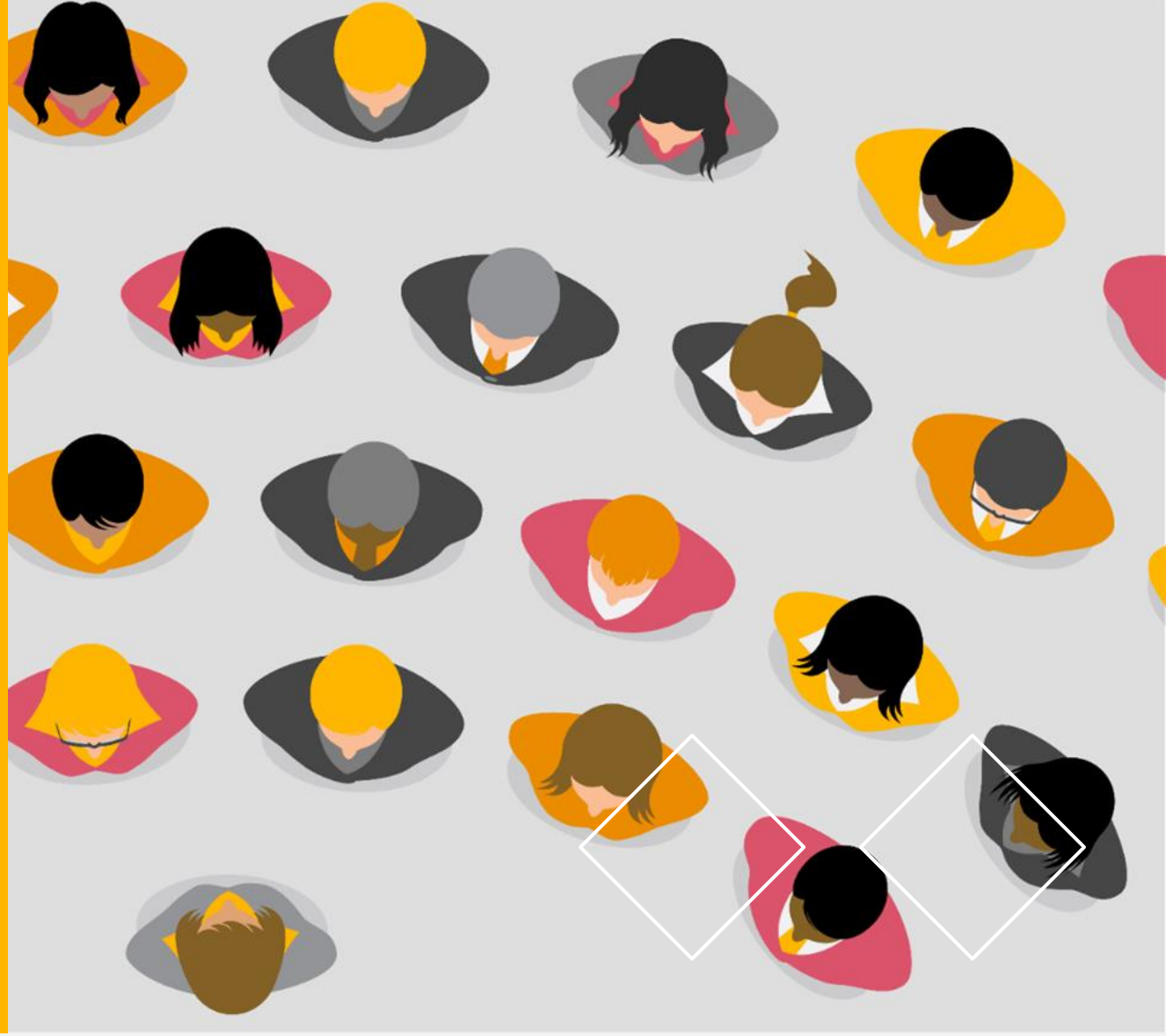
# PwC India Cyber Security

## Practice Profile



pwc

# Our Practice Overview

# Over 1250 dedicated cyber practitioners

**Resources**

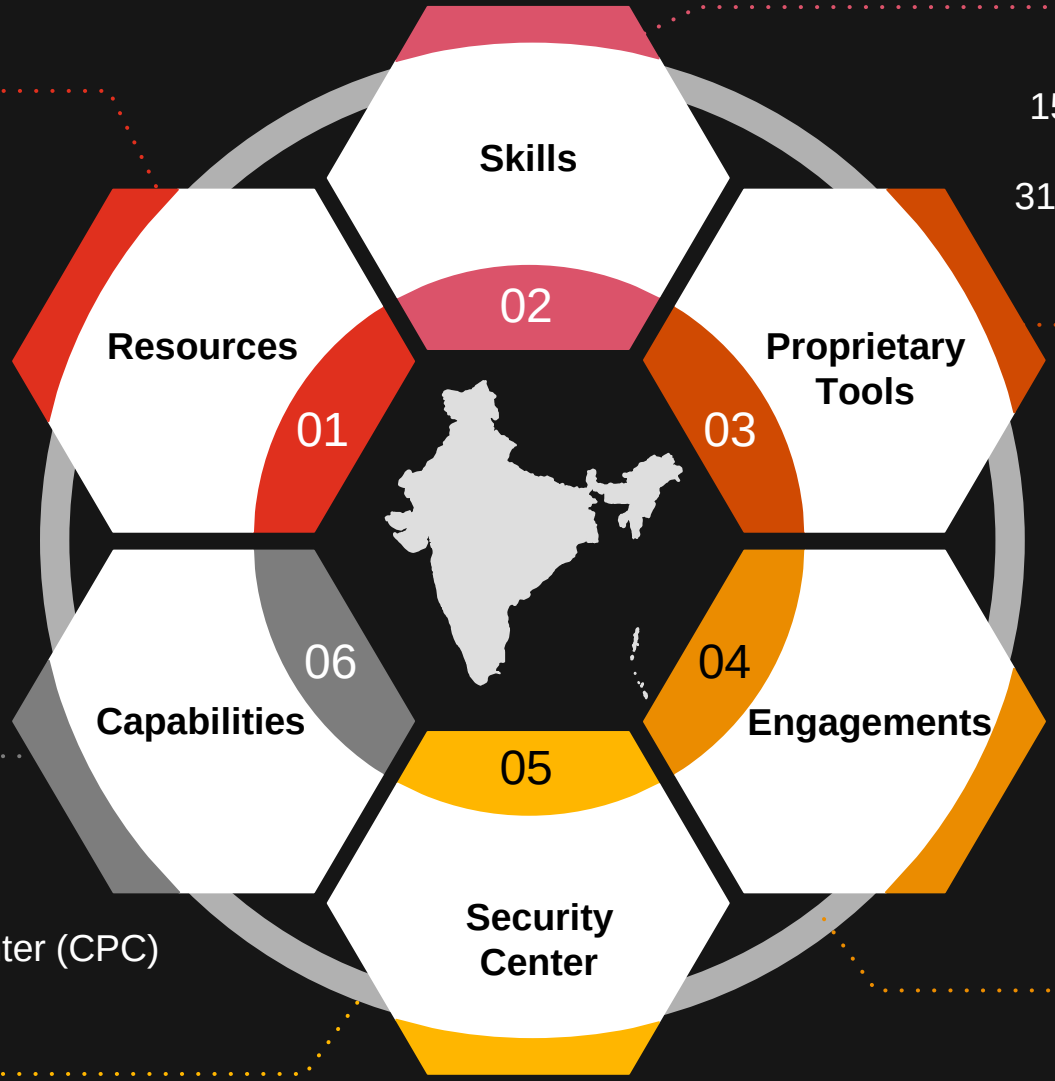
1250+ professionally trained resource pool

**Capabilities**

Dedicated Cyber Security Lab for Research, Development and Testing

**Security Center**

200+ seater SOC Cyber Protection Center (CPC)




**Skills**

1500+ certifications - OSCP, CEH, CISA, CISSP, ISO 27001, ISO 22301, ISO 31000, CISM, DSCI, PCI-DSS, and many more…

**Proprietary Tools**

06 proprietary Cyber tools incubated and developed

**Engagements**

584+ current active projects across geographies

# Driving cyber agenda through strategy to execution

At PwC, we leverage our global experience and knowledge of technology, as well as threat actors, to help our clients prepare for attacks while developing strategies and tactics to increase resilience and mitigate negative impacts.

### Strategy & Governance

Align with business, prioritize investments and align security capabilities to navigate cyber security risks & compliance requirements leveraging robust strategy & governance frameworks.

### Cloud Security

Integrate cloud governance, security and compliance into your transformation. Build confidence in your cloud journey across the enterprise.

### Identity and Access Management

Ability to manage the lifecycle of digital identities and enable them to perform business activities efficiently in a secure ecosystem with the ability to protect enterprise assets, speed up go to market, minimize misuse of access and provide business insights into access patterns and effectiveness of policies

### Data Privacy & Protection

Know your data, the handlers of data, protect exfiltration and mitigate penalties by complying to geographical, sectoral, business and regulatory mandates.

### OT Security

Embedding security controls into the design fabric of heterogeneous environment for  IoT, OT/SCADA/ICS, IIoT.

### Threat & Vulnerability Management

Manage digital infrastructure attack surface, by identifying gaps, exploiting design flaws and assisting you in remedial actions to secure your ecosystem.

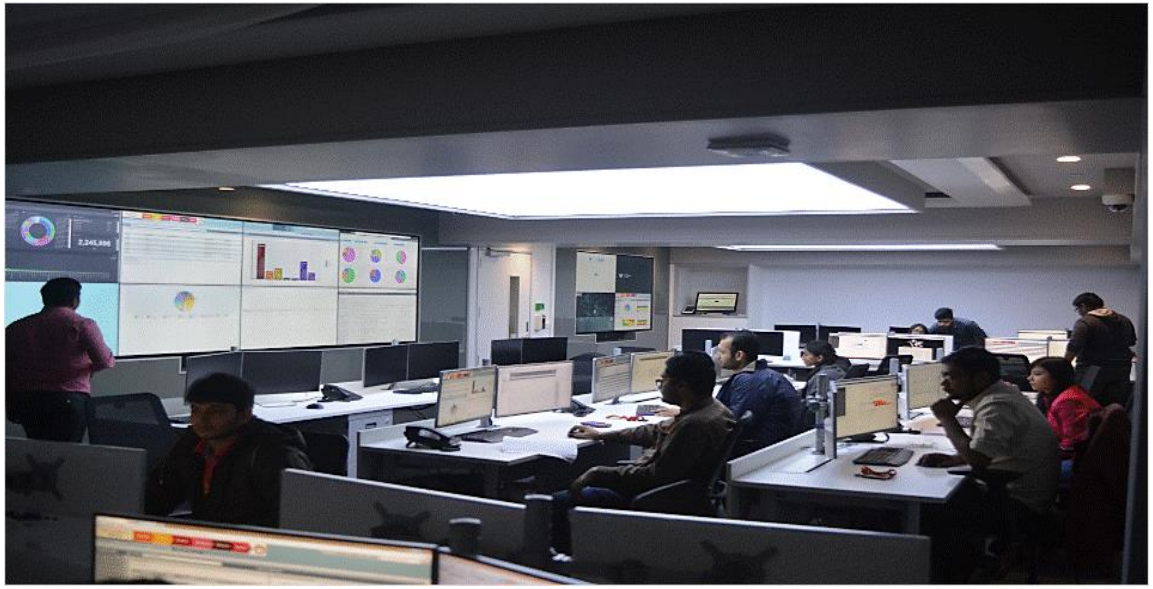
### Managed Security Services

Ability to detect, manage and respond to security incidents by leveraging our 24x7x365 Cyber Protection Centre (CPC) and active Threat monitoring services, Endpoint Detection Response, etc.

### Incident Response & Breach Investigation

Identify the root cause, nature, means and source of an incident to support as evidence for any legal action & support, through our forensic services breach.

# Cyber Protection Center (CPC)



## Services offered

**Standard**

- ✓ Security operations
- ✓ Incident management
- ✓ Threat detection
- ✓ Containment
- ✓ Attack surface management

**Advanced**

- ✓ Threat intelligence
- ✓ Analytics
- ✓ Compromise assessment
- ✓ Malware analysis
- ✓ Forensics & Counter-measures

Our State-of-the-art Cyber Protection Center (CPC) has **200+ Seater facility equipped with video walls for eyes-on-glass monitoring**.

**Confidence in your cyber resiliency**

- **On-demand** security orchestration with S.O.A.R capabilities
- **Real-time** correlation and security analytics engine
- **24 x 7 x 365 days** operations capability
- **Threat intelligence** & collaboration
- **ISO 27001** certified best-in-class center
- **Malware** reverse engineering

# Our key strategic alliances

**Palo Alto Networks**
Offers enterprise cybersecurity platform which provides network security, cloud security, endpoint protection, and various cloud-delivered security services.

**Microsoft**
Microsoft Services provides a comprehensive approach to security, identity, and cybersecurity. They include an array of Security and Identity services across strategy, planning, implementation, and ongoing support.

**Google**
Leading CSP with offerings such as threat briefings, preparedness drills, incident support, and rapid response engagements in order to keep your organization on top of the latest developments in the security landscape.

**SailPoint**
Leading identity management solution that helps organizations manage employee permissions, digital identities, information security, data access, and compliance.

**ForgeRock**
Identity governance and administration solution that can be implemented across an organization, and offers feature parity across all delivery options, including on-premise, any cloud environment, multi-cloud, hybrid, and as a service.

**Micro Focus**
Digital transformation services that addresses cyber resiliency and requires integration of cybersecurity throughout the enterprise lifecycle – to protect the business, detect changes in the risk surface, and evolve capabilities.

# Our Global Managed Delivery Center

Our Global Managed Delivery Center, in Kolkata (India) is the center for excellence for remote delivery of services across multiple domains.

## Methodologies

OWASP Top 10, SANS Top 25, CIS Benchmarks, Black box, Grey Box and White Box testing for Threat and Vulnerability assessment (including manual & automated testing). Frameworks & standards like ISO 27001:2013, ISO 22301, COBIT, HIPAA, NIST, GDPR  etc.

## Certifications

CEH, ECSA, CWASE, ISO 27001 LA, CISSP, CISA, ITIL, CISM, Six Sigma, CHFI, MCP, MCITP,CCNA, CCNP,CCSE, PRINCE2,Sailpoint IIQ Engineer, Okta Professional/Consultant, CCDE Certifications

## Technologies/ Tools

PwC proprietary SOC solution, and tools like Nessus, Burp suite, Qualys-Guard, HP-Web Inspect, Veracode, HP Fortify, Fuzz API, pURL, Acunetix, ZAP Proxy, dex2jar, appuse VM, Android SDK, Checkmarx, IBMAppScanMetasploit, Nmap / Zenmap, SQL Ping, Kali, Wireshark, Air Crack NG etc.

### Risk & Compliance

- Third Party Assurance and Supplier Assessment
- IT General Controls Review
- General Data Protection Regulation (GDPR)
- IRDA Regulatory Assessment
- IT Security/Compliance Audits
- ISO 27001 : 2013 (Information Security)
- ISO 22301

### Threat & Vulnerability Management

- Web Application Security Assessment
- Network Assessment & Penetration Testing
- API Security Assessment
- Secure Code Review
- Mobile Security Assessment
- Secure Configuration Review

### Identity and Access Management

- Strategy and architecture
- Design & implementation services across various IAM solutions
- Managed services to sustain an Identity implementation
- User Access reviews

### Key attributes

- Successful in ramping up the team at short notice.
- Ability to support global clients due to integrated delivery capabilities

# Key Client Illustration

# Our success stories (1/4)

**Threat Vulnerability Management – Telecom Service Provider**

**Requirement:** Threat and vulnerability management, integration of threat intelligence feeds

**Key outcomes:**
→ >24 months of testing efforts
→ 1000 servers
→ 750 applications tested
→ 6 platforms of testing performed


**Threat Vulnerability Management – Public Sector Bank**

**Requirement:** Threat and vulnerability assessment, source code review, vulnerability assessment, security design & technology engineering

**Key outcomes:**
→ 60+ application penetration testing
→ 1000+ Vulnerabilities Remediation Advisory
→ >10 million lines of code review

**Security Design & Technology Engineering – National ID Program**

**Requirement:** End to end security infrastructure, compliance audits, setup of fraud, forensics & security governance

**Key outcomes:**
→ 500+ ecosystem partner audit
→ 10+ Technology Security Implementation
→ 14+ partner SLA measurement

# Our success stories (2/4)

**Security Design & Technology Engineering, Emerging Technologies**
**– Oil & Gas Producer**

**Requirement:** Assessment and study of integration between security devices in the environment

**Key outcomes:**
→ Security Architecture review
→ ICS review
→ Data Centre Security
→ Physical Security Assessment

**Manage Detection Response**
**- German Automobile Manufacturer**

**Requirement:** Design and implementation of cyber centers for global operations

**Key outcomes:**
→ Construction of Cyber Control Rooms
→ Cyber Centre
→ Strategic Assessment of Technology

**Identity & Access Management and Strategy & Governance**
**– Asia Pacific Bank**

**Requirement:** Design & Implementation of IDAM, PIM & Archer GRC, IT risk assessments

**Key outcomes:**
→ 80000+ user identities managed
→ GRC Implementations for the Bank
→ 680+Applications for support
→ 21000+ Privilege Identities

# Our success stories (3/4)

**Strategy & Governance – American Wealth Management Companies**

**Requirement:** Risk Assessments based on NIST and global regulatory controls for applications, ISO implementation, certification & sustenance support

**Key outcomes:**
→ Security Assessments for 260+ apps
→ 8000+ controls Assessed
→ 150+ Risk Identified, Implementation across 10 locations in India & USA

**Strategy & Governance - Consumer Goods Giant**

**Requirement:** Assessment of Crown Jewel, assessment & implementation of CyberArk.

**Key outcomes:**
→ Next Gen. SoC Strategy & Roadmap
→ Integration of RBAC
→ VMS capability under a uniform vulnerability scanning

**Data Privacy & Protection, Strategy & Governance & Manage Detection & Response – Pharma Company**

**Requirement:** Assessment of data privacy regulations

**Key outcomes:**
→ Conducted EU-GDPR and vulnerability assessments
→ Establish Information Security governance framework
→ SIEM integration with devices

# Our success stories (4/4)


**Manage Detection Response – Indian Multinational Conglomerate**

**Requirement:** SIEM implementation and process definition

**Key outcomes:**
→ Use case library for SIEM
→ Scope data collection sources
→ Configure log sources
→ Define operational processes
→ Establish benchmark criteria

**Cyber Forensics – Co-operative Bank in India**

**Requirement:** Forensic investigation and analysis

**Key outcomes:**
→ Malware Analysis and investigation
→ Data theft analysis

# Thank you

pwc.in