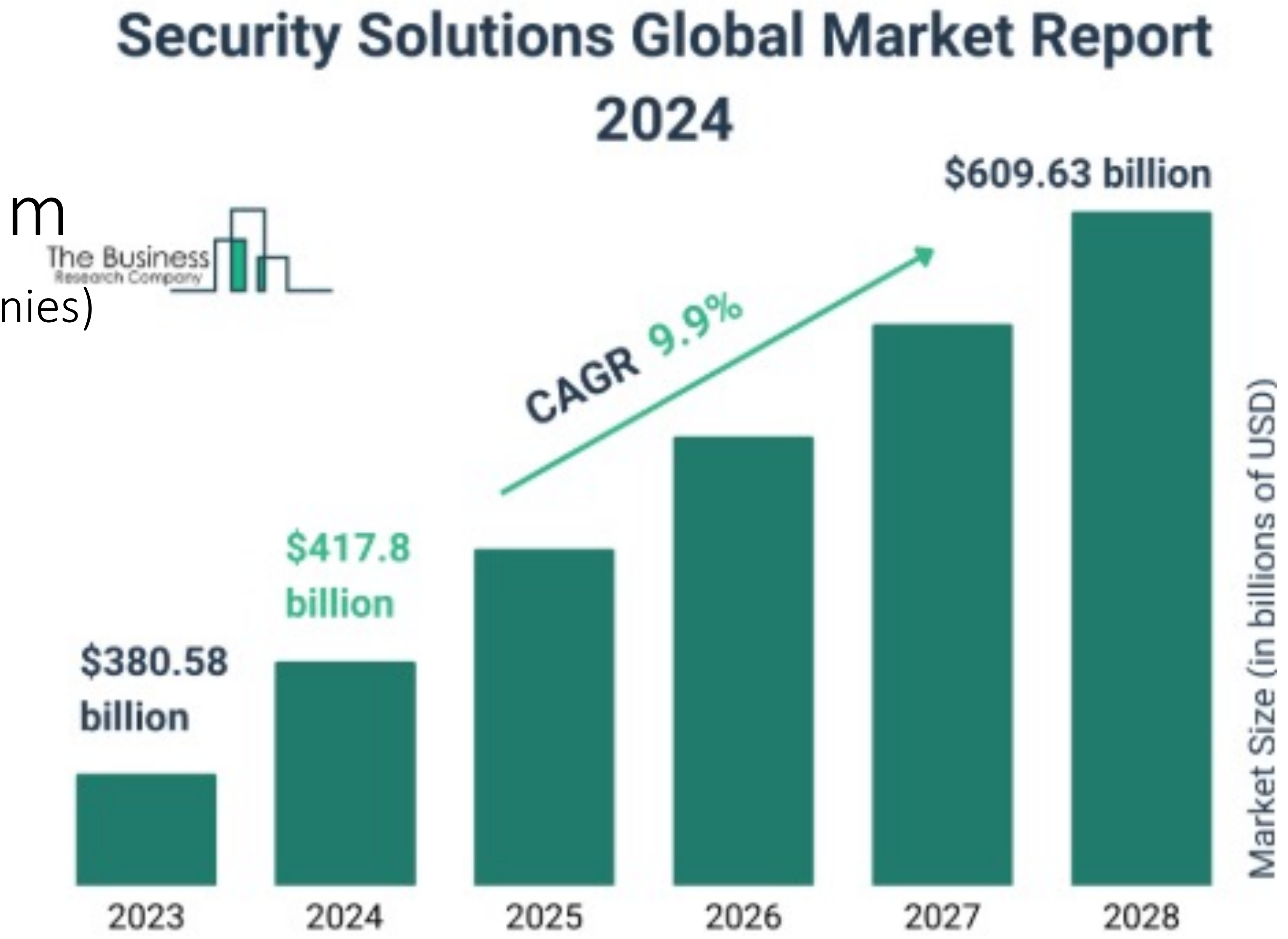
PASSIVE DEFENSE

ARCHITECTURE

technext.com

Lucrative Conundrum

(For the companies)



So… What Can We Actually Do?

- Design and Documentation
- Visibility
- Segmentation
- Technology + People + Updated Knowledge / Skill
- Sharing / Training / Best Practices (Pokhara 2024 :-))
- Laws, Standards, Regulations
- Consumer Education

Unity in Diversity

Not one solution fits all

Not everyone needs everything

Every operator is same (risks, challenges) and different (strategies, tools, people, practices) at the same time.

Days when a couple of guys staring at a black screen sufficing for a network infrastructure security are gone.

Today, a list solutions for security will overflow that black screen.

Entropy Keeps Increasing

However hard you try to solve complexities and come up with solutions, the complexity and problems will keep rising. If not anything else, the solution itself will create new problems.

That’s Exactly Why We Do What We Do

And Probably That’s Why We Are Here

The Cybersecurity Framework (NIST)

- **Govern**: The organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify**: The organization’s current cybersecurity risks are understood.
- **Protect**: Safeguards to manage the organization’s cybersecurity risks are used.
- **Detect**: Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond**: Actions regarding a detected cybersecurity incident are taken.
- **Recover**: Assets and operations affected by a cybersecurity incident are restored.

Ultimate Aim to Protect

- Infrastructure
- Computing hardware and software
- Services and their availability
- Customer data
- Classified business information and data
- No use of organization for threat to others
- Credibility and trustworthiness of organization
- Protection of business interests and RoI

Multiple Choices Cause Confusion but They Also Offer Choice

Thank You !!!