trusted
PARTNERS

Trusted Partners

Company Profile

Trusted Partners follows a unique approach to combine innovative solutions and delivery excellence where both consider the client's benefits

Saudi cybersecurity consulting company

Unique approaches and innovative cybersecurity ideas delivered to client

1st company to innovate specialized cyber capability building programs

- **Trusted Partners has engaged in national strategic discussions** and initiatives that lasted for more than nine months to shape the future in KSA regarding cybersecurity with the National Digitization Unit and MCIT
- **Trusted Partners has successfully designed, executed, and delivered many** capability building programs for several large clients
- **Trusted Partners has delivered cybersecurity consultation projects for many clients** and successfully helped them boosting their businesses

MAJOR CLIENTS

TEAM EXPERIENCE

Trusted Partners provides all inclusive services related to cyber security domains

Trusted Partners is a Saudi consulting company with excellent experience in Cybersecurity Consultation and Cybersecurity Capability Building

Trusted Dimensions

Major Business Lines

Cybersecurity Advisory

- ✓CS Strategy & Transformation
- ✓Cyber culture & Change management
- ✓Digital Identity
- ✓Incident & Threat Management
- ✓Governance, risk, and compliance

Cybersecurity Capability Building

- ✓Cybersecurity job and industrial fit training (technical, soft skills, leadership, OJT, etc..)
- ✓Innovative Train-Like-You-Fight concepts for training
- ✓Bleeding-edge partners working with leading global government & commercial organization
- ✓Cybersecurity awareness programs

Cybersecurity Assurance

- ✓Infrastructure assessment
- ✓Web application assessment
- ✓Red teaming engagement
- ✓Threat modeling

trusted
PARTNERS

Cybersecurity Advisory

Trusted Partners Cyber practice

Trusted Partner’s Cyber Security and Privacy practice

Increasing cyber risks have made an effective cyber security program a critical business requirement. Trusted Partner’s Cyber Security and Privacy practice can provide a variety of capabilities to help you manage these risks – helping to protect your data, your brand, and your business.

Strategy and Transformation

Develop business-focused strategies that support growth by making security and privacy an enterprise-wide priority.

Digital Identity

Receive the support needed to manage, support, and enhance cyber digital trust .

Privacy and Consumer Protection

Understand data lifecycles to protect data, help meet the privacy expectations of consumers, and applicable privacy regulations.

Incident & Threat Management

Confidently prepare, identify, respond, investigate and remediate threats.

Trusted Partners Cyber practice

Strategy and Transformation

Many organizations are pursuing emerging technologies to develop new products, services, or ways of doing business. However, companies don't always consider the emerging cyber security threats that could impact these systems after they are implemented.

Trusted Partner's Strategy and Transformation capability provides our client's services to help them assess, manage, plan, and transform their cyber security program and services.

Key services

Assess the Fundamentals

Performing an assessment aligned to your organization's needs, Trusted Partners can review how your organization handles cyber security risks and its relative maturity.

Transform the Program

Working with stakeholders throughout your organization, Trusted Partners can work to shift a cyber security program into one focused on proactively managing risk.

Enable Compliance

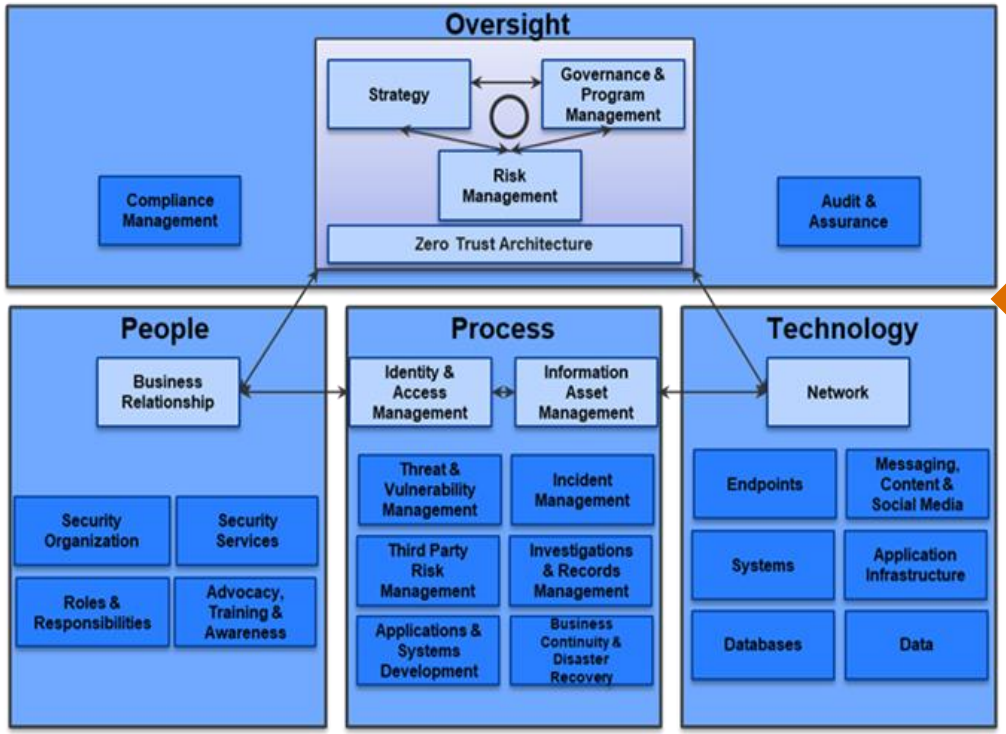
Trusted Partners can work to help your organization comply with applicable regulations, as well as providing accelerators and templates to assist your organization in maintaining a compliant cyber security program into the future.

Ongoing Program Operation and Monitoring

Trusted Partners can identify methods of operating and maintaining a program into the future, by aligning findings with risks and threats, creating key performance indicators and reporting, and creating metrics for measuring progress for program enhancement.

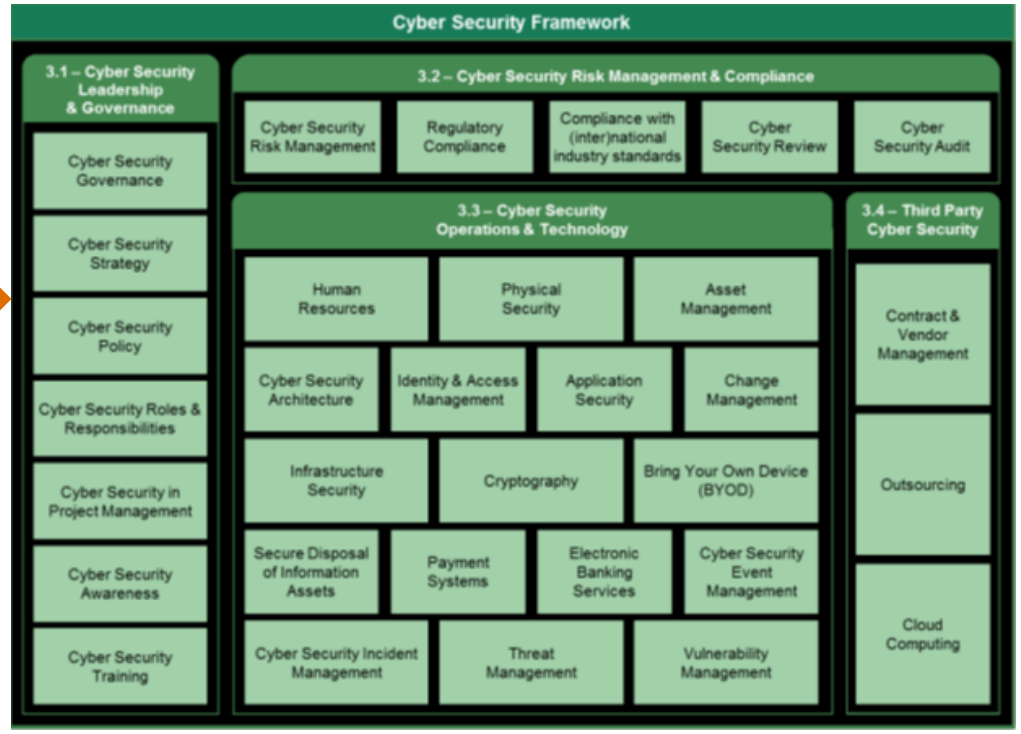
ISMM/SAMA domain/function comparison

Forrester ISMM



MAPPING

SAMA Cyber Security Framework

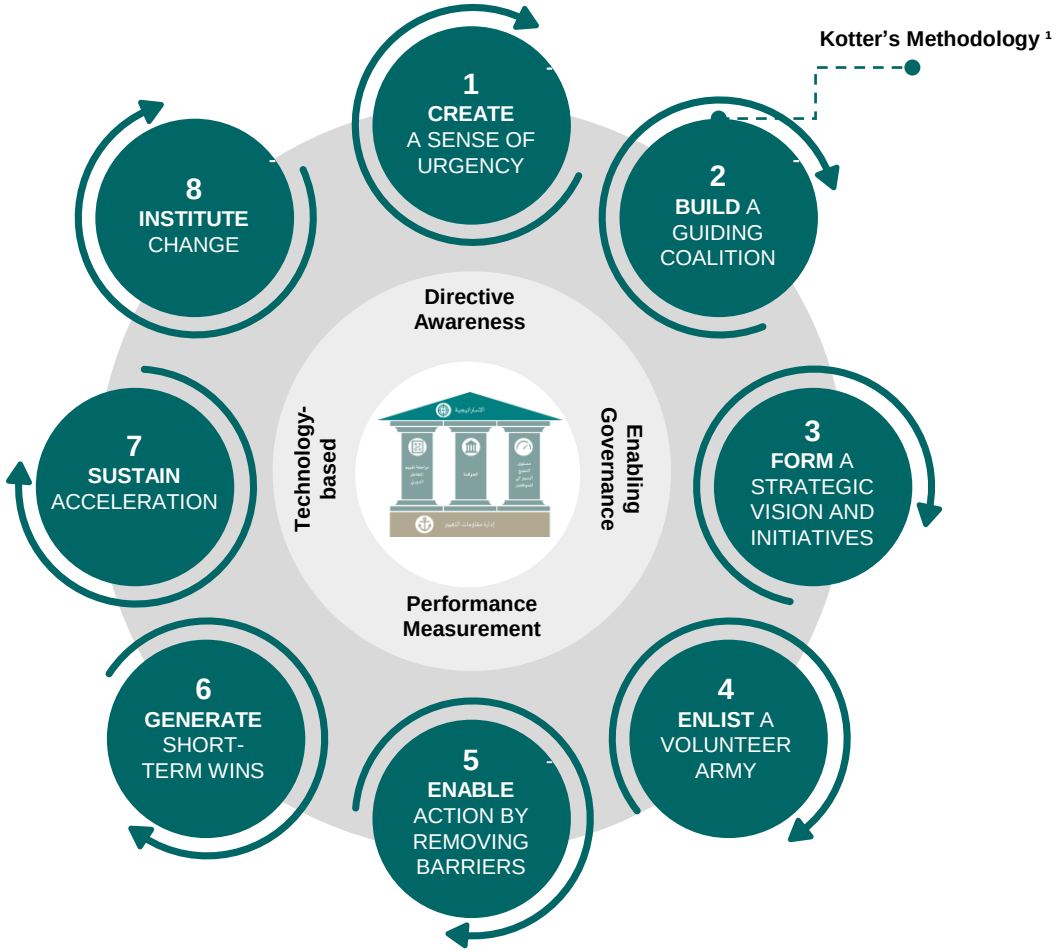


We help build and enhance organizational cybersecurity culture through our comprehensive change management program and boost awareness levels

Organizational Cybersecurity Culture

- ✓ One of the biggest challenges in incorporating awareness programs to raise the cybersecurity is being situational and temporary. Our approach is tackling the very essence of the problem which is the lack of cybersecurity culture in the organization and build it thoroughly
- ✓ Build the change management program based on the “As-is” assessment results, all accompanied by directive awareness campaign to initiate the change on all levels
- ✓ The program will utilize the technologies used in the organization to enable the aligned program governance goals and to measure performances on all levels throughout the program
- ✓ The results should be an overall aware and active staff that will help minimize the cybersecurity damages and financial losses of the organization

Change Management Framework



[1] Source: (Kotter’s 8 Steps)

Trusted Partners Cyber practice

Privacy and Consumer Protection

At Trusted Partners we help organizations build trust with consumers, regulators, and other stakeholders in their use of personal information. We can help you evaluate how privacy impacts your business, and institute a thorough rule book informed by insights from our global privacy framework. We can help you craft privacy strategies to confidently support your business growth and advance your business forward.

At Trusted Partners, we believe in consumer protection and privacy by design. Our team— which includes former chief privacy officers and implementation specialists with firsthand experience working directly with regulators—uses proprietary technology and has the diverse perspectives and experience required to help our clients stay ahead of change.

Key services

Risk Analysis and Data Discovery
Trusted Partners can perform information gathering activities to provide an understanding of your data risk and data footprint, including data types, scale, and jurisdictions

Gap Assessment and Remediation Roadmap
Utilizing Trusted Partner's Global Privacy Framework, Trusted Partners can identify your current privacy capabilities and prioritize required program remediation activities

Cross-Functional Oversight and Planning
Trusted Partners can help with defining and establishing the ongoing governance structure to coordinate, operate and, implement remediation activities

Program Implementation
Trusted Partners can assist with implementation of a privacy program in order to remediate known compliance gaps and establish a privacy program, covering key areas such as: strategy and governance; policy management; cross-border data strategy; data lifecycle management; individual rights processing; privacy by design; information security; privacy incident management; data processor accountability; and training and awareness

Ongoing Program Operation and Monitoring
Trusted Partners can assist with establishing ongoing compliance mechanisms to promote continued accountability

Trusted Partners Cyber practice

Digital Identity Services

Trusted Partner's Confidence in your systems: You need an integrated and holistic approach to designing, deploying, operating and optimising your control environment. As the business system landscape changes with users moving seamlessly between in-house systems and cloud based web services and mobile applications, a comprehensive approach to business systems control becomes even more important. With digital opportunities and risks becoming so central to business strategy, boards and audit committees must have the digital expertise to set the level of risk that they are willing to accept. They must be able to ask the right questions and hold management to account.

Key services

Privileged Access Management
Trusted Partners can help maintain and enhance technology and processes related to securing user, system and application accounts with the highest level of access.

Data Loss Prevention
Trusted Partners can help maintain and enhance technology monitoring the movement, usage, and storage of the most sensitive data within an environment.

Identity & Access Management
Trusted Partners can work to help maintain the stability as well as the maturity of an organization's investment in securing access, entitlements, and authentication to resources

Security Monitoring, Reporting and Analytics
Trusted Partners can either work alongside your Security Operations Center (SOC) or run your SOC for you, helping to monitor threats and respond, notify, and remediate cyber security incidents.

Secure Software Development Lifecycle (SDLC)
Trusted Partners utilizes established frameworks to help build secure applications from their inception to their decommission.

Trusted Partners Cyber practice

Incident and Threat Management

Trusted Partner's team helps organizations understand dynamic cyber challenges, adapt and respond to risks inherent to their business ecosystem, and prioritize and protect the most valuable assets fundamental to their business strategy. Trusted Partners can help your organization prepare for a cyber security incident by providing response policies, procedures, and playbooks, performing tabletop exercises, and using proprietary tools – including Incident Response, Readiness and Resilience (IR3) Assessment, and Game of Threats - to help build, evaluate, and test your technical incident response capabilities.

Key services

Threat Detection and Response

Trusted Partners provides support for SOC services providing professional cyber security resources to enhance SOC operations, conduct targeted threat hunt activities, analysis, and advice in the event of a breach.

Threat Intelligence & Information Sharing

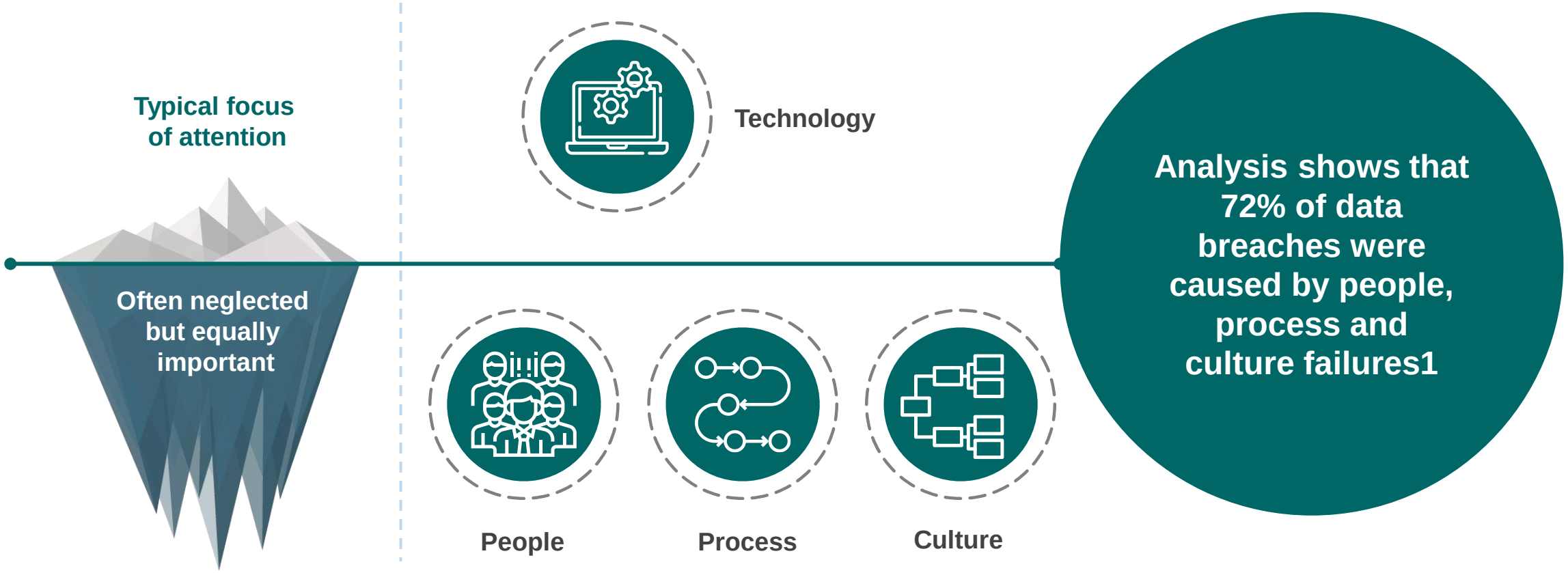
Utilizing real-time threat information, TP identifies relevant information on the threats that are affecting a client's environment.

Incident Readiness and Incident Management

Trusted Partners can help your organization prepare for a crisis — including a cyber security incident —by providing response policies, procedures, and playbooks, performing tabletop exercises, and using Game of Threats to help build and test your incident readiness.

Threat Intelligence , in details?

However, technology alone is not an adequate response



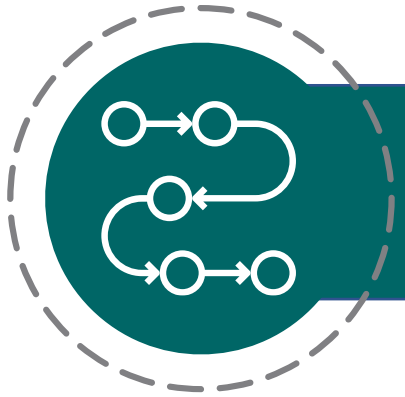
Businesses are now investing in steps to address these issues

People

Example: National Australia Bank

- National Australia Bank runs live cyber-simulation testing, monitoring employee reactions
- By 2020, they aim for all product development staff to be proficient in IT security, embedding CS in their product development end-to-end.

- Creative awareness campaigns that inform non-technical staff of the importance of CS
- Well-designed, bespoke CS trainings for IT and security staff that focus on their learning
- Carefully designed access rights, ensuring employees only have access to networks they truly need
- Cybersecurity capability building blending Jobs requirements, experience and hands-on through top notch training practices – **Secure18**

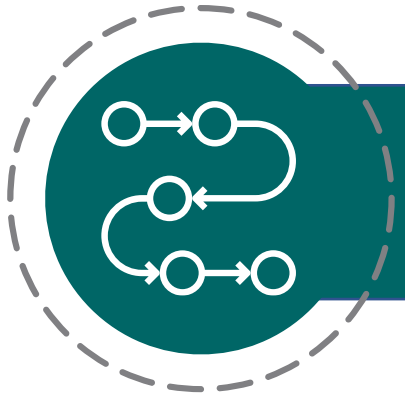


Process

Example: Tesla

- Tesla has baked CS vulnerability management processes into their vehicle design
- An example is its failure planning mechanism: if a Tesla vehicle's power is lost through a CS attack, it automatically goes into neutral, giving the driver control of the steering and brakes while the airbags remain fully functional

- Consolidating vendors to manage technology sprawl and streamline processes
- Ensuring patch management and vulnerability management processes that match risk appetite
- Implementing well-defined governance frameworks that allow for easy adaptation of CS strategy to evolving threat landscapes
- Effective, regular IT Audits organization-wide



Culture

Example: General Dynamics

- Top management built a CS-driven culture at GD through an ISRB[1]
- The ISRB oversees CS for all of GD and includes non-technical senior management Initially, the ISRB met once a month, seeking to embed CS into every part of the organization
- When the desired CS maturity was achieved, they only engaged in specific risk decisions

- Clear delineations of who is responsible for given aspects of CS
- Top management drives cultural change, with boards setting the agenda
- Business divisions and security collaborate and consider implications of new projects from their design phase
- Employees who are vigilant of security are recognized but those who admit to mistakes are not punished

CS Capabilities assessed using comprehensive CS framework covering all aspects of a world-class CS practice

Cybersecurity

Shape the practice

1 **Strategy**

Strategy | Business alignment | Operating model | Capabilities | Awareness and training | Investment and budget | Performance management

Enforce the strategy

2 **Governance**

- Governance framework
- Policies and standards
- Security architecture
- Physical and facilities management
- Resilience setup

3 **Risk**

- Risk framework
- Risk assessment
- Risk register
- Risk treatment plan
- Corrective and prevention actions

4 **Compliance**

- Compliance framework
- Third-party security
- Compliance program
- Procedures and checklist
- Legal and regulatory

Protect the business

5 **Cyber Defense**

Cyber Defense framework[1]	Endpoint protection	Identity and access management	Incident and forensic management
Infra and network protection	Pen. testing and vulnerability management	Threat intelligence and management	Information and asset management

Creating the right cybersecurity program to serve business objectives

Understanding business objectives lead to best results

Compliance-related objectives; waiving non-compliance cost and assure business alignment with industry standers and best practices

Operational objectives; maintaining operations continuity and minimize business interruptions

Learning and growth objectives; protecting organization's assets, intellectual property and customer data

Financial objectives; reducing financial loss resulting from data breaches and cyber attacks

trusted
PARTNERS

CYBERSECURITY CAPABILITY BUILDING

Cybersecurity Capability Building blends job requirements, experience and hands-on through top notch training practices

Our Added Value

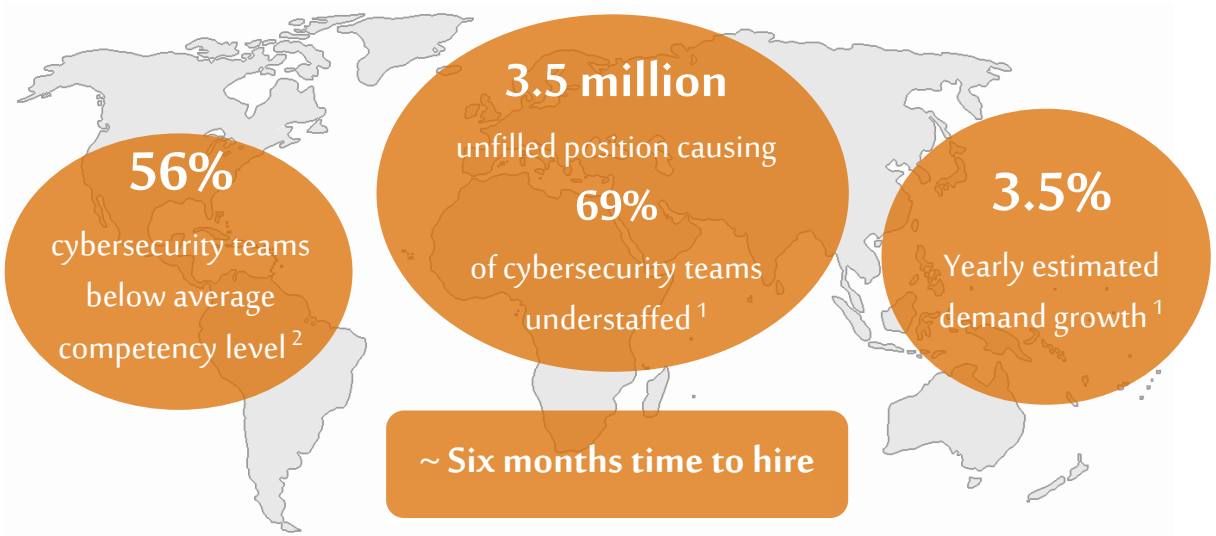
Short time-to-value	▸ Competent cybersecurity candidates with accelerated experience
Blended training	▸ Technical, soft skills, leadership and OJT delivered through unique practice
Top-notch training and certifications	▸ International and top-notch training providers delivering international and experience-based certifications
Work engagement	▸ Technical and job fit assessment ▸ Hands-on, on job training and blended experience practice
Pipeline of qualified resources	▸ Assurance of better talent acquisition and higher retention
Tailored to fit	▸ Cybersecurity workforce practice based on (NICE/SAMA/NCA) frameworks and industrial tailored training programs

Globally increasing talent gap and high turnover rate are the biggest two challenges for cybersecurity

Global Cybersecurity major challenges

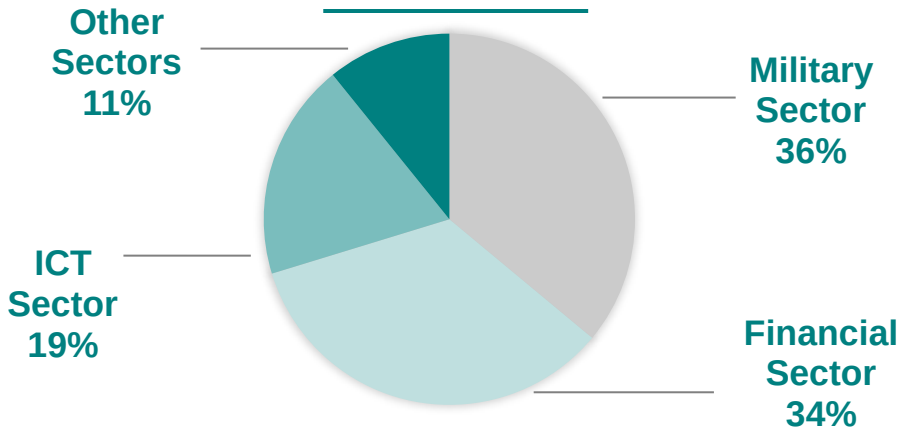
1 Increasing gap between Demand & Supply

Jobs Gap



2 High Turnover Rate

Turnover Rate [3]



1 ISACA report 2019
2 Information Systems Security Association (ISSA)
3 infosecurity-magazine

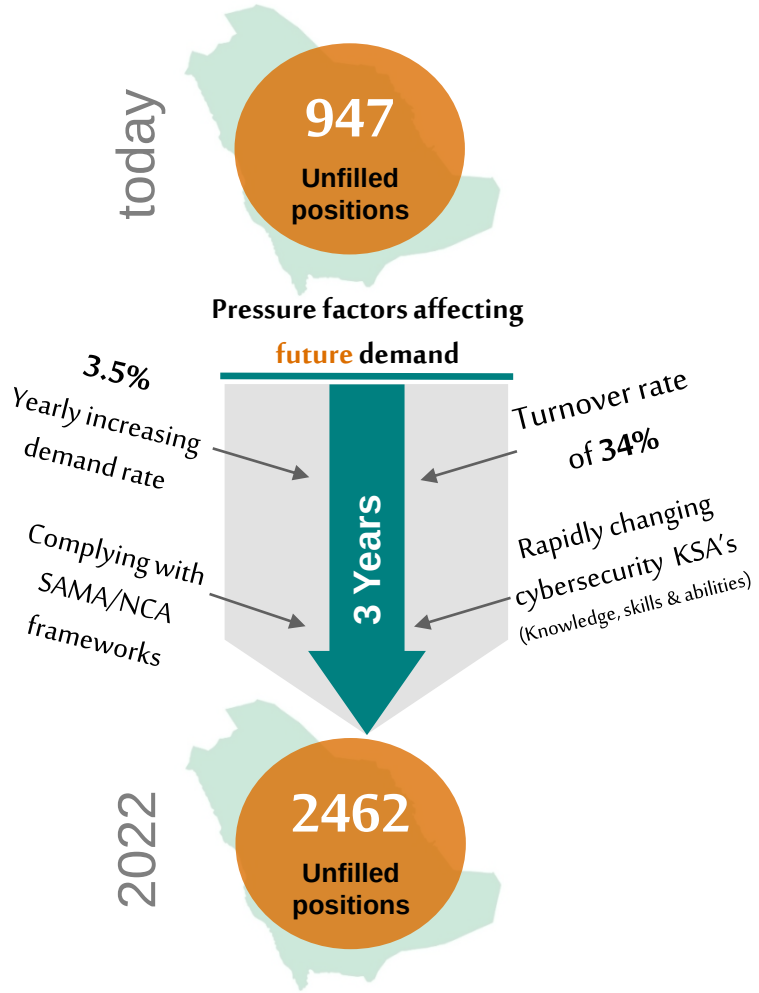
Rapidly increasing demand for cybersecurity professionals in KSA - especially in the financial sector

Cybersecurity professionals' gap for main domains in financial sector in KSA

	Number of entities *	Estimated demand **	Estimated supply **	Gap
Bank	30	390	300	90
Insurance	33	429	132	297
Financial leasing	50	650	150	500
Governmental entities	6	78	18	60

Total gap = 947

Unfilled cybersecurity positions in Saudi financial sector

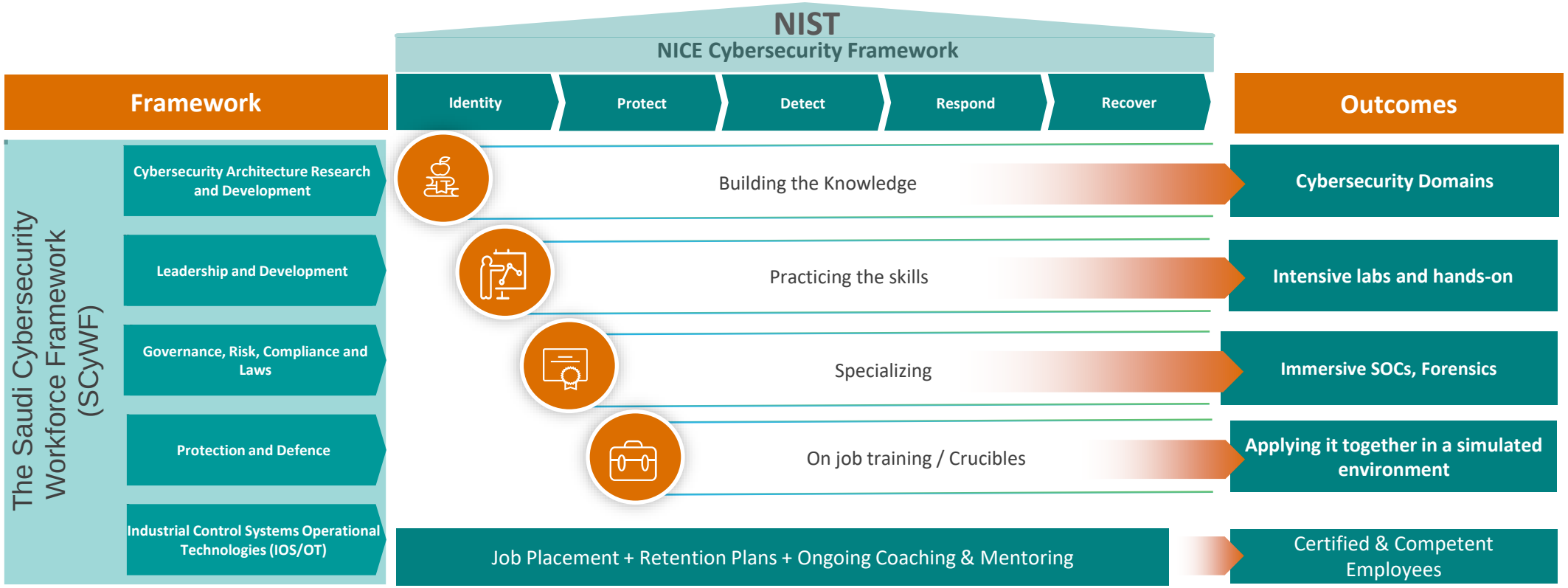


* SAMA website
** Source: Trusted Partners research

The human capital building program is built based on international and national standards (SAMA, NCA and NICE frameworks) with recognized certifications

The program structure will be designed having the most critical frameworks impacting client also designed and tailored to the clients needs after thorough understanding practice of workshops, surveys, interviews, etc..

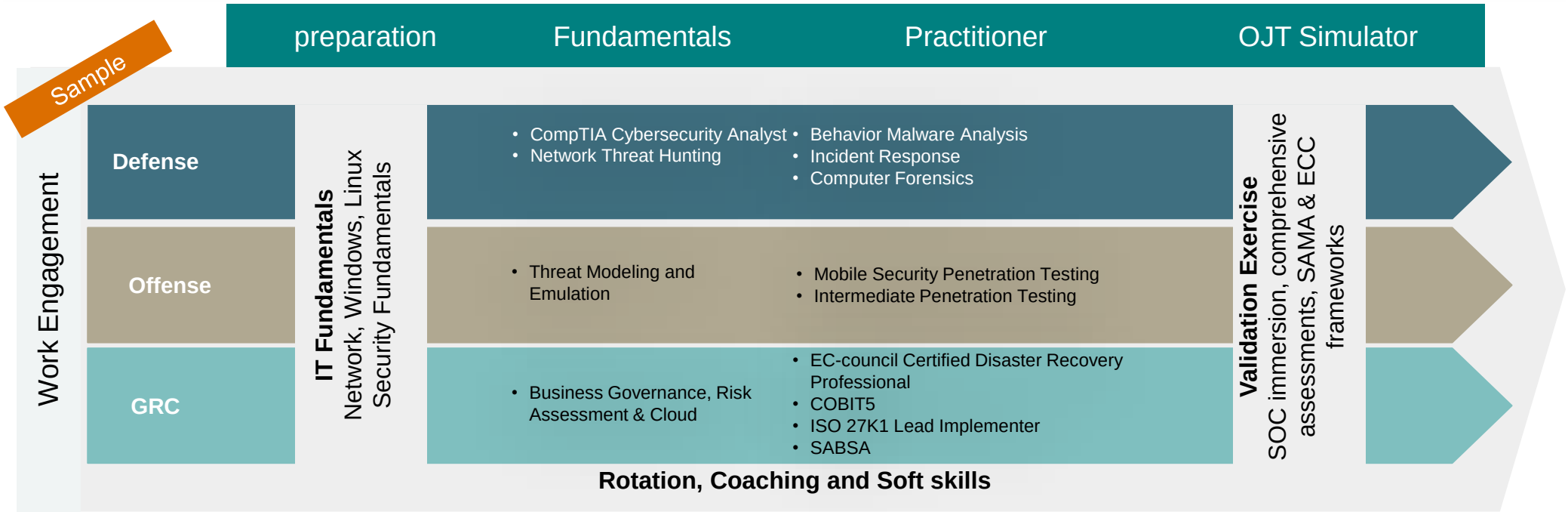
illustrative



Our Guiding Principles focuses on delivering A truly "practitioner" skills & blended learning as well as developing the "right" mindset for better work engagement

Design Guiding Principles

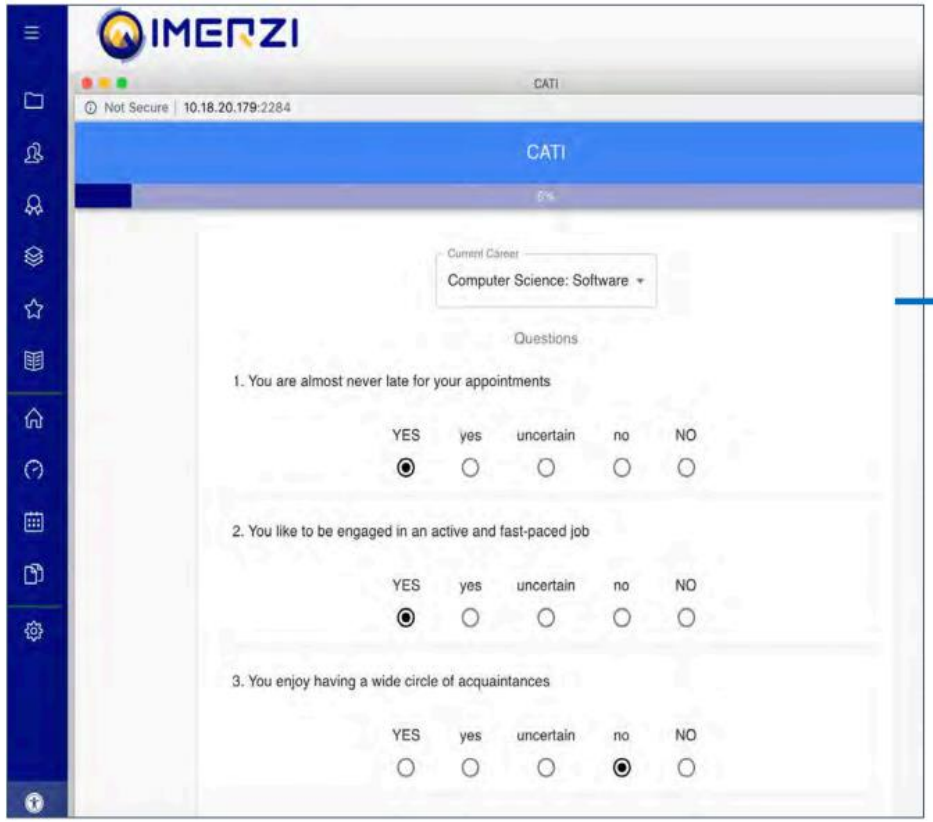
1. **Starting with the basics**
   Our experience shows fresh grads lacks solid IT fundamentals which becomes a learning barrier in such programs
2. **Developing the "right" mindset**
   Building the cybersecurity human capital requires covering all angles to understand the business, defense, and offense aspects.
3. **A truly "practitioner" skills & blended learning**
   Smart and logical flows within the different domains, and intensive hands-on and use-cases based exercises
4. **Unique simulation of OJT**
   Incorporating all the cumulative knowledge in a simulated OJT to better comprehend the business needs of cybersecurity, and accelerate the experiences
5. **Work engagement**
   Enhancing ones' skills through focused trainings, engaging the trainee in work environment throughout the program, and ensuring higher retention and ROI through individual and group coaching and mentoring

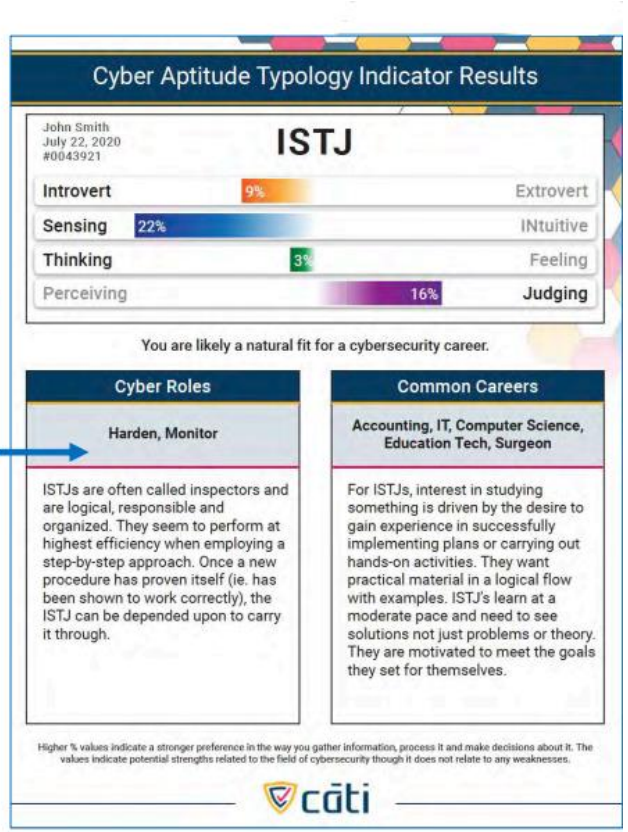


Cybersecurity profiling is key success factor to set suitable training plan and job roles based on core business demand

Cyber Aptitude Typology Indicator (CATI) Assessment

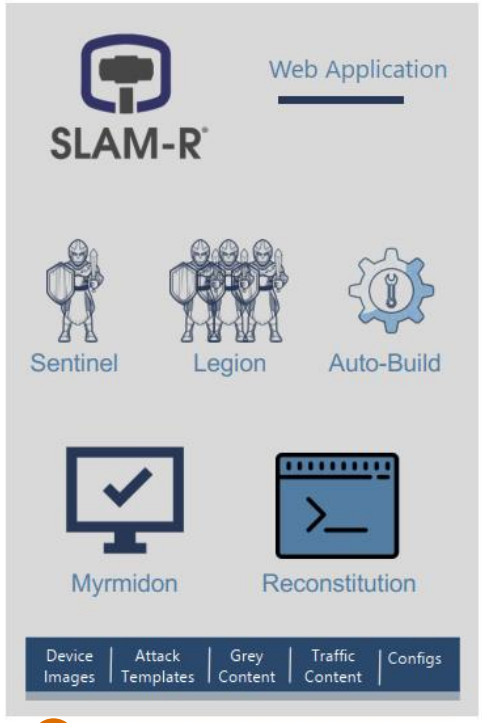
CATI evaluates each individual's unique personality characteristics, intrinsic learning preferences, and skillsets to provide actionable metrics that determine their most compatible work role and career path in cyber.

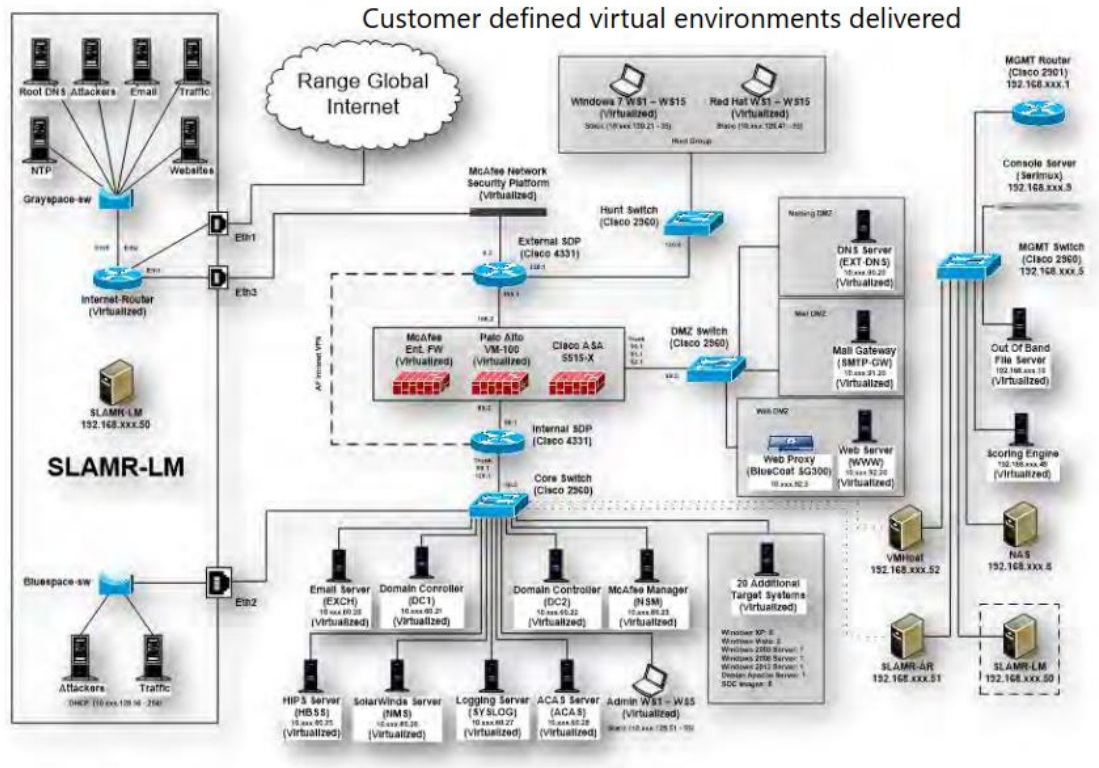




Cyber range is the new generation of cyber education to learn in a simulated environment that replicate the real world use cases

Cyber Enhanced Network and Training Simulators (CENTS)





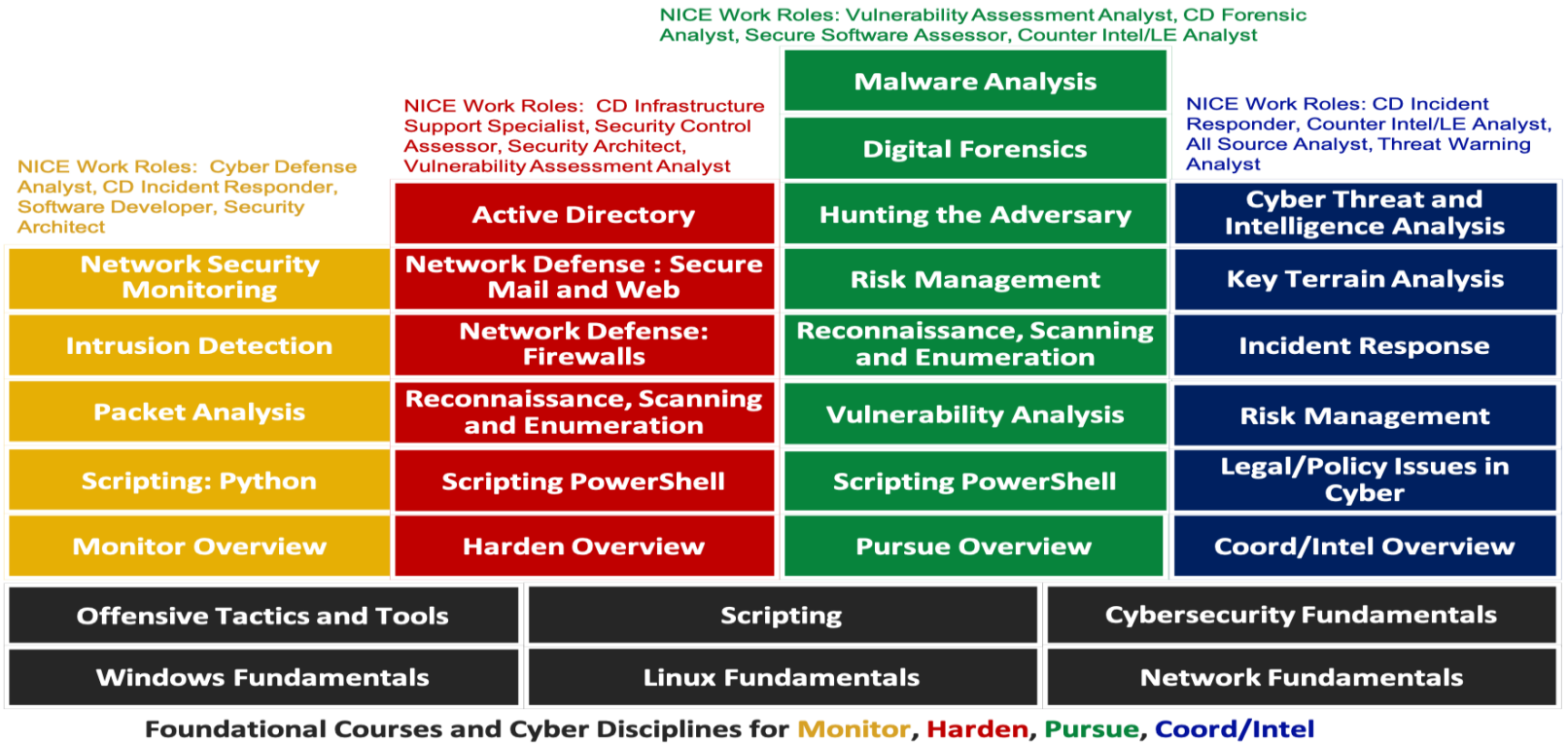
1. A fully customizable cybersecurity training environments to create client closed internet
2. Our focus is to “bring back” the gamified, immersive training through the use of adaptive learning
3. Many different options possible to support cybersecurity teaching, training and exercising

Cyber range is the new generation of cyber education to learn in a simulated environment that replicate the real world use cases

Imerzi Learning Management System (LMS)

Adaptive Immersive Sticky

- Build a LMS that supports and delivers an adaptive and immersive learning environment
- Develop engaging, high fidelity learning and training content
- Tailor the learning experience to the way an individual wants to learn
- Created technical subdisciplines used to teach cybersecurity: Harden / Protect Monitor / Detect Pursue / Respond Intel



trusted
PARTNERS

Thank You