PRESENTATION

Contemporary issues related to Cyberspace & Cybersecurity

By

Dr. Zaki Qureshey
Director General
India's 1st - National Security Cluster

Why Us?

We are India's 1st National Security Cluster

Experts in ***National Cyber Security Strategy, Cyber Warfare Solutions, Penetration testing, Digital Forensics, Capacity Building*** *and* are valuable for trustworthy Organizations & Agencies around the World.

Passion for Winning

Deliver on commitments and go further

Excel on Results

Take Ownership

Passion for People

Open communication

Develop people

Involvement

Build up trust and respect

Integrity

Opportunities

- Centre has initiated several digital initiatives and with increasing use of digital platforms, there could be more cyber-attacks, challenging the existing security infrastructure.
- Telangana being one of the major IT hubs has all the requisites to lead the cyber security.
- India needs 2 million cyber security professionals and this cluster can cater to the training needs.
- HSC will also act as a third party agency in responding to cyber attacks as it is resource and expert capable.

NSC Mission

- Become the Hub for Cyber Security.
- Create satellite clusters in tier-I and tier-II cities across the country.
- Incubate startups operating the cyber security space.
- Capture a bigger pie in the $36 billion projected market for cyber security in India.

Year 1 results

Structure

- Resources directory is up
- Secretariat functional

Innovation

- Startup Incubator is functioning
- Three hackathons conducted

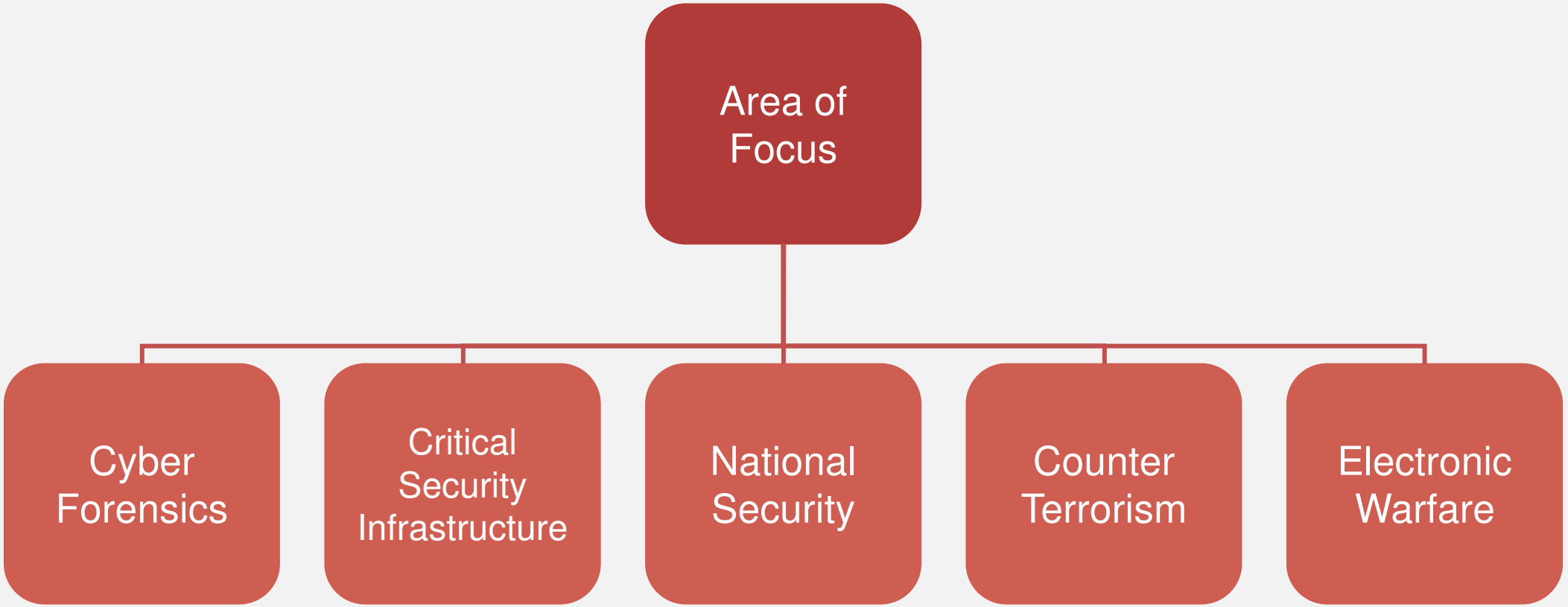
Competencies

- Summer school along with Hague.HSD
- Lab- Cybersecurity for Industry4.0

Expand industry base

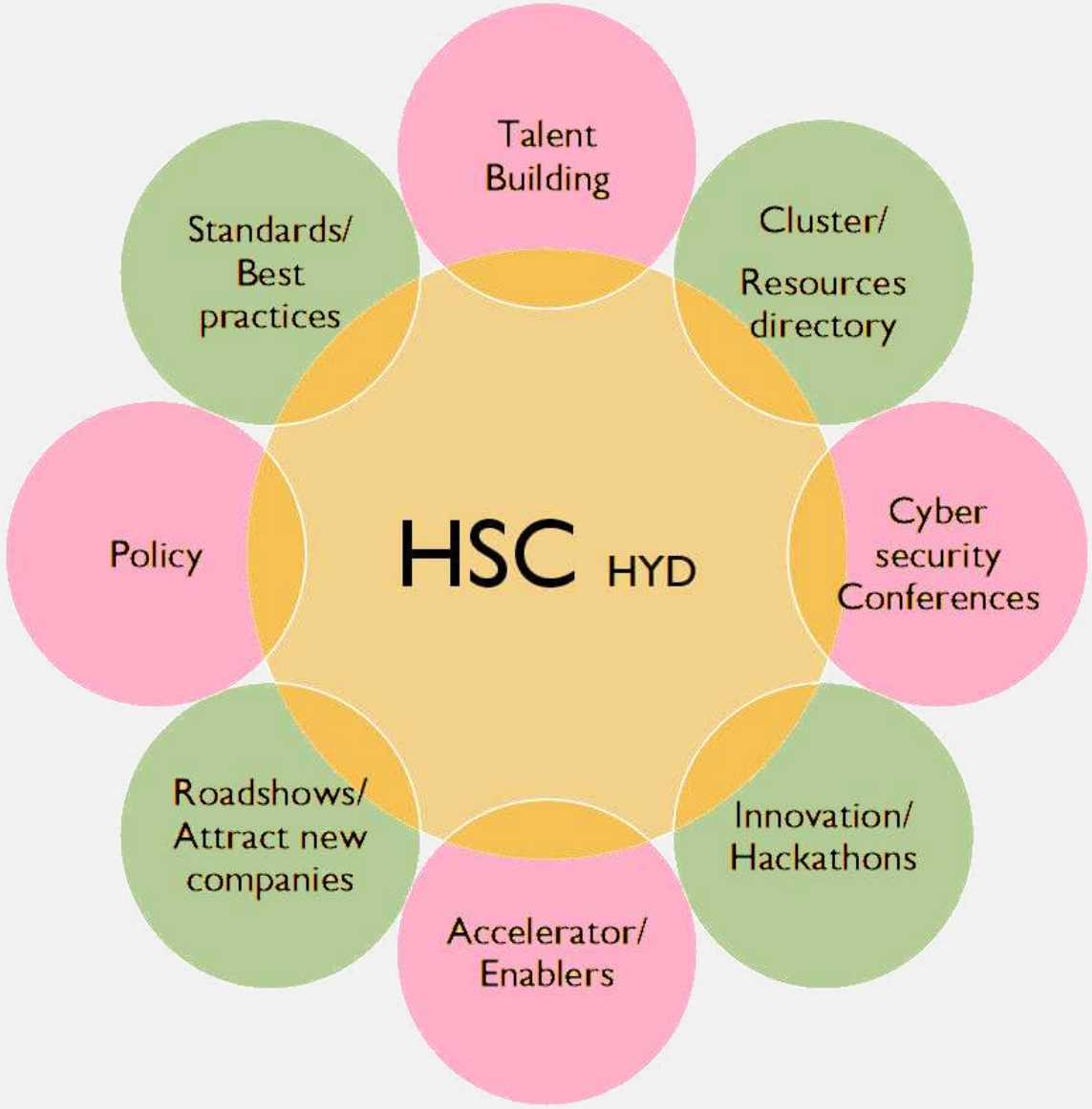
- Incentive & Support scheme defined

Area of Focus



Combat cyber threat to Aadhaar security, banking and other vulnerable areas.

Scope


Talent Building
Cluster/ Resources directory
Cyber security Conferences
Innovation/ Hackathons
Accelerator/ Enablers
Roadshows/ Attract new companies
Policy
Standards/ Best practices
HSC HYD

Cybersecurity & India

NATIONAL

World facing 'bloodless' cyber war threat: Modi

PTI

"THE BLOODLESS WAR"

- **"I dream of digital India where CyberSecurity becomes an integral part of national security"**
- **Clouds of a bloodless war are hovering over the world.**
- **The world is terrified by this... India has a big role to play in this.**
- We have to move from E-governance to M-governance.
- **Can India play this big role? India has talent. Can India provide a shield to the world by providing innovative and credible solutions?**
- Why should we not have such a confidence? We should accept this challenge to ensure that the entire humanity lives in peace

Programmes

- Accelerator programme
- Mentor Network

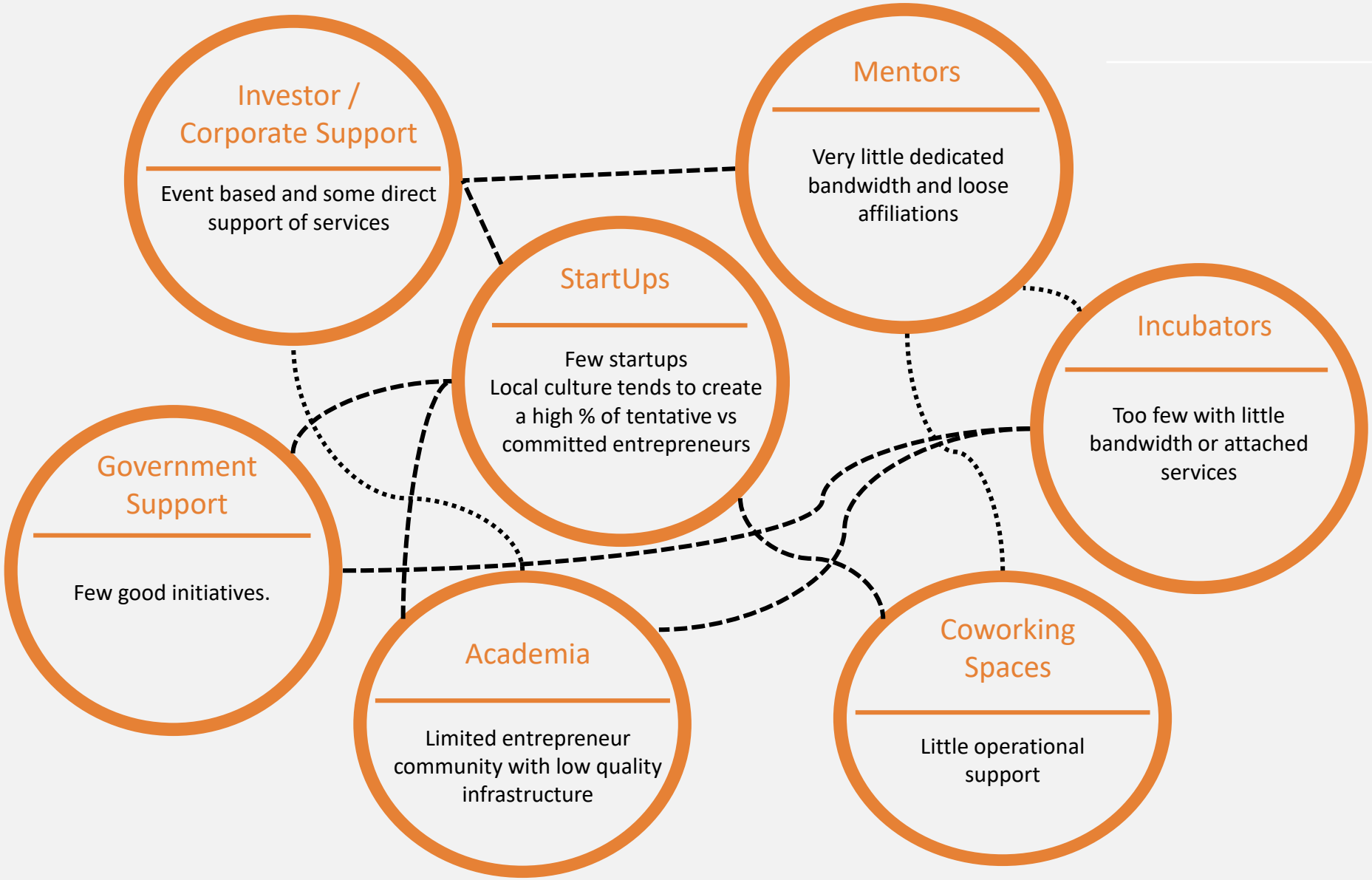
Skill ramp up plan

HSC is also rolling out a Hague-India summer school that will train candidates on cyber security.

Bug bounty programme

Train-the-trainer programme

IMMATURE STARTUP ECOSYSTEM



In The Hague region alone 400 security businesses realize more than 25% of the national turnover in security and employ 13,400 people.

The Hague Security Delta (HSD) is the ***largest security cluster*** in Europe with important regional hubs in The Hague, Twente, and Brabant.

Digital Gateway to Europe

The Netherlands is well known for its excellent logistics, infrastructure and its state-of-the-art digital infrastructure.

Wide range of cyber security organizations

- European Cybercrime Centre Europol (EC3)
- National Cyber Security Centre
- NATO Communications and Information Agency
- Cyber Security Academy.

HSD Campus Innovation Centre

The Innovation Centre is an inspiring meeting place for entrepreneurs, students and professionals in the security cluster.

HSD Campus International Centre

The international Centre is located at ***WTC The Hague***. This makes the International Centre an ideal base for international companies in the 'security' domain to enter the Dutch or European market.

Dutch Institute for Technology Safety & Security

- High-tech Solutions
- Camera
- Sensor Technology

HSD

Twente Safety & Security

- Nano technology
- Safety
- Radar
- Sensors

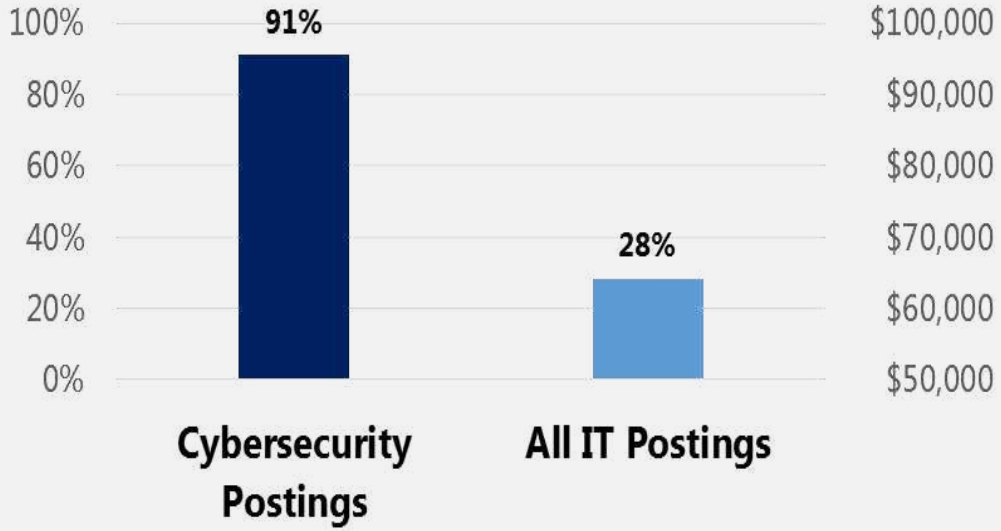
The Hague area

- Cyber Security,
- Forensics,
- National Security
- Critical Infrastructure

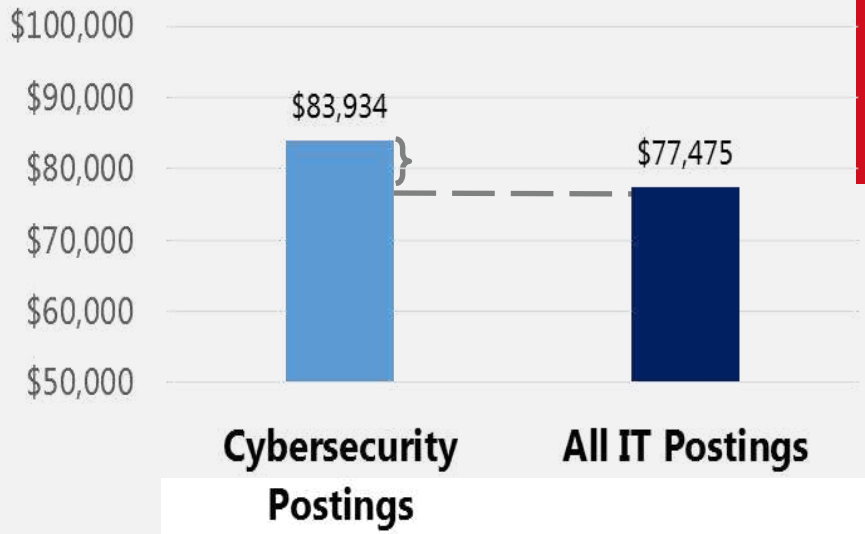
Working Across All Sectors

NATION CAPACITY BUILDING

Growth in Job Postings (2010-2014)



Cybersecurity Salary Premium



INDIA NEEDS 8 MILLION CYBER SECURITY PROFESSIONALS.

Juniper research recently predicted that Rapid Digitization of personal lives and enterprise records will increase the cost of data breaches to $ 3.1 trillion globally by 2022.

Source: Forbes

Title	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)
Engineer (e.g. Security Engineer, Information Assurance Engineer)	26%	42,355
Manager/Admin (e.g. Data Security Administrator, Information Security Manager)	19%	30,586
Analyst (e.g. IT Security Analyst, Cyber Intelligence Analyst)	18%	28,853
Specialist/Technician (e.g. IT Security Specialist, Infosec Technician)	10%	15,289
Architect (e.g. Security and Privacy Architect, Network Security Architect)	5%	8,409
Auditor (e.g. IT Auditor)	5%	7,533
Consultant (e.g. Network Security Consultant, Infrastructure Security Consultant)	4%	6,294

"CYBER EDUCATION IS THE KEY TO NATIONAL SECURITY"

To cater to the demands of the new Economy, thousands of institutes & learning centers' are being established Globally, offering skills, training & Certifications.

Unfortunately, it was evident that expert instructors, infrastructure and the proper curriculum are not easily available. This situation is leading to functionally "illiterate" and "under-prepared" ***IT Security Experts!***

Our Programs are designed to extend ***Employment, Education & Entrepreneurial*** opportunities in the world.

Our collaborative Programs are entirely scalable and replicable for simultaneous deployments throughout the cyber world with a Digital License.

CYBER SECURITY

Trends | Necessity |
Opportunities

- Cyber Space is the virtual space that connects all of us and enables information exchange
- It works over the environment of computer networks
- It has no boundaries, mass, or gravity
- It exists in the form of bits and bytes – zeroes and ones (0's and 1's) which changes every second.
- Cyberspace is the fifth domain of power after land, air, water and space

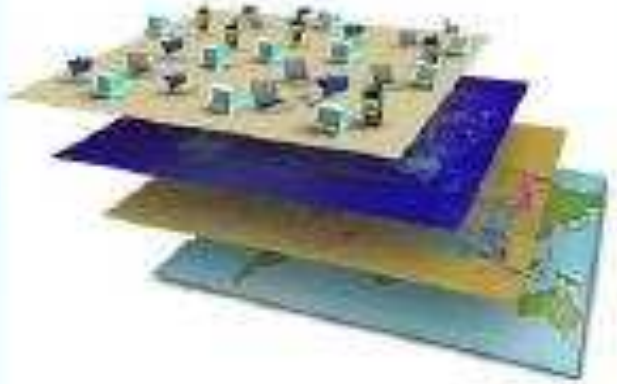
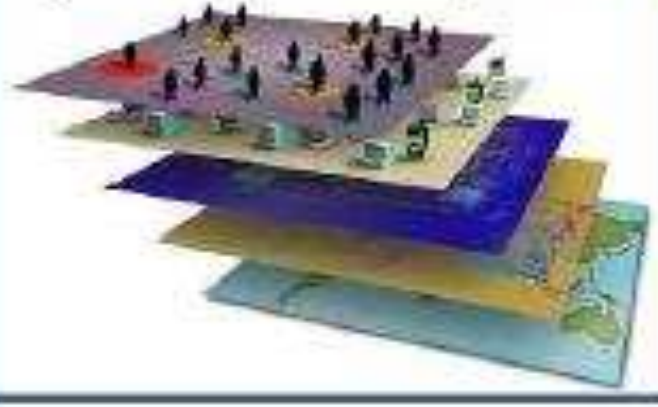
Features of cyberspace

Anonymity	Creativity
Global Access	Connectivity
Virtuality	Ambiguity
Interactivity	Expansion

Cyberspace vs. Physical World

Physical World	Cyberspace
Static, well-defined, and incremental	Dynamic, undefined, and exponential
Has fixed contours	Is vast as human imagination and has no fixed shape
It has physical time	It has execution time
Based on laws of physics	Based on program execution

Components of Cyberspace are on three levels

Physical Layer	Logical Layer	Social Layer
Geographic Components	Logical Network Components	Persona Components
		
Physical Network Components		Cyber Persona Components
		

DARK SIDE OF

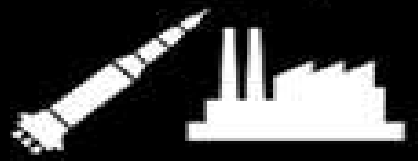
CYBERSPACE

Contemporary issues in Cyberspace

✓ Cyber Fraud	✓ Cyber Piracy/copyright infringement
✓ Cyber Gambling	✓ Cybersquatting
✓ Cyber (child) Pornography	✓ Cyber denial of service
✓ Cyber Prostitution	✓ Cyber Spoofing
✓ Cyber Impersonation	✓ Cyber Spying
✓ Cyber Blackmail	✓ Cyber Espionage
✓ Cyber Extortion	✓ Cyber Terrorism
✓ Cyber Harassment	✓ Cyber Warfare
✓ Cyber Defamation	✓ Cyber Murder
✓ Cyber Malware	✓ Cyber Jacking
✓ Cyber illicit business	

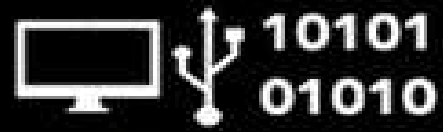
HARM TO SOCIETY VIA CYBERSPACE

intentional **physical harm**
sabotage | critical infra



accidental **physical harm**
critical infra

IN CYBERSPACE



intentional | **accidental**

attack | exploit
disruption |theft

error | failure
outage

intentional
informational
harm
crime | espionage
privacy | disinformation

accidental
informational
harm
privacy | misinformation

Various Cybercrimes / threats to the Cyberspace			
Classification	**Attack**	**Description**	**Examples**
BASED ON PURPOSE	Reconnaissance attack	It involves unauthorized detection system mapping and services to steal data.	• Packet Sniffers • Port Scanning • Ping Sweeps • DNS queries
	Access attack	It is an attack where intruder gains access to a device to which he has no right for access.	• Port trust utilization • Port redirection • Dictionary attacks • Man-in-the-Middle attacks • Social engineering attacks & phishing
	Denial of Service (DoS) attack	It is the Intrusion into a system by disabling the network with the intent to deny service to authorized users.	• Smurf • SYN Flood • DNS attacks • DDoS attack

Various Cybercrimes / threats to the Cyberspace			
Classification	**Attack**	**Description**	**Examples**
LEGAL CLASSIFICATION	Cyber Crime	It is the use of computer and Internet to exploit users for materialistic gain.	• Identity theft • Credit card fraud
	Cyber Espionage	It is the act of using the internet to spy on others for gaining benefit.	• Tracking Cookies • RAT Controllable
	Cyber Terrorism	It is the use of cyber space for creating large scale disruption and destruction of life and property.	• Crashing the power grids by al-Qaeda via a network • Poisoning of water supply
	Cyber War	It is the act of a nation with the intention of disruption of another nation's network to gain tactical and military advantages.	• Russia's war on Estonia (2007) • Russia's war on Georgia (2008)

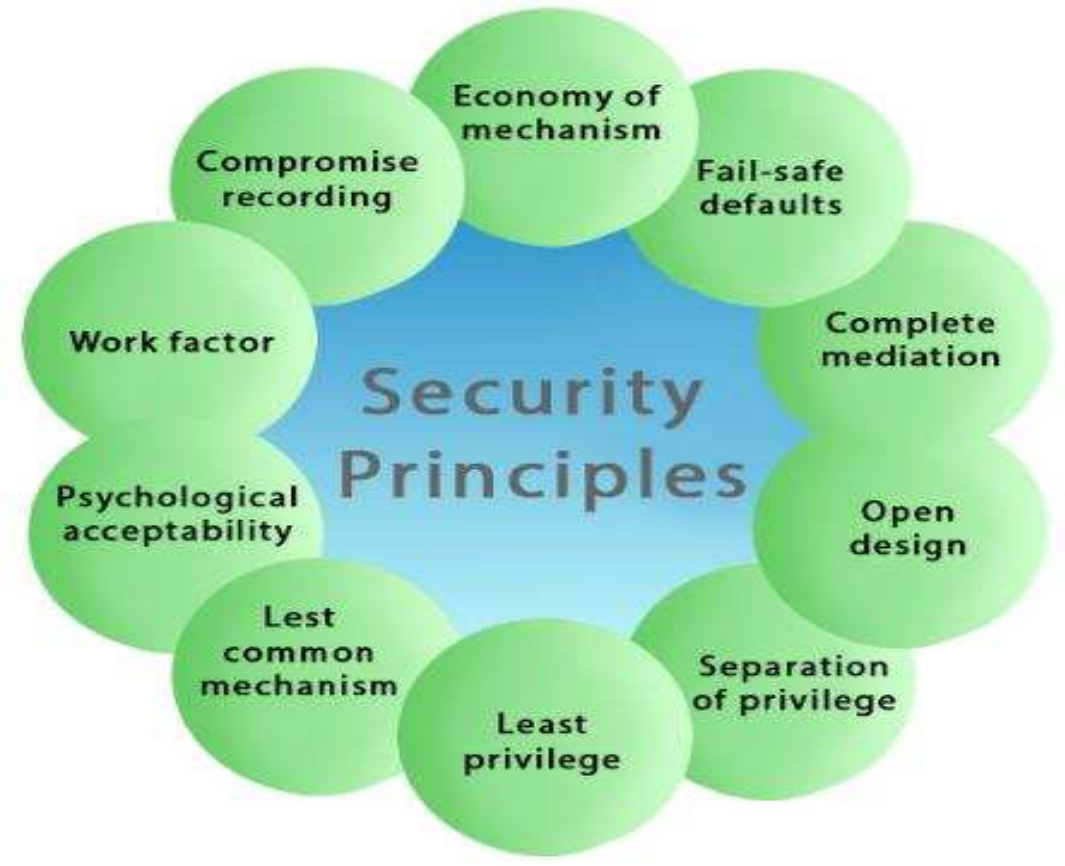
Various Cybercrimes / threats to the Cyberspace			
Classification	**Attack**	**Description**	**Examples**
BASED ON SEVERITY OF INVOLVEMENT	Active Attacks	It is the attack of data transmission to all parties thereby acting as a liaison enabling server compromise.	• Masquerade • Replay • Modification of message
	Passive Attacks	It is the attack which is primarily eavesdropping without meddling with the database.	• Traffic Analysis • Release of message contents
BASED ON SCOPE	Malicious Attack	It is the attack with deliberate intent to cause harm resulting in large scale disruption.	• Sasser Attack
	Non-malicious attack	It is the accidental attack caused due to mishandling or operational mistakes with minor loss of data.	• Registry corruption • Accidental erasing of hard disk

Various Cybercrimes / threats to the Cyberspace			
Classification	**Attack**	**Description**	**Examples**
BASED ON NETWORK	Attacks in MANET	This attack aims to slow or stop the flow of information between the nodes.	• Byzantine attack • Black Hole attack • Flood Rushing attack • Byzantine Wormhole attack
	Attacks on WSN	It is an attack which prevents the servers from detecting and transmitting information through the network.	• Application Layer Attack • Transport Layer Attack • Network Layer Attack • Multi-Layer Attacks


CYBER
SECURITY

- The process of securing information or assets contained in cyberspace is known as cybersecurity. This is especially important in governments and business world which require sophisticated defence methods.

Cyber Security Principles



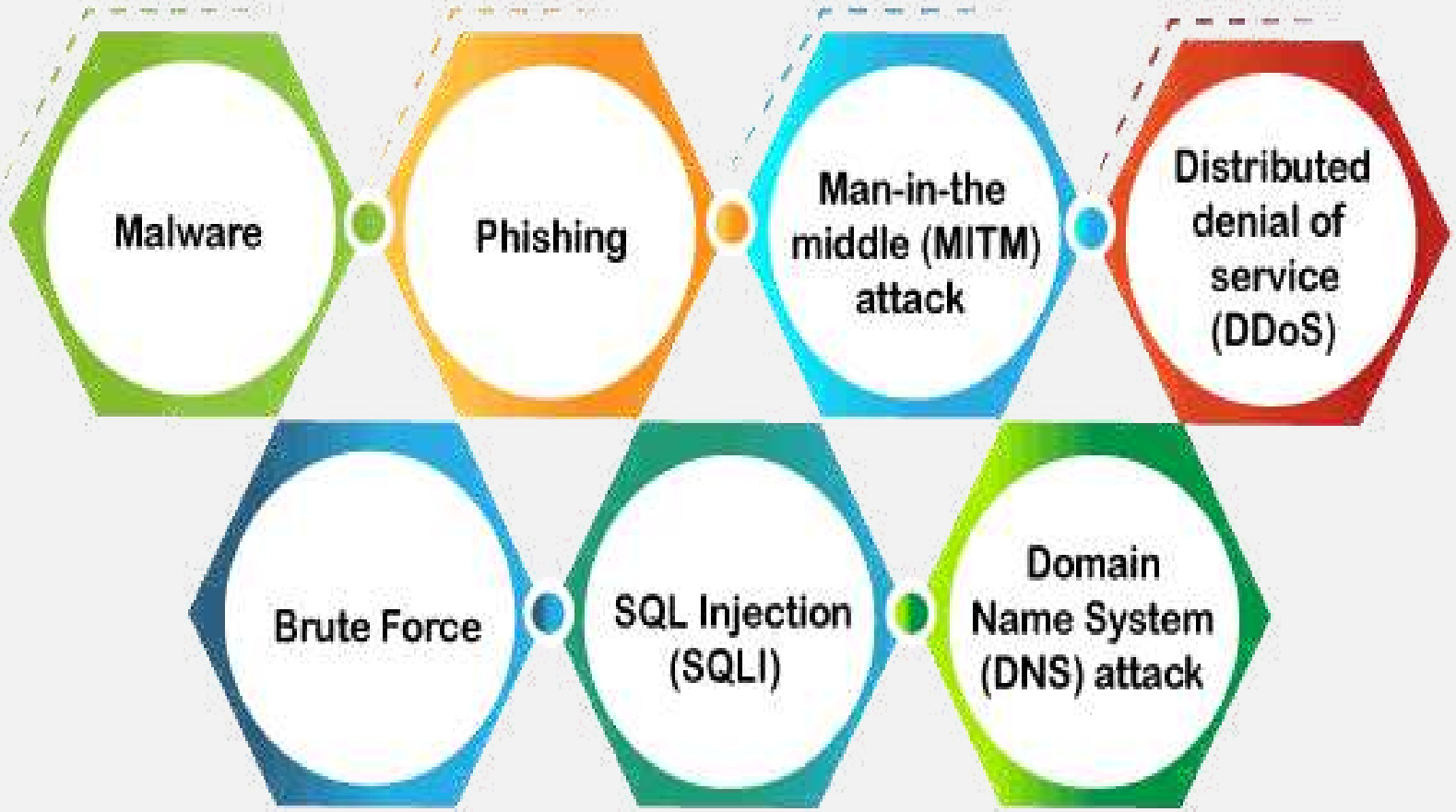
Types of Cyber Security

- Network Security
- Application Security
- Information or Data Security
- Identity management
- Operational Security
- Mobile Security
- Cloud Security
- Disaster Recovery & Business Continuity Planning
- User Education

Cyber Security Goals

- Cyber Security's main **objective is to ensure data protection**.
- The security community provides three related principles to protect the data from cyber-attacks, called the **CIA triad**. When any security breaches are found, one or more of these principles has been violated.

Types of Cyber Threats



- **Malware** is malicious software used by hacker to disrupt or damage user's system.

Some important types of malware

- **Virus** is a code that spreads from one device to another. It spreads throughout a computer system, infecting files, stealing information, or damage device.
- **Spyware** is a software that secretly records information about user activities on their system.
- **Trojans** is a malware code that appears as legitimate software or file to fool users into downloading and running. It corrupts or steals data from device or do other harmful activities on network.
- **Ransomware** is a software that encrypts a user's files and data on a device, rendering them unusable or erasing. Then, a monetary ransom is demanded.
- **Worms** is a piece of software that spreads copies of itself from device to device without human interaction. It does not attach to any program to steal or damage the data.
- **Adware** is an advertising software used to spread malware and displays advertisements on devices. The objective of this program is to generate revenue for its developer by showing ads.
- **Botnets are** a collection of internet-connected malware-infected devices which enables cybercriminals to get credentials leaks, unauthorized access and data theft without user's permission.

- **Phishing** is a type of cybercrime in which sender seems to come from genuine organization like PayPal, eBay, financial institutions, or friends and co-workers. They contact targets via email, phone, or text message with a link to persuade them to click that links. It will redirect them to fraudulent websites to provide sensitive data such as personal information, banking and credit card information, social security numbers, usernames, and passwords.
- **Man-in-the-middle (MITM) attack** is a cyber threat in which criminal intercepts conversation or data transfer between two individuals. Once cybercriminal places themselves in the middle of two-party communication, they seem like genuine participants and can get sensitive information and return different responses. The main objective of MITM attack is to gain access to business or customer data.
- **Distributed denial of service (DDoS)** is a type of cyber threat or malicious attempt where criminals disrupt targeted servers, services or network's regular traffic by fulfilling legitimate requests to the target or its surrounding infrastructure with Internet traffic. Here the requests come from several IP addresses that can make the system unusable, overload their servers, slowing down significantly or temporarily taking them offline, or preventing an organization from carrying out its vital functions.

- **Brute Force** attack is a cryptographic hack that uses trial-and-error method to guess all possible combinations until the correct information is discovered. Cybercriminals usually use this attack to obtain personal information about targeted passwords, login info, encryption keys, and Personal Identification Numbers (PINS).

- **SQL Injection (SQLI) i**s an attack that occurs when cybercriminals use malicious SQL scripts for backend database manipulation to access sensitive information. Once the attack is successful, the malicious actor can view, change, or delete sensitive data, user lists, or private details stored in the SQL database.

- **Domain Name System (DNS) attack** is a type of cyberattack in which criminals take advantage of flaws in the Domain Name System to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers.

Classification of Cyber attacks

Web-based attacks	System-based attacks
Injection attacks	Virus
DNS Spoofing	Worm
Session Hijacking	Trojan horse
Phishing	Backdoors
Brute force	Bots
Denial of Service	
Dictionary attacks	
URL Interpretation	
File Inclusion attacks	
Man-in-the-Middle (MITM)	


Security Monitoring
Data Security
Endpoint Protection
Application Security
Network Security
Backup & Archiving
Identity Management
Cyber Security Solutions
DSGVO
Mail-, Web- & Mobile Security
Industrial Security
IOT Security
Cloud Security
Artificial Intelligence


national
security
Shift

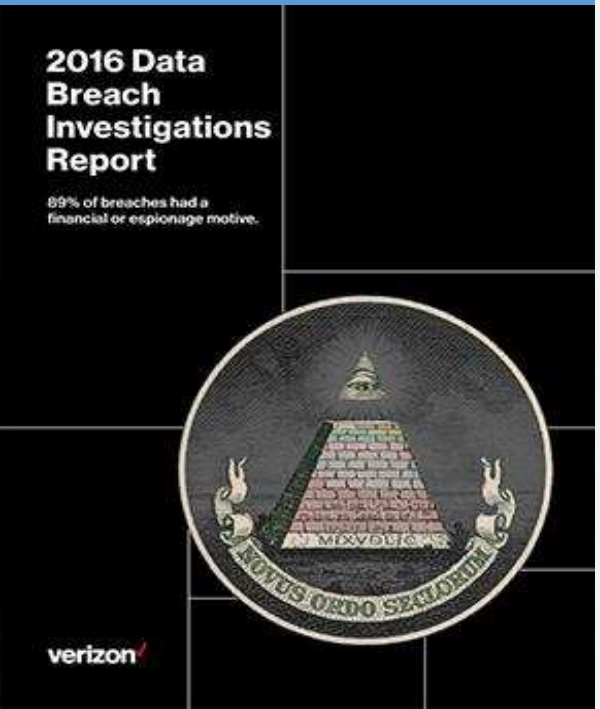
- Cyberspace has become the cheapest weapon in present era.
- India has the second highest number of internet users in the world.
- According to Indian Computer Emergency Response Team (CERT) in 2020 India witnessed 6.97 lakh cyber security incidents.
- The major challenge that exists in cyberspace is the anonymity, as it creates security breaches and complexity between individuals and government legislations.
- The cyberspace becomes more dangerous with advent of Artificial Intelligence (AI), Worms, viruses and Zombie software. Cyberspace has made the task of terrorist organisations easier in order to recruit, radicalize and train people across continental boundaries.
- Recent major cyber-attacks on India are by a Chinese group, Red Echo which targeted the power facilities.
- Another incident Stone Panda a Chinese hacker group tried to hack into IT infrastructure of India and supply chain of Bharat Biotech and Serum Institute of India.

- **National Cyber Security Strategy 2020** of India is the latest attempt to strengthen cybersecurity in India.

- Its main objective is to secure the national cyberspace, prevent critical infrastructure of the country like financial services, power services, nuclear power plants, and manufacturing services. The adoption of **5G technology** in India also paved the way for this strategy.

- This strategy aims to form strong security mechanism for government, individuals and for businesses. In order to implement these strategies there are dedicated departments and agencies which ensures proper resolution of cyber related issues such as Ministry of Electronics and Information Technology, National Security Council Secretariat, Cyber Swachhta Kendra, Cyber and Information Security Division (C&IS) under ministry of Home Affairs, National Technical Research Organisation.

VERIZON DBIR



Verizon's annual Data Breach Investigations Report, mentions that the number of attacks by state-affiliated actors had nearly tripled from last year.

Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	159	102	20	37
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

CYBER CRIMES AND ITS TYPES

Crimes Against Persons Property:

- Intellectual Property Crimes
- Cyber Squatting
- Cyber Vandalism
- Hacking Computer Systems
- Transmitting Virus
- Cyber Trespass
- Internet Time Thefts

Cybercrimes Against Government

- Cyber Terrorism:
- Cyber Warfare:
- Distribution of pirated software
- Possession of Unauthorized Information

Cyber Crimes against an individual

- Harassment via E-Mails
- Cyber-Stalking
- Morphing
- Dissemination of Obscene Material
- Defamation
- Hacking
- E-Mail Spoofing
- SMS Spoofing
- Carding
- Child Pornography
- Cheating & Fraud
- Assault by Threat/Cyber bullying

CYBER SECURITY TRENDS

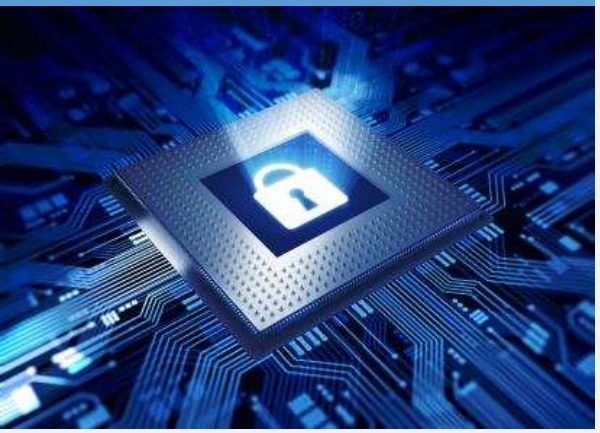
JOBS ARE IN DEMAND

Cybersecurity jobs are in demand and growing across the economy

- The Professional Services, Finance, and Manufacturing/Defense sectors have the highest demand for cybersecurity jobs.

- The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as Finance (+137% over the last five years), Health Care (+121%), and Retail Trade (+89%).

FINANCIAL SKILLS OR A SECURITY CLEARANCE ARE EVEN HARDER



Positions calling for financial skills or a security clearance are even harder to fill than other cyber security jobs.

- The hardest-to-fill cybersecurity jobs call for financial skills, such as Accounting or knowledge of regulations associated with the Sarbanes-Oxley Act, alongside traditional networking and IT security skills. Because finance and IT skills are rarely trained for together, there is a skills gap for workers who meet the requirements of these “hybrid jobs.”

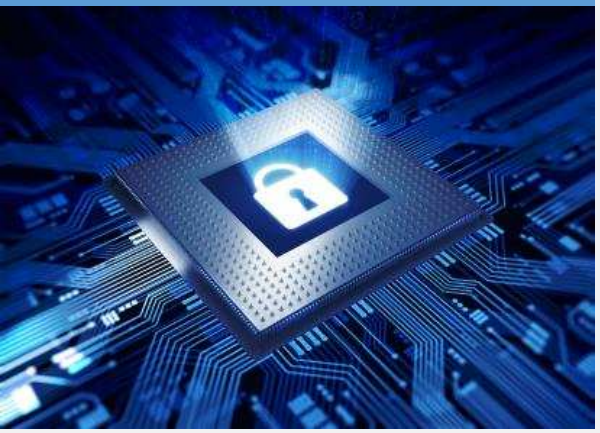
- More than 10% of cybersecurity job postings advertise a security clearance requirement. These jobs, on average, take 10% longer to fill than cybersecurity jobs without a security clearance.

REQUIRE CERTIFICATIONS

Cybersecurity positions are more likely to require certifications than other IT jobs

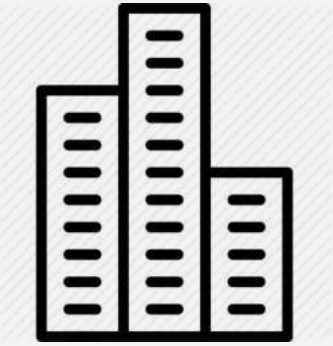
- One third (35%) of cybersecurity jobs call for an industry certification, compared to 23% of IT jobs overall.

HIGH CONCENTRATION OF JOBS IN GOVERNMENTS



Geographically, cybersecurity jobs are concentrated in government and defense hubs, but are growing most quickly in secondary markets

- On a per capita basis, the leading states are Washington D.C., Virginia, Maryland, and Colorado; all have high concentrations of jobs in the federal government and related contractors.



CYBER SECURITY IN ACADEMICS

CYBER SECURITY PROFESSIONALS NEEDED

It is estimated that India will require 8 lakh cyber security professionals by 2022 to support its fast growing internet economy as per an estimate by the union ministry of information technology.

The financial sector alone is expected to hire over 2 lakh people while telecoms, utility sectors, power, oil & gas, airlines, government (law & order and e-governance) will hire the rest.

The country's information security market is expected to grow by 18% to reach Rs. 1,415 crore in 2013 and **36 Billion USD** by 2020.

Despite a continuing economic slowdown, cyber security would continue on an upward trajectory, reaching $86 billion in 2016, up from $60 billion in 2012.

Universities with Cyber security in their curriculum

Abertay University

Created in 2006, this course became the first undergraduate degree in the world with the word 'hacking' in the title. This course is now recognized as one of the UK's leading vocational security programs.

Florida International University

FIU is one of the first public universities to offer a graduate degree program in cyber security and an undergraduate degree with a concentration in this field. The undergraduate track has 50 students and includes cutting-edge classes in malware analysis, digital forensics and security of the Internet of Things. Student research topics sound like the titles of Hollywood cybercrime capers: Pharming, Creating Exploits, Key loggers.

Oakland University

Oakland University has partnered with Merit Professional Development and the Michigan Cyber Range to offer an introductory Certified Professional Ethical Hacker (CPEH) course on the fundamentals of penetration testing and ethical hacking.

CAREER PROSPECTS

CYBER SECURITY

- Auditing
- IS Management Leadership
- Application and secure code
- Healthcare
- Virtual Machine
- Wireless Security
- Incident Handling
- Disaster Recovery
- Forensics

ITS NOT ONLY ABOUT HACKING

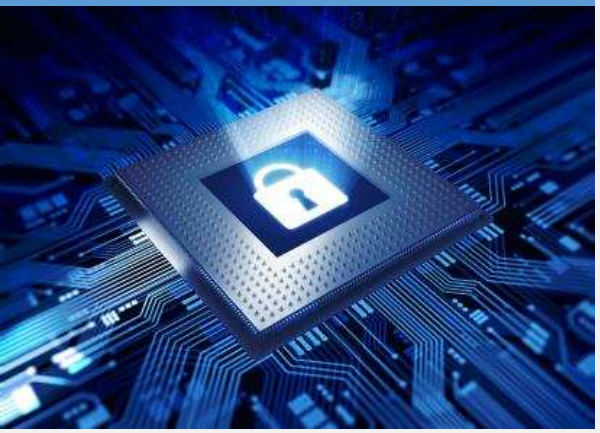
ITS ABOUT UNDERSTANDING COMPUTERS

- Computer components
- Computer architecture
- Programming languages
- System application programming
- Socket programming
- Web application programming
- Automation
- Embedded systems
- Distributed Operating systems
- Kernel and User spaces
- TCP/IP and networking
- Protocols and PDUs
- Cryptography

UNDERSTAING HACKING DRIVES US TO UNDERSTAND BASICS AND SECURITY MECHANISMS

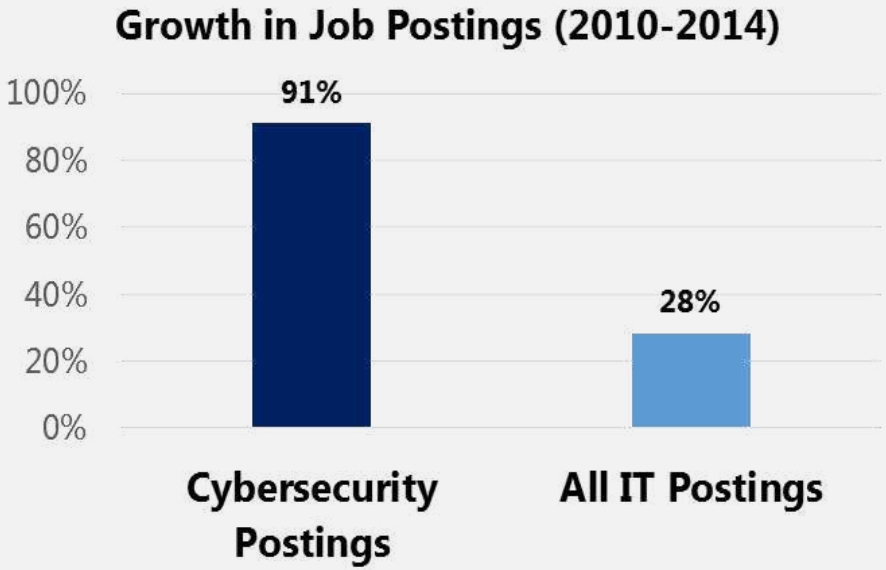
- Access control lists
- Firewalls
- IPS/IDS
- Authentication servers
- Sandboxing
- Anti Viruses
- Anti Malwares
- SIEM
- SOC
- Network monitoring
- Information Rights management
- VPNs and Proxies

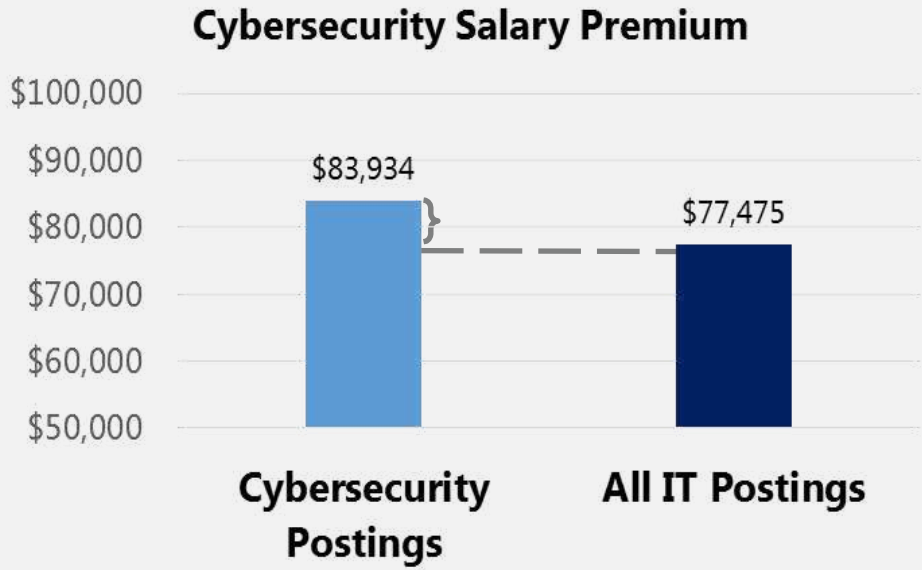
JOB MARKET BY NUMBERS



In 2014, there were 238,158 postings for cybersecurity-related jobs nationally. Cybersecurity jobs account for11% of all IT jobs.

- Cybersecurity postings have grown 91% from 2010-2014. This growth rate is more than faster than IT jobs generally.
- Cybersecurity posting advertise a 9% salary premium over IT jobs overall.
- Cybersecurity job postings took 8% longer to fill than IT job postings overall.
- The demand for certificated cybersecurity talent is outstripping supply. In the U.S., employers posted 49,493 jobs requesting a CISSP, recruiting from a pool of only 65,362 CISSP holders nationwide



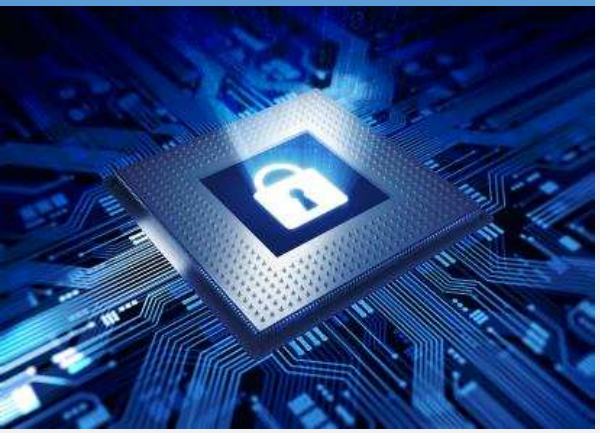


DEMAND GROWS IN FINANCE, PROFESSIONAL SERVICES

Industry Sector	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)	2010 - 2014 Posting Growth
Professional Services	37%	49,765	57%
Finance and Insurance	13%	17,873	131%
Manufacturing & Defense*	12%	15,968	57%
Public Administration	7%	9,725	N/A**
Information	6%	8,522	65%
Health Care and Social Assistance	6%	7,915	118%
Retail Trade	3%	3,505	120%
Other	15%	19,983	N/A**

Engineers, Managers, and Analysts Dominate the Field

Title	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)
Engineer (e.g. Security Engineer, Information Assurance Engineer)	26%	42,355
Manager/Admin (e.g. Data Security Administrator, Information Security Manager)	19%	30,586
Analyst (e.g. IT Security Analyst, Cyber Intelligence Analyst)	18%	28,853
Specialist/Technician (e.g. IT Security Specialist, Infosec Technician)	10%	15,289
Architect (e.g. Security and Privacy Architect, Network Security Architect)	5%	8,409
Auditor (e.g. IT Auditor)	5%	7,533
Consultant (e.g. Network Security Consultant, Infrastructure Security Consultant)	4%	6,294



In todays world ethical hacking is not enough. We are the future in IT Security.

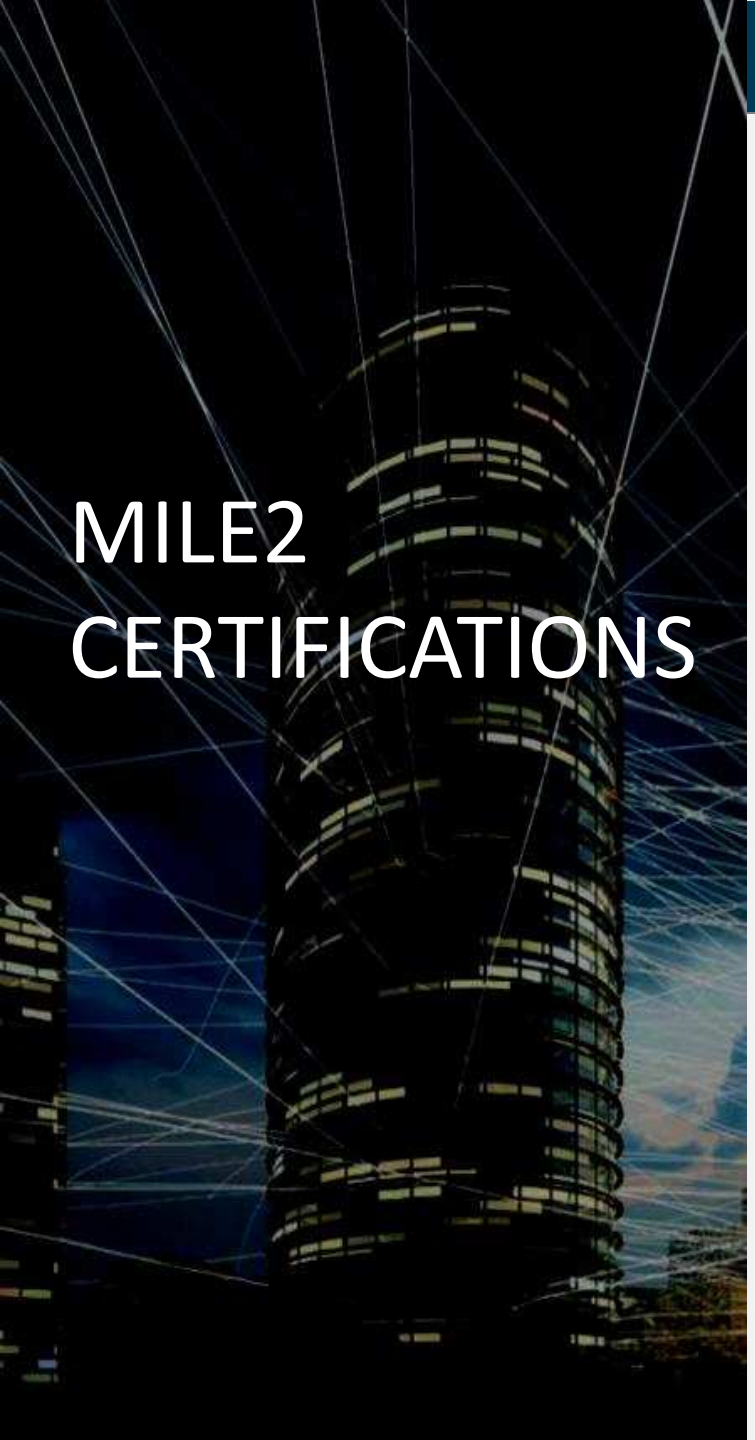
Courses specifically designed for elite organizations

C)PTE
Certified Penetration Testing Engineer
United States Air Force

C)NFE
Certified Network Forensics Examiner
United States Counterintelligence Agency

C)ISSO
Certified Information Systems Security Officer
Canadian Department of National Defense

C)SWAE
Certified Secure Web Application Engineer
Boeing Aerospace



MILE2 CERTIFICATIONS

CAREER AREA	FUNDAMENTAL	FOUNDATIONAL	SPECIALIZED	ADVANCED
IS Management Leadership	C)SP & C)SAP	C)ISSO	IS20Controls	C)SLO
Pen Testing Hacking	C)VA	C)PEH*	C)PTE*	C)PTC*
Incident Handling	C)SP	C)ISSO	C)IHE*	-
Forensics	C)SP	C)DFE*	C)VFE*	C)NFE*
Disaster Recovery	C)SP	C)ISSO	C)DRE	-
Wireless Security	C)SP	C)ISSO	C)WSE	-
Healthcare	C)SP	C)ISSO	C)HISSP	
Auditing	C)SP	C)ISSO	C)ISMS-LA & C)ISMS-LI	C)ISSA
Application & Secure Code	C)SP	C)ISSO	C)SWAE*	C)SWAC*
Cloud Security	C)VCP	C)VE*	C)CSO*	C)CSC*
Virtualization & Virtualization Security	C)VCP	C)VE*	C)VSE*	C)VDE*
IS Management Electives	C)ISSM	C)ISRM	ISCAP	C)ISS*
Virtualization &Cloud Electives	C)PCE*	-	-	-

U.S. Air Force -Testimonies

U.S. Air Force Base: "These courses cannot be substituted with a **Certified Ethical Hacker (CEH)** curriculum."

U.S. Air Force Statement of Work 05T0273 won by mile2. Prospective respondent to the solicitation asked the following question:

Q: "Why doesn't Wright-Patterson AFB want a CEH-certified curriculum?"

USAF's response was as follows: "CEH-certified courses tend to focus on teaching the student how to use a handful of tools that are available on the internet. While this knowledge is somewhat useful during a penetration test, our goal is to expand on this and learn how to turn our results into a professional report. We need to learn the methodology behind a full penetration test with identifying protection opportunities, justifying testing activities and optimizing security controls to reduce business risk."


1 Year Ultimate Combo
$950 (SAVE $1100)!
• Course Video
• E-Workbook

Ministry of External Affairs
Government of India

The formation of India's 1st CyberSecurity Cluster-HSC was endorsed by both the Prime Ministers with signing a "Program of Corporation"

Aadhaar link & De
cyber vulnerable:

Dutch cyber shield for Hyd security & forensic cluster

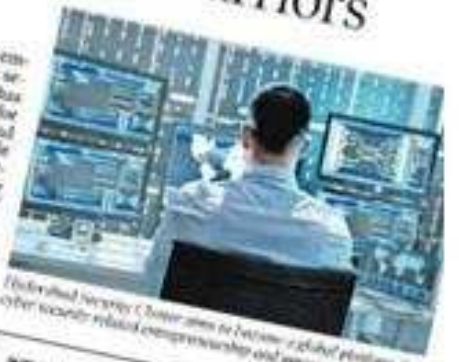
Artificial Intel
'o Plug Chinks
n The Armour

GEARING UP FOR SECURITY

- India's first cyber security cluster, HSF, to cover cyber forensics
- 'Programme of cooperation' between HSF and

HSC, academia to jointly create cyber warriors

Y V PHANI RAJ



INTU-H came up with a special course in cyber security in line with the emerging industry demands and job opportunities

Hyd to have largest cyber security hub

Hyderabad Security Cluster being developed to combat cyber-attacks and create cyber warriors

India's first cyber security cluster to come up in Hyd

It Is Modelled On The Hague Security Delta

A CRADLE OF COLLABORATION

Hyderabad to create cyber warriors for world

Y V PHANI RAJ

Hyderabad Security Foundation (HSF), which is creating the country's first cyber security cluster — Hyderabad Security Cluster (HSC), is going to address the growing cyber threat experienced in banking healthcare, power, telecom

Our Partners

VREDE EN RECHT
Den Haag

NCI AGENCY

EUROPOL
EC3 | European Cybercrime Centre

INTERNATIONAL COURT OF JUSTICE

verizon

The Hague Centre for Strategic Studies

GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

HSD
The Hague Security Delta

جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences

HSC
HYDERABAD SECURITY CLUSTER

mile2
IT SECURITY TRAINING & CONSULTING

group 2000

Templar Executives
Timely, Relevant and Valued Delivery

SERIOUS GAMING & EDUCATION

- Based on

- Research
- Table Top Gaming methodology
- Interactive group facilitation

- Examples

- Cyber Forensics & Investigation
- Cyber Warfare
- AI & AR
- Block Chain
- IOT Security

NSC Partners with Worlds Largest & Recognized Certification Body

NSA

Recognized Certification Courseware

Proprietary Accredited Cyber Security Certifications. diversified trainings and certifications based on the role and expertise of the trainee.

20+

Preferred **by FBI's (Federal Bureau of Investigations) Tier 1-3** certification training requirement

Mapped with NIST's (National Institute of Standards and Technology) cyber security workforce framework

150+

Accredited training partners across the globe. Thus ranking as the **World's largest** certification body for Information Security professionals

Has received 6 prestigious accreditations by CNSS(Committee on national security systems.). Refer **NSA-CNSS 4011-4016**

Approved on Dept of Homeland Security NICCS (National Initiative for Cyber Security Careers and Studies) Program

Courses specifically designed for elite organizations

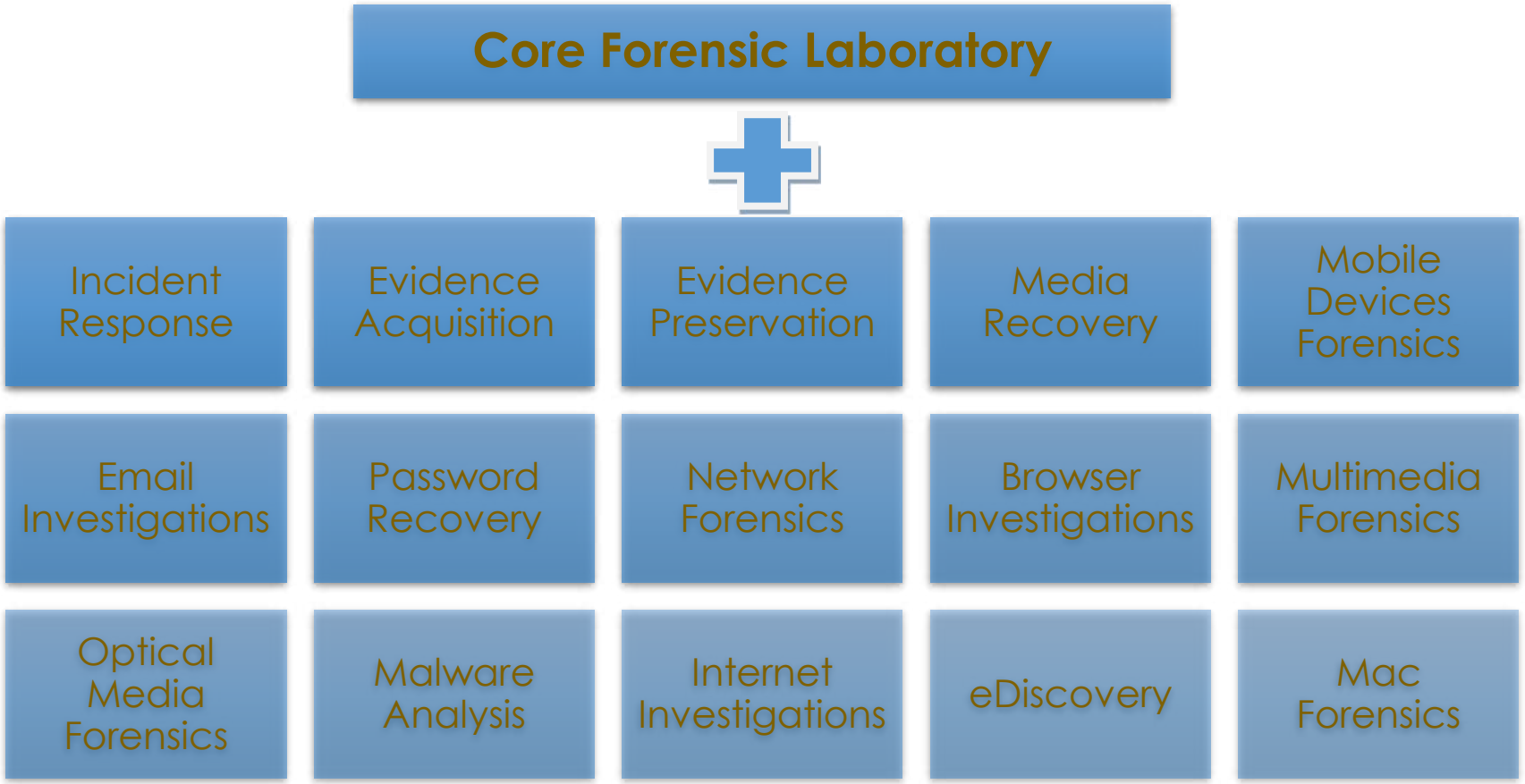
C)PTE
Certified Penetration Testing Engineer
United States Air Force

C)NFE
Certified Network Forensics Examiner
United States Counterintelligence Agency

C)ISSO
Certified Information Systems Security Officer
Canadian Department of National Defense

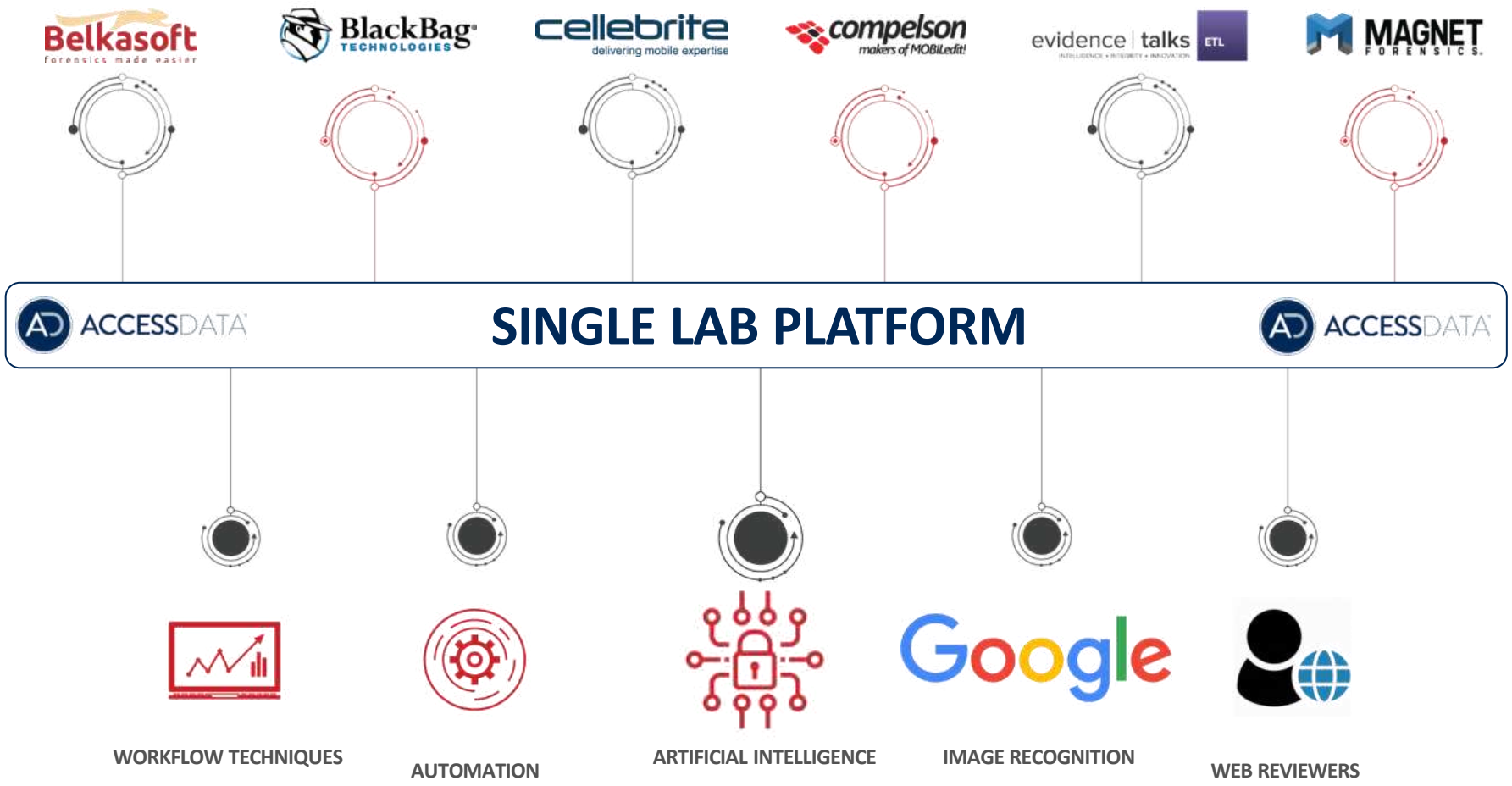
C)SWAE
Certified Secure Web Application Engineer
Boeing Aerospace

Lab Designs & Modules



Digital Forensics & Ediscovery - ACCESSDATA

AD LAB PLATFORM



Forensic Hardware - MH SERVICE GMBH

With more than 20 years' experience, mh-SERVICE is one of today's leading providers and suppliers of products and services related to IT, mobile phone and audio-visual forensics. Moreover, Europe's only forensics supplier with its own hardware development and manufacturing departments.

AntAnalyzer

Trecorder

Beecube

Rack Mount Server

Octagraph

Forensic Cube

Paldin/Forensic Laboratory

Experts in Setting up of LABS

Central Cyber Forensics Lab

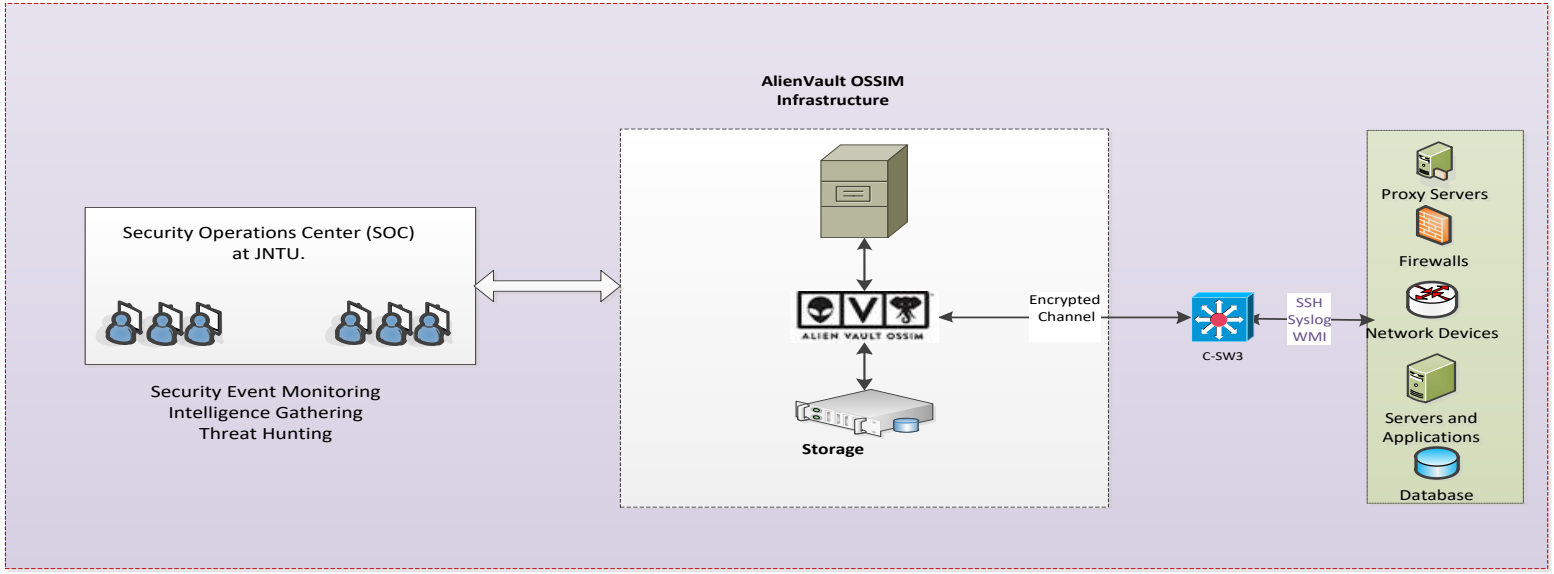
Centre of Excellence for Cyber – Forensics that will provide leadership, evangelization, best practices, research, support and/or training

Setting Vulnerability Research Lab

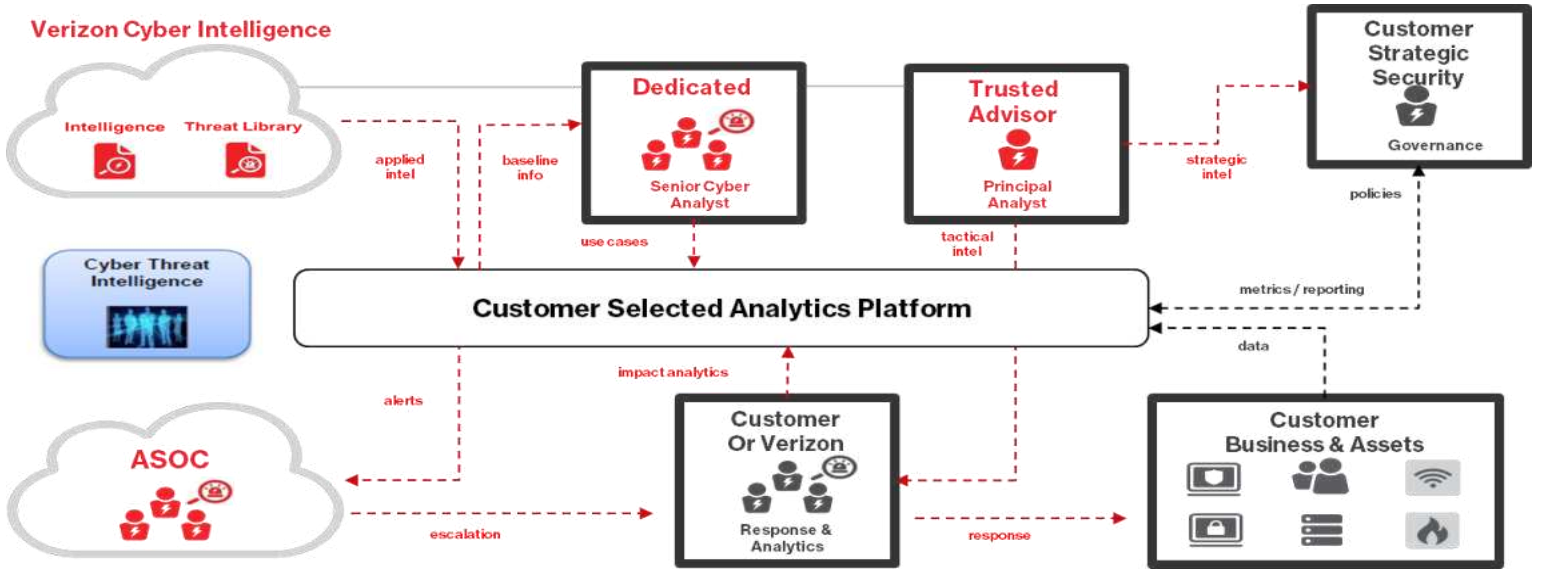
- External Network Vulnerability Assessment and Penetration Testing to identify security weaknesses
- Series of vulnerability assessment and manual techniques to identify and validate security vulnerabilities
- Our DIVER2 Methodology and testing as per this methodology is conducted in the following five phases

Setting Cyber Intelligence Center

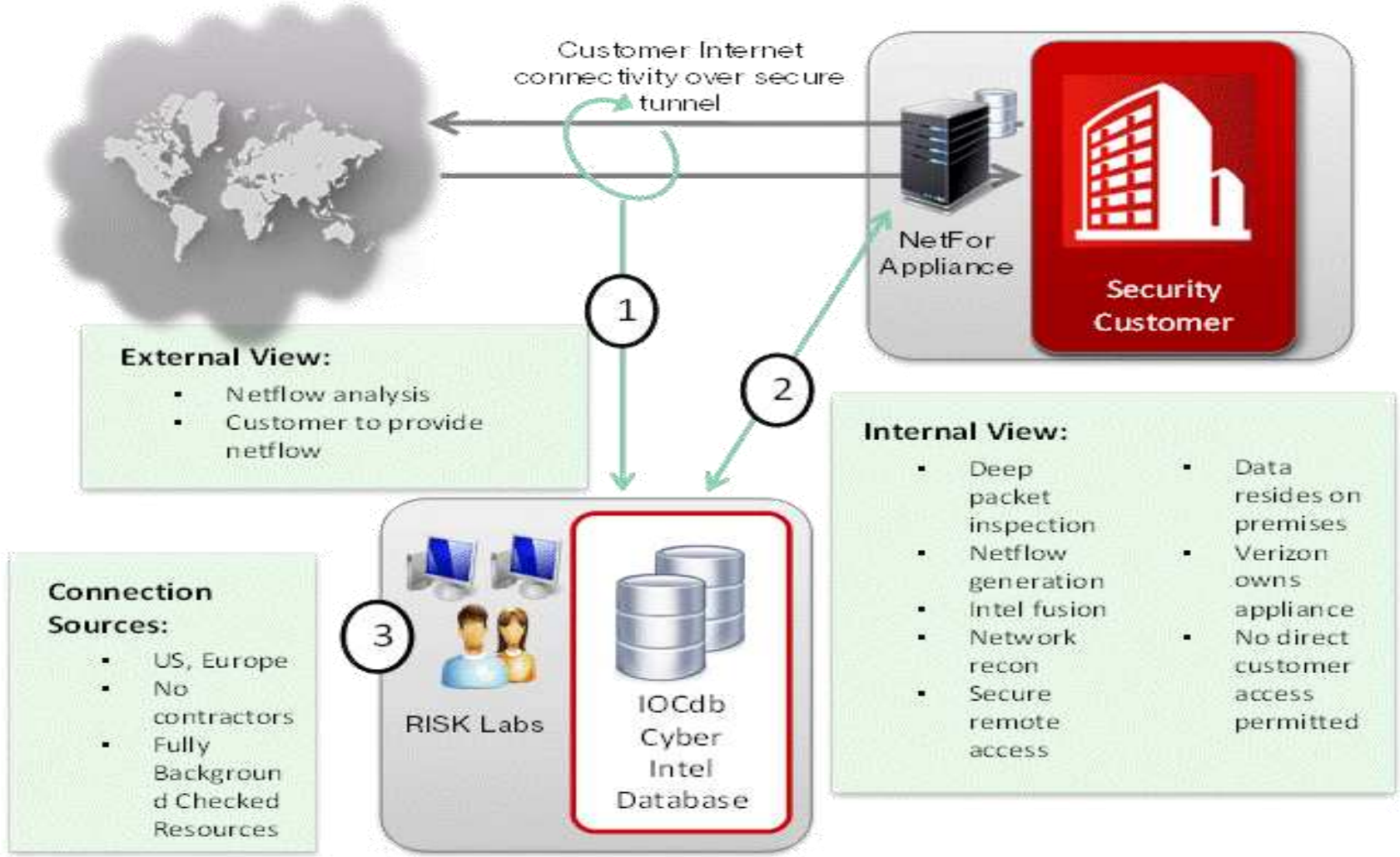
Architecture



Integrated Operational Model



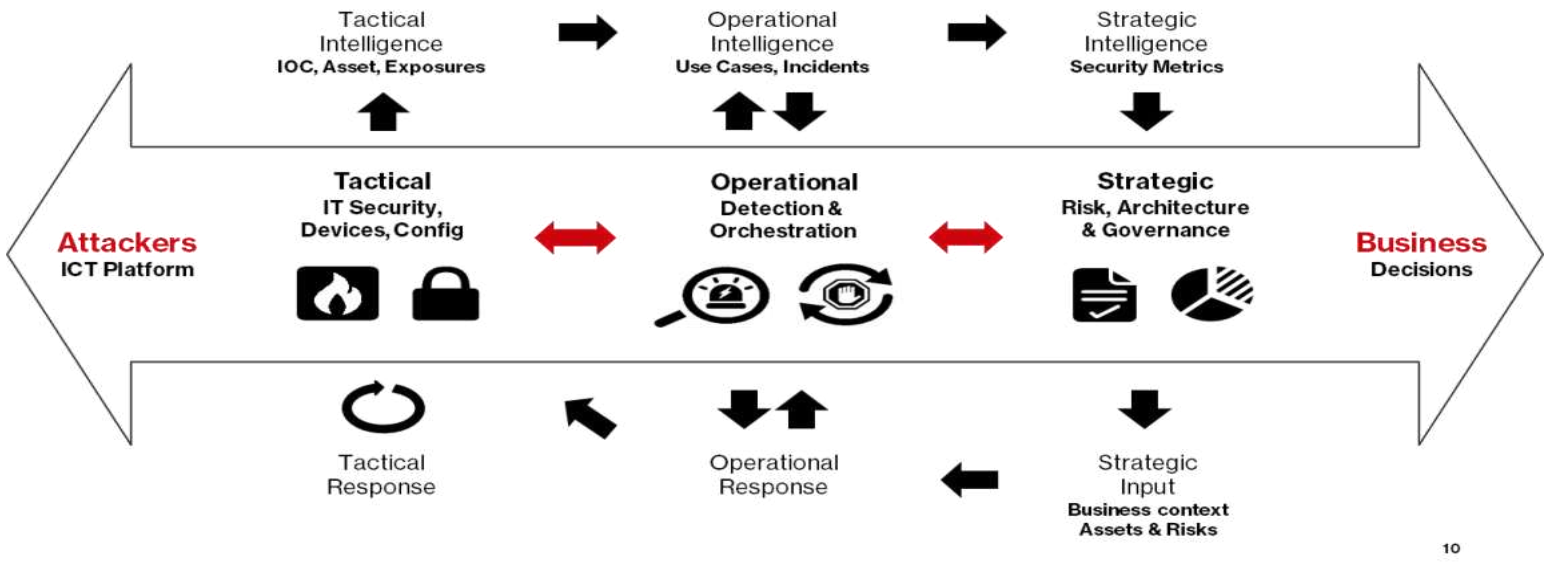
Setting Cyber Intelligence Capabilities



Setting Computer Emergency Response Team (CERT)

CERT delivers Incident Response Activities to react and respond to information security issues, such as:

- Provide a single point of contact aligned with customer's incident response team
- Identify security threats and analyze the impact to the customer organization
- Lead security incident response, damage control, remediation & recovery
- Provide incident research, threat mitigation, strategic planning and training
- Share experiences, information, lessons learned
- Security incident response capability assessment services / consulting
- Vulnerability management services



First Hague India Cyber Security Summer School

Our Consulting & Services

Below listed are the indicative list of services we render to clients specifically in cyber security domain,

Cyber Strategy & Governance	• Define the cyber strategy and roadmap based on the organization requirements • Support the organization with the various IT initiatives, design the governance including policies, procedures, roles & responsibilities, organization chart etc.
ISO-27001 / PCIDSS Assessment Certification Assistance	• Support organizations to build the ISO-27001 framework and roll out the various aspects within the organization. • Support with PCIDSS control assessment and implementation support. Assist the organization for the certification
Vulnerability Assessment & Penetration Testing	• Perform Vulnerability Assessment Penetration Testing of Applications, Servers, Databases, Network devices, Payment gateways etc. • Black box testing and Grey box testing (with credentials) Both Internal & External Assessments
Application Security Assessment	• Perform Application security control testing including access management, change management, incident management, security configurations etc. • Perform Application source code review and suggest improvement areas / vulnerabilities at the code level.
Compliance Reviews (SAMA & other regulatory compliances)	• Conduct SAMA compliance audits to banks, NBFC and other financial institutions on Cyber Security and other **SAMA** requirements. • Conduct other country specific compliance requirements to Banks (For eg. Middle east, Africa etc. as applicable)
Third Party Risk Assessment	• Perform third party / vendor risk assessments to the third parties of the client and arrive at the gaps and control improvement areas • Report the gaps, deviations from vendor agreements and share the recommendation
Technology / Security Solution Design & Implementation Support	• Design of solutions including IDAM, DLP, SIEM based on the client needs • Provide implementation support services including motoring and sustenance of the solution

How we can help to prepare your business

The legal landscape of data protection is evolving rapidly, and presenting challenges for businesses, government and public authorities. If your organisation is consumer-facing, online, in the financial services sector or in possession of sensitive personal data it may be particularly affected.

With the deadline growing closer, you'll need to scrutinise the regulatory changes and understand how they will affect your business operations. Bear in mind that the impact of GDPR isn't confined to a specific area of your business – it will require business-wide adoption of a more process- orientated approach.

It's likely you'll need to amend your business practices to become compliant with this new regulation, and implement new controls. So where should you start? We've created a simple visual, below, to help structure your approach to achieve compliance.

E2Labs can understand your needs and can support you in the following:

GDPR

Understand the key changes this legislation will bring

Data protection quick check

Assess your organisation's current data architecture, processes, and risk and compliance controls

Audit results and analysis

- Identify the current data risks in your business
- Review how ready your business is for the GDPR

Implementation roadmap

- Develop an implementation roadmap that embeds suitable regulatory and compliance architecture
- Ensure the plan is realistic and achievable for your organisation

Implementation

- Appoint a trusted advisor to:
  - identify and document data processing activities
  - carry out data impact assessments
  - develop a data breach response action plan
  - implement ongoing data protection processes.
  - Write a detailed data protection policy and define a standard that ensures your business will meet the GDPR
- Where necessary, appoint a data
- Protection officer/ or a data protection management control for ongoing control

Measure data protection effectiveness

- Undertake a GDPR FIT/ GAP analysis or ISO 27001- this is an effectiveness test for your GDPR efforts

Continuous improvement

- Hold regular GDPR audits and Data Privacy Impact Assessments
- Ensure data risk management is integrated into your overall risk management structure
- Regularly review your organisation's data protection training methods

Have you started your General Data Protection Regulation (GDPR) journey?

What questions should you ask yourself to prepare your business for the GDPR?

1 Where are you now?

GDPR Quick Check

Identify your current status using our GDPR Quick Check tool. This will help you to identify the initial areas of focus.

2 Do you have a data protection people resource?

Appointing DPOs and data protection organization

You may need a designated data protection officer (DPO). If you don't have one already, you might need additional resource to coordinate all data protection processes and

3 Do you have business processes that protect the rights of the individuals for whom you hold data?

Enhanced rights for individuals

For most companies, the requirements of the GDPR will lead to major changes, such as new business processes and measures in many areas of the IT and process landscape. measures. Documented business processes are helpful to integrate data protection aspects, such as the rights of the data subjects.

4 Have you documented your data protection processes?

Implementation

For effective and efficient management of data protection you must create a set of actions that includes the necessary policies and procedures.

5 Do you know where you process personal data?

Increased record keeping

Your data protection officer should maintain a record of processing activities (RPA) under his responsibility and make those records available to the supervisory authority on request.

6 Do you know how to conduct a data protection impact assessment?

DPIA

Where a processing activity poses high risk, a data protection impact assessment (DPIA) is required.

7 Do you know how to report a data breach?

Stricter breach reporting

Your data protection officer has to notify the supervisory authority no later than 72 hours after a personal data breach under certain conditions. When the breach is likely to result in a high risk, the date subject must be notified immediately.

8 Are you measuring the effectiveness of existing data security and data protection processes?

Test, check and evaluate

The GDPR requires a process for regularly evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

9 Have you considered implementing a data protection management system (DPMS)?

Data protection management system

The GDPR not only asks you to assess and implement your data protection measures but also to continually improve them. A DPMS will help you to monitor and govern the GDPR measures through your organisation.

10 Do you have an effective data protection awareness and training programme?

Awareness programme

An effective data protection awareness and training programme is essential to make sure employees follow your defined guidelines and prevent data breaches.

We can help

Our global network of GDPR specialists can help you to assess, design, implement and monitor any new data protection process you need to comply with the GDPR. Our global methodology means you will receive consistent advice, tailored to you throughout your GDPR journey.

Fast track with E2LABS

Don't start from scratch, we can help guide you through with the our **GDPR toolkit** covering:

- Quick check
- Control assessment
- Data protection processes
- Record of processing activities
- Data protection impact assessment methodology
- Data protection blueprint

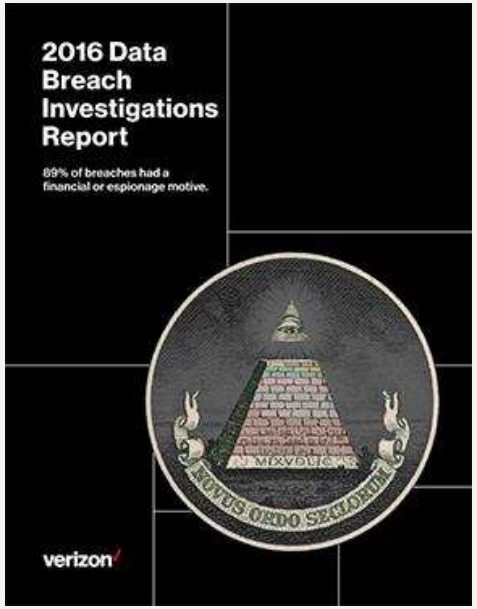
MANAGED SECURITY SERVICES

verizon

GARTNER'S MAGIC QUADRANT

2015 Gartner Magic Quadrant for Managed Security Services, Worldwide.

Verizon is the backbone for 78% of the world's internet.



Verizon mints Cybersecurity's most comprehensive investigations report annually.

FORTUNE 100

Verizon Ranks #13 as fortune 100 global companies bagging a revenue of more than 130 billion USD. And being the leading telecom and info security provider.

ICSA labs
An Independent Division of Verizon Business

ICSA Labs, an independent division of Verizon, has been providing credible, independent, third-party product assurance for end-users and enterprises since 1989.

terremark®

Terremark is one of the leading service providers for *managed hosting, colocation, disaster recovery, data storage, and cloud computing.*

Fast Facts

Verizon is a global leader delivering innovative information and communications technology solutions that improve the way our customers live, work, and play.

VERIZON

- **Fortune 500 Rank:** #16
- **2013 Capital Investment:** $16.6B
- **2013 Revenues:** $120.6B
- **Global Employees:** Over 177,800
- **Connected Fleet:** Over 32,000
- **Foundation:** $14M+ matched funds
- **Verizon Credo:** Ethics and culture

VERIZON ENTERPRISE SOLUTIONS

Wireless

- 100% wholly owned business with 104.6M connections
- 4G LTE network covering 97% of U.S. population
- Over 2K company-owned stores and 12K agents

Business

- Serving 97% of the Fortune 1000
- Global workforce serving over 150 countries
- Global solutions for Cloud, M2M & Cyber Security
- Mobility solutions for a work and life balance

FiOS

- 100% fiber-optic network with speeds up to 500 Mbps
- 6.1M FiOS Internet and 5.3M video customers
- Ongoing IT transformation with fiber replacement of copper

Verizon is a leader in the following analyst reports:

Gartner

Magic Quadrant Reports:

- Global Network Service Providers
- Global MSSPs
- Cloud-Enabled Managed Hosting, Europe

IDC
Analyze the Future

MarketScape Reports:

- Worldwide Managed Security Services
- Global Telecommunication Services

FORRESTER

Forrester WAVE reports:

- Managed Global MPLS Services
- Global BYOD Management Services

Current Analysis

Verizon receives a "Very Strong" rating for:

- Managed Security Services
- Global M2M Services
- Global Managed Mobility Services
- Global Data WAN Market
- Global Enterprise Collaboration and Communication Services

Rapid Response Retainer Services

Act fast when seconds count !!!

Emergencies

- Incident response
- Digital forensics
- IT investigations
- Malcode analysis
- E-discovery consulting
- Electronic data recovery and destruction
- Litigation support

Non-emergencies

- Dark Web Research
- Breach simulations
- IR capabilities assessment
- Security health checks
- IR plan review
- Network penetration testing
- Computer incident response training
- Payment card industry consulting

verizon

E2LABS
Consulting•Investigation•Academy

Rapid Response Retainer

ACT NOW & subscribe to Rapid Response Retainer

LAWFUL INTERCEPTION & SURVEILLANCE SOLUTIONS

GOVERNMENTS

TELECOM PROVIDERS

LAW ENFORCEMENT

INTERNET PROVIDERS

20+ years of global experience in the public, telecommunication domain and delivering Lawful interception solutions.

Group 2000 is a Leading provider of Lawful Intercept and surveillance Solutions in Europe

ETSI World Class Standards

Full time active member if ***European Telecom Standard Institute (ETSI)***.

LIMA solutions are modular and scalable to support the largest networks.

Lima®

Our people and technology help you to enable safer societies and protect mission critical, IT and telecommunication infrastructures.

WHAT WE ARE LOOKING FOR ?

The world has woken up to the looming threats of cyber attacks, Warfare & Cyber Terrorism.
Budgetary allocations Globally have risen to Billions of $.

We seek to align with capable & like minded partners to commence this lucrative & immediate Journey for assured Gigantic Success.


It's time to
END CYBER RISK