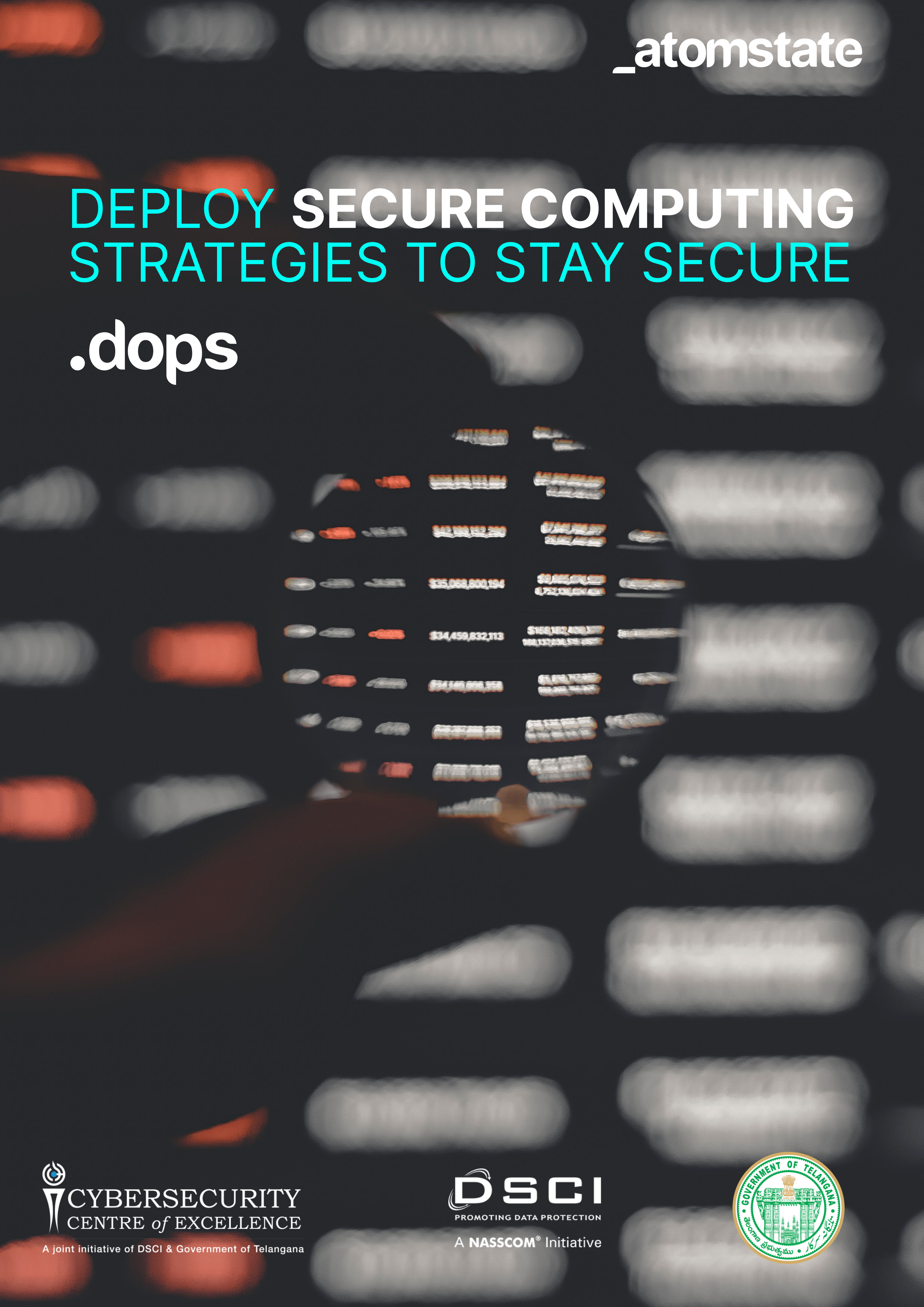
_atomstate

DEPLOY SECURE COMPUTING STRATEGIES TO STAY SECURE

.dops



CYBERSECURITY CENTRE *of* EXCELLENCE
A joint initiative of DSCI & Government of Telangana

DSCI
PROMOTING DATA PROTECTION
A **NASSCOM**® Initiative

GOVERNMENT OF TELANGANA

Cover Image Attribution

Sajad Nori/Unsplash

Contents

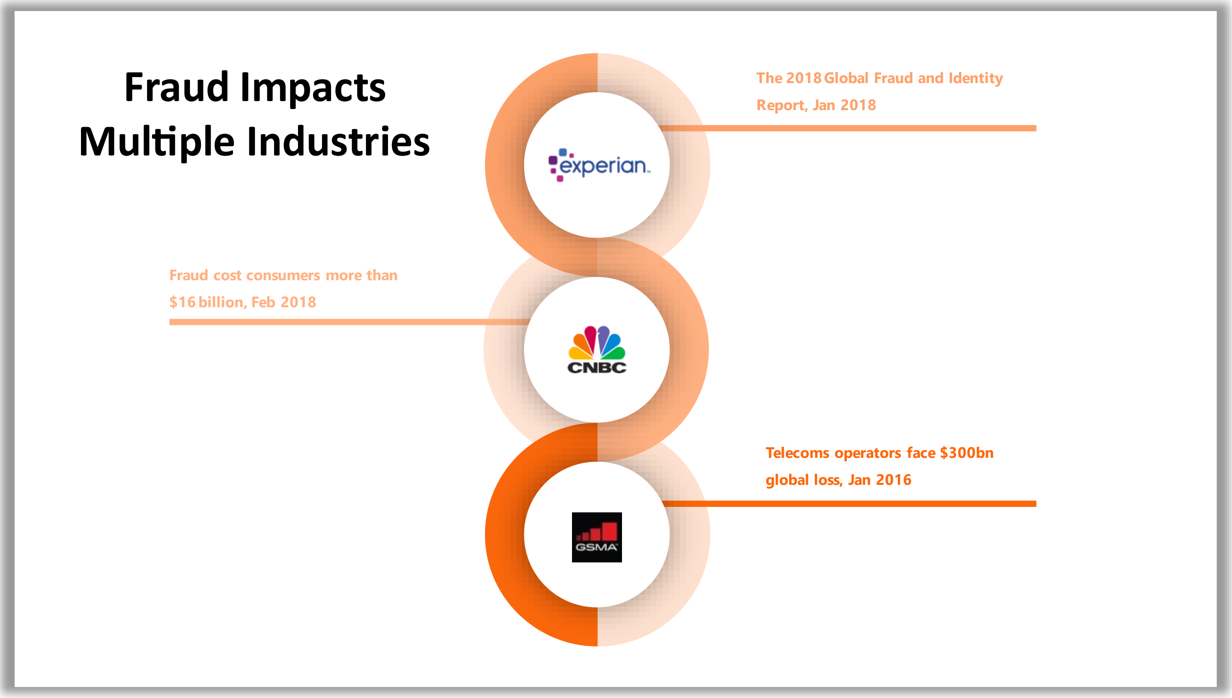
Table of Figures

Page intentionally left blank

Introduction

In the current digital landscape, safeguarding data is critical for businesses since it has become a valuable asset. To protect against cybercrime, fraud, and hacking, secure computing is a fundamental aspect of a cybersecurity strategy. The internet is a powerful tool, but it also poses a risk, and these threats have become more advanced, resulting in substantial financial losses across all industries. As a result, a comprehensive approach is required to detect and prevent such fraudulent attacks.

Refer below image highlighting the losses reported due to fraudulent instances and cybercrimes in telecom sector alone. The sector suffers an yearly loss to the tune of ~USD 6 Billion on an average.



Fraud Impacts Multiple Industries

The 2018 Global Fraud and Identity Report, Jan 2018

Fraud cost consumers more than $16 billion, Feb 2018

Telecoms operators face $300bn global loss, Jan 2016

Figure 1 Telecom Industry Loss due to Cyber Frauds

How do we counter and protect? The best way to counter and protect against cyber threats is by implementing a real-time, multi-layered security solution that uses advanced technology, such as Artificial Intelligence. Rule-based solutions are no longer effective against the sophisticated methods used by fraudsters. It is important to understand the aspects of secure computing and the cybersecurity threats, how to mitigate them, and how to respond if attacked.

Information Security Overview

Information Security (IS) is crucial for any organization to protect sensitive data, but many organizations are still vulnerable to cyber-attacks. These threats are constantly evolving and can be costly, with an average breach costing over $4.82 million[1]. This white paper provides information on specific threats to organizations, how to mitigate them, and what to do if attacked.

Cyber-attacks are often caused by management's lack of will, ignorance of the impact, or the assumption that they are a one-off occurrence. Despite the cost, many organizations neglect robust security measures and fail to gauge the intensity and sources of potential attacks. To address this, management should consider implementing secure measures such as clear guidelines, continuous monitoring, employee awareness, risk management strategies, and vendor vetting. Adequate budget and investment in cybersecurity tools and resources are also critical to an organization's success in risk management.

The factors and Suspects

The article highlights various threats that can impact an organization, such as malicious software, spyware, insiders, and outsiders. It emphasizes the importance of assessing these threats and implementing effective measures to counter them. The article suggests including legal clauses in appointment letters or third-party agreements and having a strong automated backup system to minimize the impact of threats.

Important factors for cyber security

The figure below highlights the critical factors of Cyber Security. Assessing the maturity levels and identifying gaps is crucial in understanding past attacks and internal or external factors that contributed to them. To establish a secure environment, a strong plan is needed to detect and protect, with prevention measures and an action plan in place.

Teams should be trained to manage any situation that arises. Additionally, a response mechanism and periodic internal security audits by third-party experts are important. Technology is also crucial, and investing in the best tools and resources is necessary as data is the backbone of any business. Although this may be expensive, it is worth the cost.

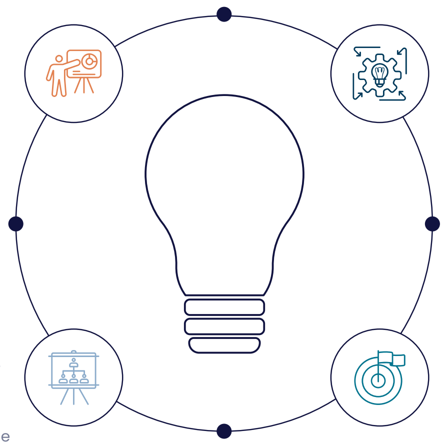
Pivotal factors of Cyber Security

Assessment

An honest assessment on as-is-scenario, past attacks, identify gaps resulting in attacks, and develop a robust blueprint to combat threats. A reference architecture, infrastructure model, and employee training & enablement model can help establish good cyber governance and identify threats and vulnerabilities quickly.
.

Response Mechanism

Response mechanism to combat cyber threats should be in place. A response manual should be regularly updated, and stakeholders should be aware of the relevant agencies and law enforcement to notify incidents..



Planning & Prevention

Cyber governance plan identifying and detecting digital crimes, instituting an alert state, and mitigating risks. covering all the gates and edges and protect the network and data layer,Mock sessions to cascade awareness to stakeholders and evaluate risks, which is essential as data tends to be the heart and soul of any organization.

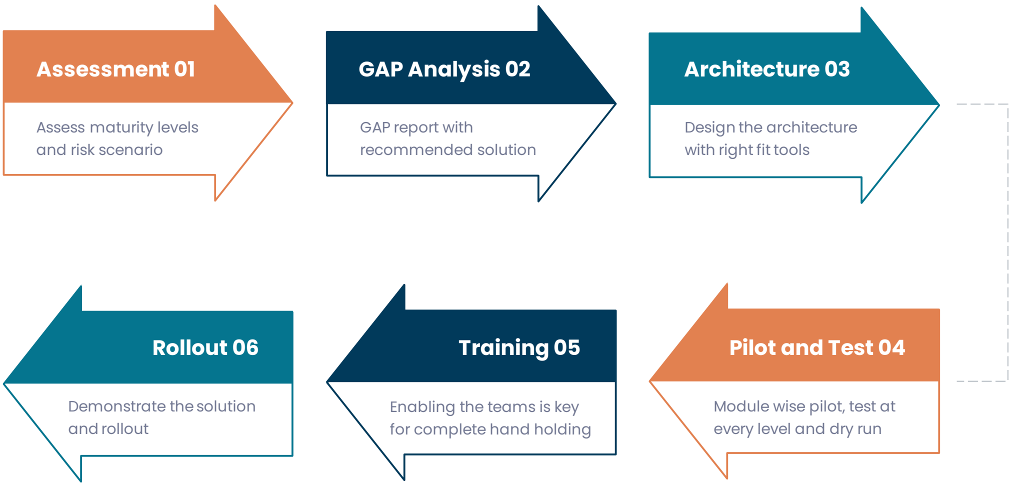
Technology

Constant Monitoring and protection with well-vetted & validated firewalls, network access controls,email filtering systems, cloud applications, endpoint management, backup and disaster management solution to be in place.

Figure 2 Pivotal factors of cybersecurity

Recommended Flow

Recommended Flow



Assessment 01
Assess maturity levels and risk scenario

GAP Analysis 02
GAP report with recommended solution

Architecture 03
Design the architecture with right fit tools

Pilot and Test 04
Module wise pilot, test at every level and dry run

Training 05
Enabling the teams is key for complete hand holding

Rollout 06
Demonstrate the solution and rollout

Figure 3 Our recommended cybersecurity implementation flow

Cyber Security Assessment- Maturity levels (policies, guidelines, tooling, sacrifices, threat detection & management, prevention methods, alert management etc)

- Threat assessment & mapping.
- Security policies and guidelines.
- Assets integrated with the system.
- Number and types of end points integrated.
- Access Management.

GAP Analysis Report

- List the gaps.
- Security lapses.
- Regulatory compliances.
- Vulnerability patterns.
- Recommendations.

Blueprint the E2E 360 Cyber Security Solution

- Framework covering SIEM, UEBA & SOA
- Framework designing with important 4 factors.
  - Existing protective systems.
  - Compliance with security regulations.
  - Vulnerability to security incidents.
  - Resilience against potential harm.

Pilot & Rollout

The next step is pilot, rollout, training and handing over.

Assessment Goals

- Close vulnerability gaps
- Remediate weaknesses.
- Prioritizing issues with the highest potential for bottom-line impact.
- Improve communication with top management.
- Security policies integration with the operations
- Bring all stakeholders under one roof.
- Effective monitoring
- Assessment to include below to achieve the goals.
- The nature and value of the company’s cyber assets
- The origin of potential threats
- The vulnerabilities that could allow cyber threats to materialize.
- The likelihood of harm
- The risk or possible impact on operations and assets

- Level of compliance with privacy and security regulation

Assessment Steps

Define Existing Security Posture

The security posture of an organization is a crucial part of its cybersecurity framework, encompassing hardware, software, policies, and processes that govern data movement across the network. It involves.

- Taking inventory of protection measures in the tech stack,
- Documenting procedures to mitigate risks, and
- Creating formal protocols if they don't exist.

Review Compliance Requirements

It's important to comply with at least one cybersecurity regulation that suits the organization, and assembling a complete list of regulations is necessary to close any knowledge gaps. To ensure cybersecurity compliance, organizations should

- Assess the maturity of their existing security controls,
- Develop a risk mitigation roadmap, and
- Ensure that compliance software is in place.

Assess the Maturity of Existing Security Controls

The security strategy's effectiveness is based on the company's goals and industry norms. The following steps can help define and evaluate the security strategy:

- Defining the risk profile and setting acceptable risk targets,
- Evaluating security maturity against those targets, and
- Measuring any gap between controls and risks

Develop a Risk Mitigation Roadmap.

To close the gaps between security posture and risk targets, an organization must

- Develop a strategy which includes prioritizing action steps and allocating resources properly.
- It's important to value each asset and have a reporting mechanism in place to provide recommendations to decision-makers based on organizational priorities.

Cyber Security Assessment Practices

Assessment of Cyber Infrastructure Effectiveness

To ensure the effectiveness of an organization's security controls, it is important

- To conduct a complete inventory check and evaluation of these controls.
- Penetration testing is recommended to evaluate an organization's security posture and assess its resilience against cyberattacks.
    - It documents attempts to breach defences and tests the speed and effectiveness of response and recovery in the event of an attack.

Assessment of Operational Resilience

- Operational resilience aimed at the below.
    - Prevent disruptions from happening.
    - Quickly respond to and recover from a disruption in business processes.

To test operational resilience, an organization must

- Evaluate its ability to adapt management approach and strategy based on prior threats,
- Prepare for potential threats,
- Monitor critical functions of at-risk systems,
- Withstand cyber assaults while maintaining normal operations, and
- Recover operations and restore tech infrastructures after an assault.

This type of assessment tests the responses of an organization's IT assets and systems, not just its cybersecurity practices or security posture.

Assessment of Management of External Dependencies

To effectively manage external dependencies, organizations must evaluate and guard against the risks posed by each relationship. This involves assessing

- How well the company manages these relationships and having a strategy in place for external dependencies.
- It also involves identifying and mitigating risks related to each dependency, implementing relationship management systems to stay informed about risks, and having a plan in place to maintain continuity if a threat materializes.

This is a complex and multifaceted process that requires involvement from stakeholders across all departments.

Assessment of Risks and Vulnerabilities

This method focuses on identifying the areas of an ecosystem that are most vulnerable to attack, including human assets and systems.

It can help determine the susceptibility of systems to social engineering tactics used by hackers to gain access to critical data.

Penetration testing is useful in evaluating the effectiveness of cybersecurity practices and response strategies to potential threats.

By identifying the weaknesses in the security controls, this testing method provides insights on where to improve and strengthen the security posture.

Benefits of Risk & Security Assessment

- Recognise and control hazards in your workplace.
- Create awareness among your employees and use it as a training tool as well.
- Set risk management standards, based on acceptable safe practices and legal requirements.
- Reduce incidents in the workplace.
- Save costs by being proactive instead of reactive.
- Predict security threats as it proactively identifies exposures throughout the environment and understand how it impacts the organization.
- Validate critical vulnerabilities: Increase efficiency, pinpoint critical threats through penetration testing.
- Assess security controls: Test defence efficacy and make informed spending decisions based on risk to individual units within the organization.
- Analyse web application vulnerabilities: Reduce risk and minimize development spending by identifying exposures before going live.
- Communicate risk clearly and effectively: Present risk analytics in the context of key assets, operational areas, compliance mandates, and business objectives.
- Scalability: Gain insight into meeting compliance requirements and long-term security management

AI Enabled Cybersecurity Check List

Create Data Platforms

- Identify data sources and create platforms.
- For better AI, data must be up to date and processed to give shape to a palatable data for deep learning models.

Choose Right Set of Use Cases

- Right use case is important for AI implementation for cybersecurity.
- The selected use case must have sizable data that’s frequently refreshed.
- Ensure SMEs verify the output from use cases.

Collaborate

- Creation of a platform to collaborate, discuss, and share latest data threats is vital.
- Helps in to keep up the pace with threats that other security professionals manage.
- The above helps in improving the logic of AI algorithms to detect threats efficiently for best security.

Deploy SOAR

- SOAR helps organizations to gather security data and alerts from varied sources.
- Technologies enable businesses to conduct incident analysis and triage the incidents.
- SOAR helps in increased alert triage quality, improved security, effective operations centre management, and less time to onboard cyber analysts.

Making Cyber Analysts AI-Ready

- Educate and enable employees with the cyber security rules, policies, and guidelines.
- Train the cyber analysts for increasing their efficiency to create proper interfaces. This would help them understand incident alerts and AI tools.
- Intelligence chatbots may help security operation centres to respond to high demand levels from people who need help.

Instil Governance

Define roles and responsibilities for cyber analysts.

- Supervise AI algorithm output by cyber analysts before an action is taken.
- Create control processes to see if an AI algorithm showcases anomalies.
- Detect the risk tolerance for AI algorithm output generation.
- Implement a mechanism to supervise output logic and upgrades of AI algorithms.
- Measure success of AI-enabled cybersecurity through KPIs.

3 Pillars of Cyber Security

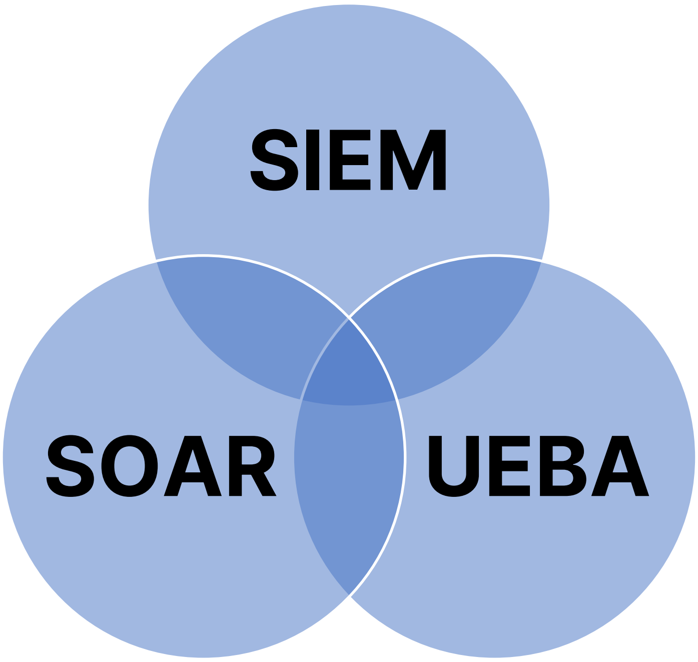


Figure 4 3 Pillars of Cyber Security

Cybersecurity is crucial to protect information from malicious threats that compromise the confidentiality, integrity, and availability of data. The right practices, technology, and tooling must be in place, with thorough evaluation and selection based on fitment, utilities, and cost-effectiveness.

Organizations often compromise on the selection of tools, prioritizing cost over functionality. An end-to-end 360-degree cybersecurity solution cannot be designed without integrating SIEM, UEBA, and SOAR.

Consultants and product vendors may also contribute to the confusion, by promoting their tools as providing an end-to-end posture. However, the consultant should suggest tools that meet all three needs or recommend separate tools for SIEM, UEBA, and SOAR.

SIEM

SIEM is a tool that goes beyond firewalls and antivirus to protect IT infrastructure by detecting attacks and analysing past behaviour to determine the type of attack. It efficiently manages updates and upgrades and can increase a system's incident protection to avoid damage to systems and virtual property.

- Real-time analysis of security alerts generated by applications and network hardware.
- It is a protective layer for
  - Log management systems
  - Security log- Event management
  - Security information management
  - Security event correlation
  - Data collection from various endpoints
  - Log collection & transformation
  - Data combing to discover threats in the infrastructure.
  - Security monitoring
  - Advanced threat detection
  - Machine Learning algorithms to detect patterns.
  - Broadcast notification and alerts
  - Highlight security breaches to investigate the alerts.
  - Detect security incidents.
  - Threat response workflow

UEBA

UEBA is an extension of SIEM where, in addition to observing suspicious network behaviour, it also triggers alerts on unusual entity or user behaviour is observed.

- UEBA constantly collects and stores usage information in specific to applications, instances, data storage frameworks and network traffic.
- Ensure transparency in hardware and user interactions and helps in identifying a broader range of threats concerning users as well as entities within an IT infrastructure.
- Monitor and analyse the behaviour of users and entities.
- Collect, process, and generate reports based on high quantities of information, including activity and access to emails, user files, networks etc.,
- Detect anomalous behaviour that could indicate an insider attack or compromise of user credentials.
- Correlate multiple anomalous activities that could be related to a single security incident.
- Flag if any user logs from unassigned workstation and trigger an investigation.

SOAR

SOAR helps in prioritizing threats derived from SIEM platform in a proactive manner. It facilitates the collection and consolidation of security threat data from various sources. It enables the gathering of alarm data from integrated platforms and combines them into a single platform, which allows for further investigation.

- SOAR platform is a solution stack for varied compatible software programs and SOAR product improves security.
- Automated platforms ensure that the tasks are efficiently executed in quick time. Helps in efficient resource management and increases productivity.
- Automates the user response to the threats.
- Improves digital and physical security operation efficiency.
- SOAR tools are enhancement for SIEM management task.
- With the help of case management, users can conduct research and perform additional investigations within a single case.
- Complex and complicated incident response workflows are accommodated to deliver agile results and facilitate an adaptive defence.
- Multiple playbooks are provided as solutions by SOAR tools to detect specific threats.

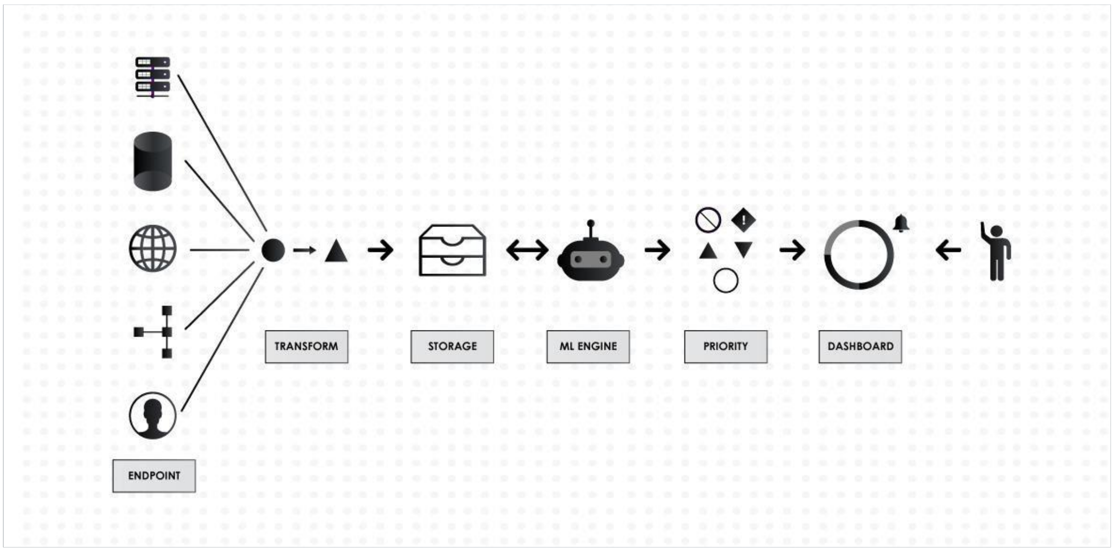


Figure 5 A well-rounded cybersecurity framework

Key benefits of having E2E Cyber Security Solution

- Teams across organizations experience healthier and stronger collaborations.
- Experience stronger agility.
- Protect networks and data from unauthorized access.
- Improved information security and business continuity management
- Improved stakeholder confidence in your information security arrangements
- Effectiveness and efficiency of operations improvement

- Improved company credentials with the correct security controls in place
- Faster recovery times in the event of a breach
- ROI improvement
- Vulnerabilities for applications and systems identification
- Stops your website from going down.
- More freedom to focus on high value projects.
- The cloud experiences improved scalability
- Quality assurance and automated builds have a more conducive environment.
- Inspires customers confidence.

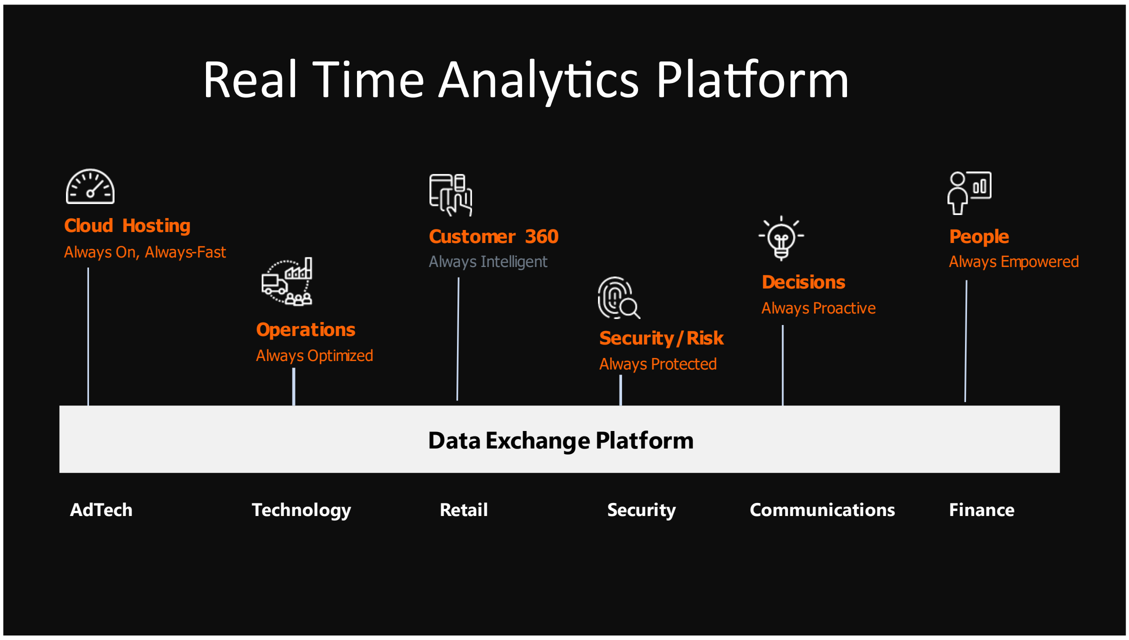
The functions and characteristics that a cybersecurity consulting firm and tool should perform.

- Thorough probing and assessment techniques
- Strong analytical and diagnostic skills
- Proper understanding of common web vulnerabilities
- Knowledge of contemporary standards, practices, procedures, and methods
- Understand architecture, administration and management of OS, networking, and virtualization software programming/software development concepts and analytics skills.
- High degree of adaptability to any situation and environment
- Manage security issues associated with OS, networking, and virtualization software.
- Knowledge of security across various platforms
- Good understanding of ethical Hacking
- Capable of doing technical vulnerability assessments, including systems and network
- Assess security setup from a holistic view, including threat modelling, specifications, implementation, testing, and vulnerability assessment.
- Strong on VAPT, web application, social engineering, physical security, wireless security assessments and implementing secure infrastructure solutions.
- Typical E2E Secure Computing Flow

AtomDops- an E2E Secure Computing Framework

Designing a framework that fits the organizational environment is a crucial priority, and customization should be implemented to achieve optimal results. The following outlines the key features of a real-time analytics platform and how it should be envisioned.

Traditional rule-based solutions are no longer sufficient to combat threats and fraud. The figure above illustrates how **AtomDops** platform by Atomstate is architected to cover cloud, operations, risk protection, and information flow using cutting-edge technology. It facilitates real time communication channels are put in place for rapid decision-making, and empowering individuals to take ownership of tasks can lead to improved finance and operations management. Our platform ensures organizations are proactive instead of being reactive.



Real Time Analytics Platform

Cloud Hosting
Always On, Always-Fast

Operations
Always Optimized

Customer 360
Always Intelligent

Security / Risk
Always Protected

Decisions
Always Proactive

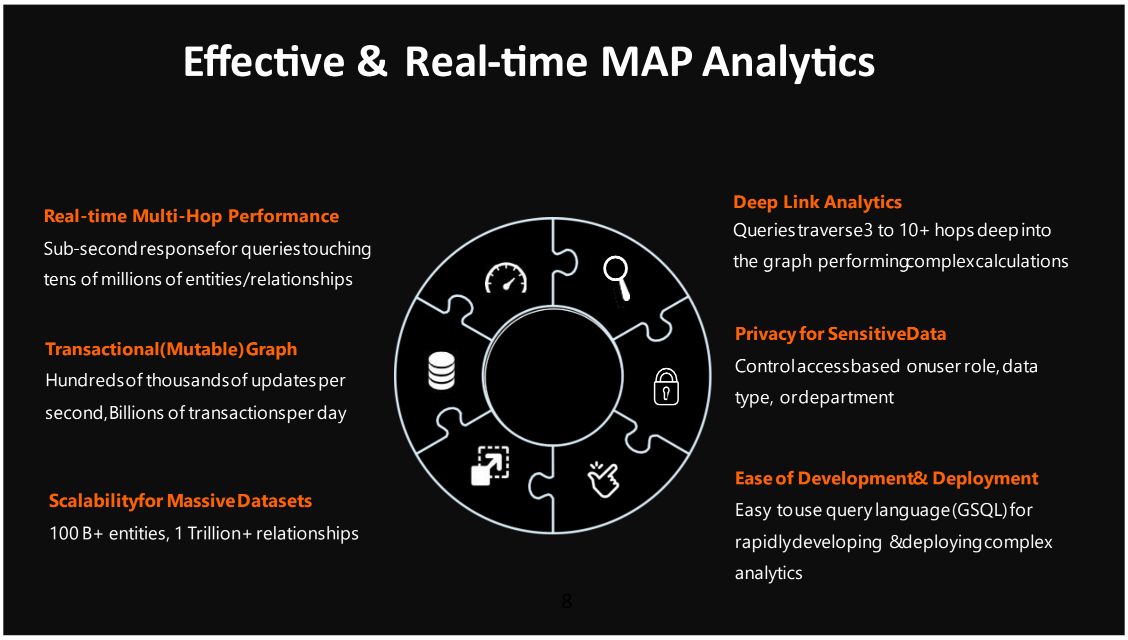
People
Always Empowered

Data Exchange Platform

AdTech
Technology
Retail
Security
Communications
Finance

Figure 6 Our AtomDops Platform- A cybersecurity data platform

The figure below illustrates our real-time MAP model analytics in **AtomDops** platform, which aids in traversing through millions of endpoints using queries to measure impacts of threats, identifying instances of fraud, and establishing a path to protection.



Effective & Real-time MAP Analytics

Real-time Multi-Hop Performance
Sub-second response for queries touching tens of millions of entities/relationships

Transactional (Mutable) Graph
Hundreds of thousands of updates per second, Billions of transactions per day

Scalability for Massive Datasets
100 B+ entities, 1 Trillion+ relationships

Deep Link Analytics
Queries traverse 3 to 10+ hops deep into the graph performing complex calculations

Privacy for Sensitive Data
Control access based on user role, data type, or department

Ease of Development & Deployment
Easy to use query language (GSQL) for rapidly developing & deploying complex analytics

Figure 7 AtomDops' MAP Model Analytics

Case Study

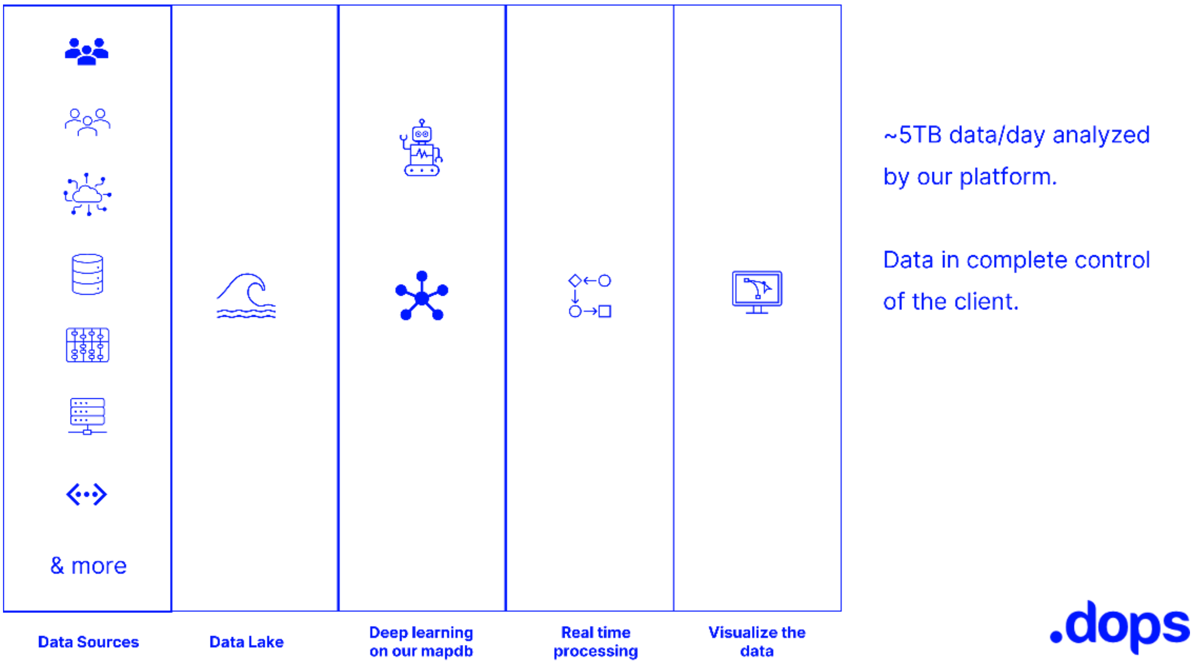

& more
Data Sources
Data Lake
Deep learning on our mapdb
Real time processing
Visualize the data
~5TB data/day analyzed by our platform.
Data in complete control of the client.
.dops

Figure 8 Architecture implemented in a client place.

We have deployed AtomDops for large insurance player to track their 360° data landscape. The platform was deployed as a control in client's AWS cloud platform. We have integrated their existing data lake to ingest data coming in from various sources.

- IoT devices,
- Internal users,
- External users,
- Databases,
- Applications,
- Network,
- External APIs data, and more.

On an average the platform ingested ~5TB worth of data/day which is processed/enriched in real time. Our customized deep learning model run on top the data to bring forward lurking dangers.

Benefits of using AtomDops

- Be in complete control of your data as we deploy AtomDops in control plane mode.
- It facilitates proactive approach and chucks off reactive state management.

- It can expand its storage based on the data without you worrying about increasing data size.
- Processes the data in real time as it comes by.
- Customized deep learning models which suit your scenarios.
- Time series and go back in time to understand the impacts over time.
- Case and SLA management.
- Integrate with any kind of data source.

Typical Questionnaire to Implement

- Assessments
    - Have you performed a cybersecurity risk analysis, or compliance risk analysis in the past year or two?
    - Was the assessment performed using a specific methodology (like ISO, COBIT, NIST)?
    - Was the assessment performed by a third party?
- Plan/Management
    - Do you have an active security plan containing items identified in the risk analysis report that you actively implement and regularly review?
    - Does your security plan include staff training?
- Policies and Procedures
    - Do you have written security policies and procedures, including an enforced network password policy and a mobile device policy?
    - Do they meet all the requirements of the HIPAA Security Rule regulations (if applicable)?
    - Is your appropriate staff trained on the security policies and procedures?
    - Do you have documentation demonstrating implementation of the policies and procedures?
- Infrastructure
    - Do you have up to date firewalls, including next-generation firewall appliances, protecting your network?
    - Do you have network access control to create separate secure networks and virtual local area networks (VLANs) for staff and businesses, residents, and guests?
    - Does access to your network require authentication?
    - Do you regularly monitor your network traffic and analyze threats?
    - Do you use modern e-mail gateway security monitoring and filtering services?
    - Do you have up to date anti-virus and anti-malware, including cloud anti-virus detection?
    - Do you keep all devices' operating systems and all applications running on your network, including mobile devices and Internet of

Things (IoT) appliances, patched and up to date?
  - Do you have tools to manage mobile devices and other endpoint devices?
  - Do you perform data backup regularly?
  - Do you have a disaster recovery plan?
  - Have you tested your disaster recovery plan?
- Organization/Management
  - Do you have a security officer?
  - Do you have a privacy officer?
- Training
  - Do you have training for staff on privacy, data security, and your applicable policies and procedures?
  - Do you offer training upon onboarding?
  - Do you offer regular refresher training on the topic?
- Governance/Communication
  - Do you have a compliance committee?
  - Is IT/cybersecurity part of the regular compliance committee?
  - Is IT security addressed regularly at compliance committee meetings?
  - Is compliance a topic in your management meetings?
  - Do you report compliance status to the Board of Directors?
  - Does IT security fit within your organization’s broader risk management program?
  - Does your organization understand the action and communication plan in case of a security breach?
- Cyber Liability
  - Do you have cyber liability insurance?
  - Did you read the fine print of your cyber liability insurance?
  - Do you know the types of attacks or breaches covered, the specific expenses covered and their limits, the types of events not covered, and the conditions that would result in revocation of the policy?
  - Do you know who in your organization knows the insurance carrier’s breach team and attorneys in case of a security breach?

Abbreviations

SME- Subject Matter Expert
AI- Artificial intelligence
SOAR- Security Orchestration Automation & Response
KPI- Key Performance Indicators
SIEM- Security Information Event Management
E2E- End 2 End/End to End
SOAR- User Entity Behaviour Analytics

Reviewed By

Dr. Srikanth Sundarajan

Dr. Srikanth Sundararajan has 25+ years of international experience in the software product and services space and 8+ years as an investor. He has been an Entrepreneur, an Executive, a Professor, and an Investor. He has worked at HP, Informix in the US, and was part of the executive leadership team at HCL, the worldwide CTO at Cognizant and the COO at Persistent through its successful IPO. In the US he had also successfully founded his own start up, Pretzel Logic Software Inc., which was acquired by BEA spinoff WebGain. BEA was later acquired by Oracle. He was also part of the founding team at IDS, which was also acquired.

Currently he is a General Partner with VenturEast, an India focused fund to help technology focused start-ups looking to go global from India across segments like education, health, financial services, agritech, and Enterprise SaaS. Prior to that he was a Venture Partner with Helion Advisors with a similar investment thesis. He is also on the GC of CIE at IIITH, and an advisor to THub. He is founding member of the Nasscom DeepTech Club, and part of the Nasscom Product Conclave initiative. Advisor to Stongher Ventures, and Auctus Advisors.

He was also a visiting faculty of computer science at IIT Bhubaneswar and has taught at several US universities. He also serves on national committees on technical education, an initiative of MHRD, Government of India. He was also a member of the tech committee for the Government of India initiative on indirect taxes (Customs and Excise)

He holds a B Tech degree from Indian Institute of Technology, Madras, and a MS/PhD in Computer and Information Sciences from University of Illinois, Urbana Champaign. He has several publications and is the holder of patents, jointly with HP.

About DSCI-CCoE

The Cybersecurity Center of Excellence (CoE) is a joint initiative of the Government of Telangana and Data Security Council of India (DSCI) to accelerate the cybersecurity momentum and create a conducive cybersecurity ecosystem that nurtures innovation, entrepreneurship and capability building. CoE works with all industry organisations, government agencies, academia and R&D centers and user groups and collaborates with other industry bodies, incubators, and accelerators to accomplish its mission. DSCI is a not-for-profit, industry body on data protection in India, set up by NASSCOM®, committed to making the cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI is the apex industry body for Cybersecurity in India.

ccoe.dsci.in   cybersecurity-coe-telangana   ccoe.hyd   CCoE_Hyd   dscivideo

About Atomstate

Atomstate Technologies Private Limited is deep-tech startup which works in the fields of NLU, IoT, Blockchain, and Cybersecurity. AtomDops is its secure computing platform-as-a-service to manage recursive and traversing data of organizations. Apart from AtomDops, it also has AtomAX and AtomMesh. AtomAX is an end-to-end NLU platform offered as a service for organizations. It has been deployed to work on tasks like crunching sentiment analysis on wide range of data with automations, data platforms, minutes of meeting contextualization, etc. AtomMesh is our IoT cloud which has been deployed to work on aspects like smart energy audits, anomaly management, etc for large hardware and manufacturing industries. Atomstate has been awarded top-10 startup in India Start-up Festival 2022, BITS Pilani Pitchers 2023, and part of RevvUp Cohort 3 of T-AIM.

atomstate.com   atomstatehq   Atomstate   atomstatehq   atomstate

CYBERSECURITY CENTER OF EXCELLENCE
Servcorp - Business Center In Hyderabad:
Level 7 Maximus Towers Building 2A,
Raheja Mindspace, HUDA Techno Enclave,
HITEC City, Hyderabad, Telangana 500081
FOR ANY QUERIES:
P: +91 040 40339650
E: marketing.ccoe@dsci.in

ATOMSTATE TECHNOLOGIES PRIVATE LIMITED
THub2.0, Knowledge City, HITEC City,
Vittal Rao Nagar, Inorbit Mall Road,
Hyderabad 500081, Telangana, India.

FOR ANY QUERIES:
P: +91 040 6639 6639
E: hello@atomstate.com

_atomstate

IDENTIFY **HIDDEN** DANGERS & STAY **PROACTIVE**

CYBERSECURITY
CENTRE *of* EXCELLENCE

A joint initiative of DSCI & Government of Telangana

For any queries

P: +91 040 40339650
E: marketing.ccoe@dsci.in
W: ccoe.dsci.in