प्रशासनिक सुधार और लोक शिकायत विभाग
DEPARTMENT OF
ADMINISTRATIVE REFORMS &
PUBLIC GRIEVANCES

सत्यमेव जयते

Proceedings

National e-Governance Webinar Series 2025 - 2026

Excellence in Central level initiative in e Governance Practices/Innovation in Cyber Security

November 21st, 2025

Contents

1. Background

The Department of Administrative Reforms and Public Grievances institutionalised National e-Governance Webinar Series to showcase the award-winning initiatives that have received the prestigious National Award for Excellence in e-Governance, with the objective of greater learning, dissemination and replication.

These initiatives have leveraged technology to improve governance with a potential to enhance efficiency, transparency and inclusivity of government operations. By harnessing the power of digital tools and data analytics, governments can streamline administrative processes, expedite service delivery, and make informed policy decisions.

The National e-Governance Webinar Series focuses on the following themes:

- Government Process Re-engineering by use of technology for Digital Transformation
- Innovation by Use of AI and other new age technologies for Citizen- Centric Services
- Best e-Governance Practices/Innovation in Cyber Security
- Grassroots Level Initiatives for Deepening / Widening of Service Delivery
- Replication And Scaling Up of Successful National Awarded Projects like NAeG, Prime Minister Awards in Excellence, Awards conferred by other Central Ministries by State/UT/District
- Digital transformation by use of data analytics in digital platforms by Central Ministries / States/UTs

NeGW seeks to foster a culture of continuous learning, skill development, and knowledge exchange. Each webinar emphasises on a unique e-governance theme, featuring award-winning initiatives that have demonstrated outstanding contributions to their respective domains. NeGW aims to inspire and instill a new spirit of enthusiasm among administrators and stakeholders involved in government programs' implementation.

- The fourth webinar of the NeGW Series 2025-26 was convened on **'Excellence in Central level initiative in e Governance Practices/Innovation in Cyber Security'** on **November 21st, 2025.** The webinar highlighted innovative projects at the level of Central Government that that demonstrate groundbreaking advancements in cybersecurity measures, resulting in stronger protection against emerging cyber threats. It underscored initiatives leveraging advanced technologies, methods, and processes to bolster security infrastructure, enhance the resilience of systems and networks, and safeguard critical data. The session also encouraged Startups, Academia, and R&D institutions to showcase exemplary research and innovations in the application of cybersecurity for e-governance, particularly those which contribute meaningfully to citizen-centric digital security.

2. Theme

The theme of the fourth session of NeGW 2025-26 held on **November 21st, 2025** was **Excellence in Central level initiative in e Governance Practices/Innovation in Cyber Security**.

The award-winning initiatives under this theme highlight the transformative potential of digital innovation in strengthening cybersecurity and enhancing national digital resilience as NCRTC's robust IT-OT convergence framework secures India's critical railway infrastructure through AI-enabled threat detection, digital twin technology, unidirectional gateways, and predictive maintenance analytics—cutting cyber risks by 50%, improving incident response by 40%, and ensuring near-zero downtime for millions of daily passengers. Meanwhile, NIC's DHRISTI platform redefines cyber defence across the Government of India through AI/ML-driven log analytics, automated incident response, and real-time threat intelligence, enabling the protection of mission-critical services, supporting faster investigations, and empowering SOC teams with unprecedented accuracy, scale, and situational awareness, embodying the vision of a secure, resilient, and future-ready digital governance ecosystem.

3. Proceedings

3.1. Welcome Address

Smt. Sarita Chauhan, Joint Secretary, DARPG, welcomed all the participants to the fourth session of the National e-Governance Webinar Series 2025-26, focusing on the theme 'Excellence in Central Level Initiative in e-Governance Practices / Innovation in Cyber Security'. She highlighted the growing scale of e-services across the country, noting that States and Central Ministries together now deliver more than 23,000 digital services, marking significant progress in public service delivery, transparency, efficiency, and reduction in turnaround times.

She emphasized that, with the rapid expansion of digital public infrastructure, ensuring robust cybersecurity has become pivotal for safeguarding personal data, maintaining business continuity, and protecting critical national assets. She shared that the category on Innovation in Cyber Security was introduced in the National Awards for e-Governance 2025 to recognise initiatives that strengthen the security and resilience of digital platforms.

Smt. Chauhan underscored that the NeGW series serves as a platform for knowledge dissemination, enabling public administrators to understand the objectives, challenges, and impact of award-winning initiatives that advance secure, citizen-centric service delivery.

She introduced the two award-winning initiatives featured in the session: NCRTC's Robust Cybersecurity Measures in IT-OT Convergence for Railway Systems, which enhances the safety and reliability of high-speed rail operations through advanced cybersecurity and predictive monitoring; and NIC's Data Harmonisation for Risk Insights and Security Threat Intelligence (DHRISTI), which leverages AI/ML-based analytics for real-time threat detection and resilience of government digital services.

3.2. Shri Manvendra Singh, Group General Manager (Operations), NCRTC

Following the Joint Secretary's opening remarks, Shri Manvendra Singh, Group General Manager at the National Capital Region Transport Corporation (NCRTC), delivered an insightful presentation on NCRTC's pioneering work in establishing robust cybersecurity frameworks for the seamless convergence of Information Technology (IT) and Operational Technology (OT) within modern railway systems. His address outlined the technological vision, strategic approach, and innovative security architecture adopted for India's first Namo Bharat regional rail network.

He began by offering an overview of NCRTC's mandate and achievements. NCRTC is implementing India's first regional rapid transit system, with the Delhi–Meerut corridor already operational. Designed for a speed of 180 kmph and operating at 160 kmph, the Namo Bharat system incorporates several India-first and world-first innovations. These include the country's first indigenous platform screen doors, a captive mission-critical LTE network with 5 MHz allocation in Band 28, Austria-based precast slab track technology enabling low-maintenance high-speed tracks, NCRTC's in-house developed Common Operating System (COS) for project efficiency, and the world's first ETCS Hybrid Level 3 signaling system over LTE.

Transitioning to the core theme, Shri Singh explained that traditionally, railway systems maintain strict separation between IT and OT domains. While IT systems, such as ticketing platforms, customer services, websites, and internal networks, are connected to the internet and therefore more vulnerable, the OT side (signaling, telecom, AFC, rolling stock, lifts, and escalators) historically functions in isolated, closed-loop environments perceived to be secure from external cyber threats.

However, this separation also limits opportunities for leveraging real-time data for predictive and preventive maintenance, data analytics, and enhanced passenger experience. Recognizing this gap, NCRTC undertook a pioneering initiative to safely integrate OT systems with the IT ecosystem, enabling data flow to a central data lake where AI/ML-driven analytics support proactive maintenance and operational optimization.

He emphasized that this integration significantly increases the system's cyberattack surface. Linking OT infrastructure with IT networks exposes critical operations to potential external threats, including ransomware, denial-of-service attacks, and exploitation of outdated or unpatched legacy systems. While traditional approaches rely on demilitarized zones (DMZs) and multilayered firewalls, NCRTC identified inherent vulnerabilities in these models and sought a more secure and fail-proof mechanism.

To address this, NCRTC adopted unidirectional gateways, also known as data diodes: impenetrable, one-way hardware devices that allow data to flow only from OT to IT, ensuring that no external command or intrusion can reach operational systems. This "Made-in-India" innovation not only enhances security but also ensures cost-effectiveness and scalability across large railway operations. Through this architecture, critical OT data is mirrored to IT networks without creating pathways for cyberattacks.

Shri Singh outlined several categories of cyber risks affecting railway environments:

- External threat agents, both domestic and international, who continuously scan for vulnerabilities
- Physical security risks arising from unauthorized access to critical rooms and systems
- Network vulnerabilities due to misconfigured or unhardened switches, servers, or firewalls
- Software dependency risks, especially where outdated operating systems and unpatched applications create exploitable weaknesses

He elaborated on how ransomware and denial-of-service attacks have emerged as the most common and disruptive threats to global railway systems, often targeting ticketing systems and public information platforms, which are closely linked to IT infrastructures. Citing recent incidents globally, he noted the clear trend of attackers increasingly focusing on transportation networks, recognizing them as high-value, high-impact targets.

To ensure comprehensive protection, NCRTC aligned its cybersecurity framework with leading global standards, including IEC 62443 for industrial automation and CLC 50701:2023, the dedicated cybersecurity standard for railways. These frameworks serve as the foundation for NCRTC's security policies, threat management practices, and system-hardening protocols.

Concluding the session, Shri Singh reiterated NCRTC's cybersecurity vision: to achieve data-driven operations through IT–OT integration without compromising the safety and integrity of operational systems. He highlighted that the secure convergence framework not only enhances operational reliability but also benefits passengers directly through improved service availability, minimized downtime, and proactive maintenance interventions.

His presentation set a strong precedent for how next-generation high-speed and regional rail systems can adopt advanced cybersecurity architectures while embracing digital transformation at scale.

3.3. Shri Hariharan M., Joint Director (IT), NIC

The second presentation of the session was delivered by Shri Hariharan, representing the National Informatics Centre (NIC). Speaking on behalf of the DHRISTI leadership, he presented a comprehensive overview of the initiative Data Harmonisation for Risk Insights and Security Threat Intelligence (DHRISTI), a flagship cybersecurity programme designed to elevate the resilience, intelligence, and preparedness of India's government-wide digital ecosystem.

He began by situating DHRISTI within the broader operational environment of NIC, explaining that NIC not only enables e-governance across the Union and State governments but also manages some of the largest and most complex digital infrastructures in the country. With National Data Centres located in Delhi, Pune, Bhubaneswar, Hyderabad, and an upcoming centre in Guwahati, NIC hosts or routes over 80% of the Government of India's IT systems, websites, and internal networks. This central vantage point ensures that virtually all digital interactions, ranging from ministry websites and mission-critical portals to desktops, laptops, and service endpoints, pass through NIC's secure infrastructure.

Because of this, NIC's networks are under continuous and sophisticated cyber targeting, including attempts from cybercriminal organisations, hacktivist groups, and state-sponsored threat actors. Every attempted access, anomaly, or incident generates logs, hundreds of thousands of them every second. Shri Hariharan clarified that these logs are not just system leftovers but are essentially digital fingerprints, recording minute-by-minute events such as successful or failed login attempts, suspicious access patterns, deviations in network behaviour, and early indicators of potential intrusions.

However, the volume, velocity, and diversity of this data made manual monitoring nearly impossible. Earlier, SOC teams had to scan logs manually or rely only on predefined rules, making it difficult to detect new or evolving attack vectors. This operational bottleneck, combined with the increasing sophistication of cyber threats, laid the foundation for conceptualising DHRISTI as early as 2017.

He described the SOC environment prior to DHRISTI: analysts had to navigate massive amounts of traffic originating from desktops in ministries, systems in Central Vista, government websites, external user traffic, and internal department workflows. Without AI-enabled support, critical attack patterns could go unnoticed simply due to scale. This operational reality sparked the idea of a centralised, AI/ML-powered, real-time threat intelligence platform that could ingest, correlate, and analyse logs from across the government ecosystem to detect threats faster and more accurately than humans alone.

The need for such a system became even more pronounced as cyberattacks globally began targeting public-sector infrastructure with increasing frequency. He shared how modern threats, ranging from brute-force intrusions and credential stuffing to sophisticated zero-day exploits, ransomware campaigns, and malware targeting government websites, required an automated, intelligence-led monitoring framework rather than a manual, rule-based approach. DHRISTI was envisioned precisely to meet this challenge.

Transitioning to the system's capabilities, Shri Hariharan explained how DHRISTI processes logs from varied IT and security components: servers, firewalls, intrusion prevention systems (IPS), endpoint detection and response tools (EDR/XDR), switches, routers, and application infrastructures. By harmonising data across these diverse systems, DHRISTI creates a unified, searchable, and analysable data lake. He broke down simple examples, such as the difference between a successful login log and a failed login attempt, and explained how correlating thousands of such micro-events can reveal patterns of malicious behaviour that would otherwise remain hidden.

He emphasised that DHRISTI transforms cybersecurity operations through AI/ML models, automated triaging, pattern analysis, and risk scoring. This shift significantly reduces dependence on manual interventions and dramatically improves detection timeframes. The platform's architecture enables it to analyse millions of events per second, correlate them, and highlight early signs of threats, giving SOC teams the ability to respond before an incident escalates.

Shri Hariharan also reaffirmed the national significance of this initiative. With government data and services becoming increasingly digital and interconnected, any vulnerability, no matter how small, can have cascading repercussions. DHRISTI ensures that the government remains prepared against the evolving landscape of cyber threats, enhances compliance with cybersecurity frameworks, and empowers analysts with a deeper understanding of network behaviour.

He concluded by reiterating that DHRISTI marks a pivotal move from reactive cybersecurity practices to proactive, predictive, and intelligence-driven defence, aligning with global best practices and significantly strengthening India's cyber resilience. Through this initiative, NIC has demonstrated a future-ready approach to securing mission-critical infrastructure, making DHRISTI a transformative asset in the nation's cybersecurity roadmap.

3.4. Vote of Thanks

Shri Suvasish Das, Director, DARPG, delivered the Vote of Thanks for the session. He expressed his heartfelt gratitude to all participants for their active engagement in the fourth session of the National e-Governance Webinar Series. He conveyed appreciation to all attendees for contributing to an insightful and enriching discussion, and extended special thanks to Secretary, DARPG, for her continued guidance and support to the webinar series. Shri Das expressed his deep appreciation to the esteemed speakers, Shri Manvendra Singh, Group General Manager, NCRTC, and Shri Hariharan from NIC, for their detailed presentations and for elucidating how robust cybersecurity measures, data analytics, and advanced monitoring frameworks are strengthening India's digital governance and transport infrastructure.

He highlighted that NCRTC's IT-OT convergence initiative, incorporating tools such as digital twins, CI monitoring, and secure network architectures, is significantly enhancing the safety and reliability of high-speed rail systems. He also noted that NIC's DHRISTI platform, powered by AI-driven log analytics and automated incident response, is transforming threat detection and safeguarding critical e-government services.

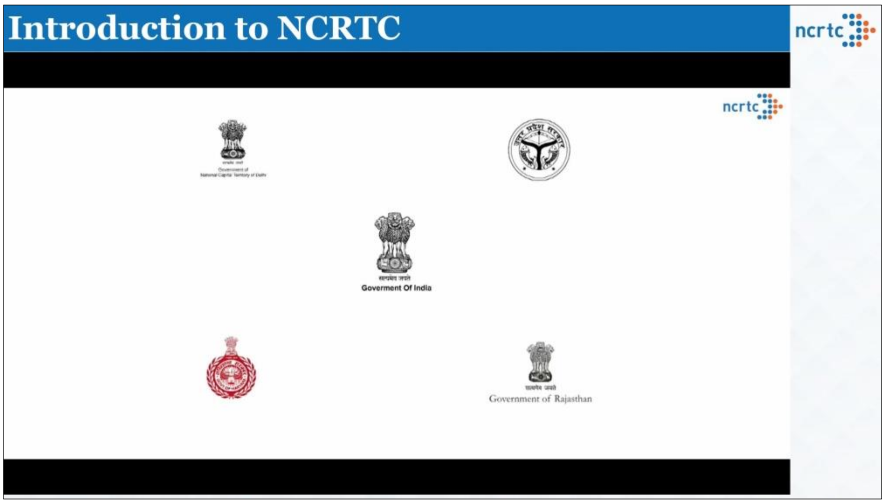
Shri Das extended his appreciation to senior officers from the States/UTs, public administrators, and participants from across the country for their valuable time and engagement. He encouraged continued participation in future sessions of the webinar series. Before concluding, he also reminded all attendees that the last date for submission of nominations for the National e-Governance Awards 2026 is 30th November, and urged organisations to submit their entries and showcase their exemplary initiatives.

In conclusion, he thanked all attendees for their valuable time and contributions and expressed hope for their continued participation in the forthcoming sessions of the National e-Governance Webinar Series 2025-26.

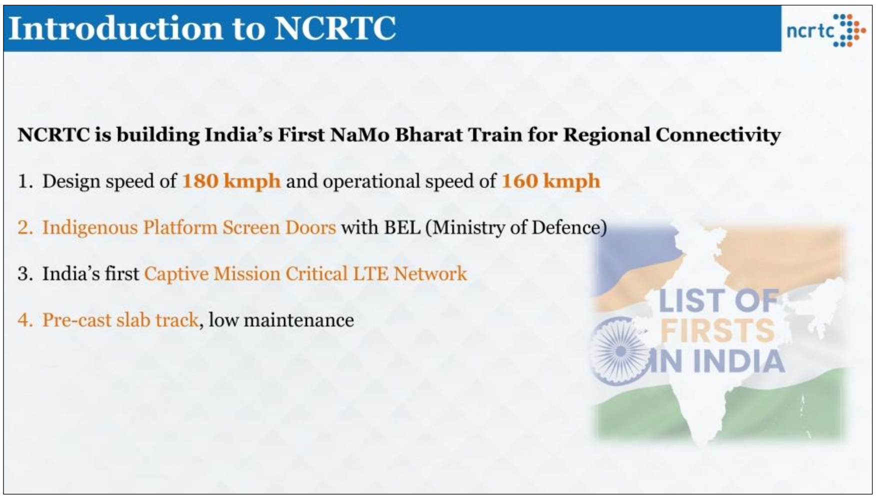
4. Annexure

4.1. Presentation by the Shri Manvendra Singh, Group General Manager, NCRTC

Robust cybersecurity measures in IT-OT convergence for railway systems



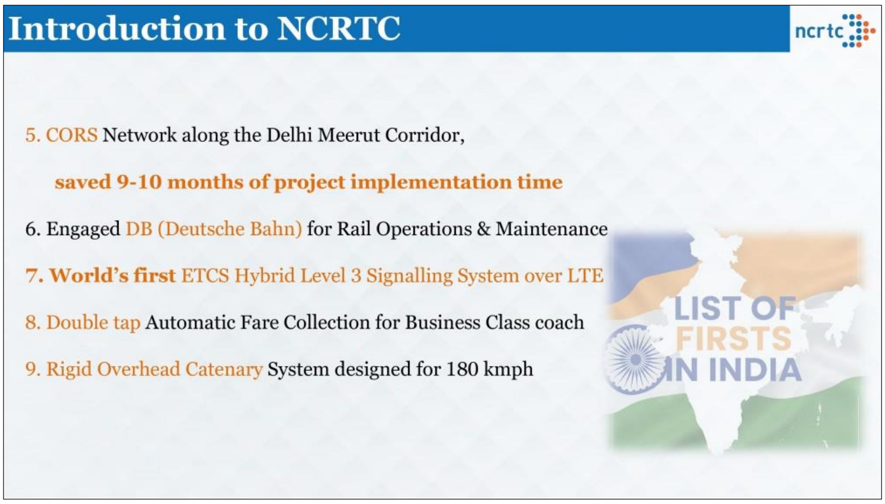
Introduction to NCRTC



Introduction to NCRTC

NCRTC is building India's First NaMo Bharat Train for Regional Connectivity

1. Design speed of **180 kmph** and operational speed of **160 kmph**
2. Indigenous Platform Screen Doors with BEL (Ministry of Defence)
3. India's first Captive Mission Critical LTE Network
4. Pre-cast slab track, low maintenance



Introduction to NCRTC

5. CORS Network along the Delhi Meerut Corridor,

saved 9-10 months of project implementation time

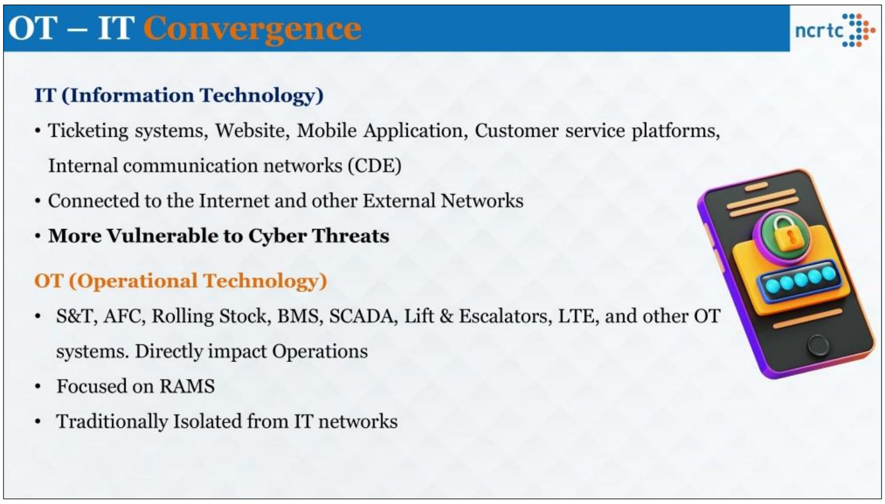
6. Engaged DB (Deutsche Bahn) for Rail Operations & Maintenance

7. World's first ETCS Hybrid Level 3 Signalling System over LTE

8. Double tap Automatic Fare Collection for Business Class coach

9. Rigid Overhead Catenary System designed for 180 kmph

LIST OF
FIRSTS
IN INDIA



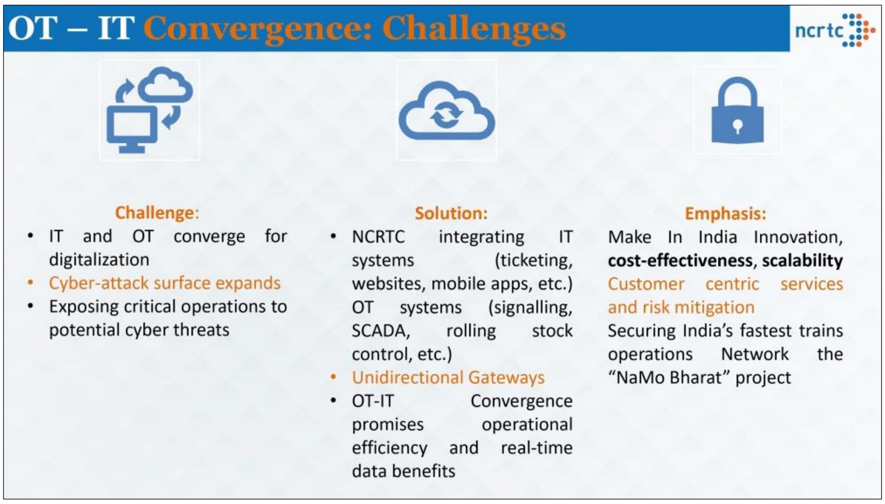
OT – IT Convergence

IT (Information Technology)

- Ticketing systems, Website, Mobile Application, Customer service platforms, Internal communication networks (CDE)
- Connected to the Internet and other External Networks
- **More Vulnerable to Cyber Threats**

OT (Operational Technology)

- S&T, AFC, Rolling Stock, BMS, SCADA, Lift & Escalators, LTE, and other OT systems. Directly impact Operations
- Focused on RAMS
- Traditionally Isolated from IT networks



OT – IT Convergence: Challenges

Challenge:

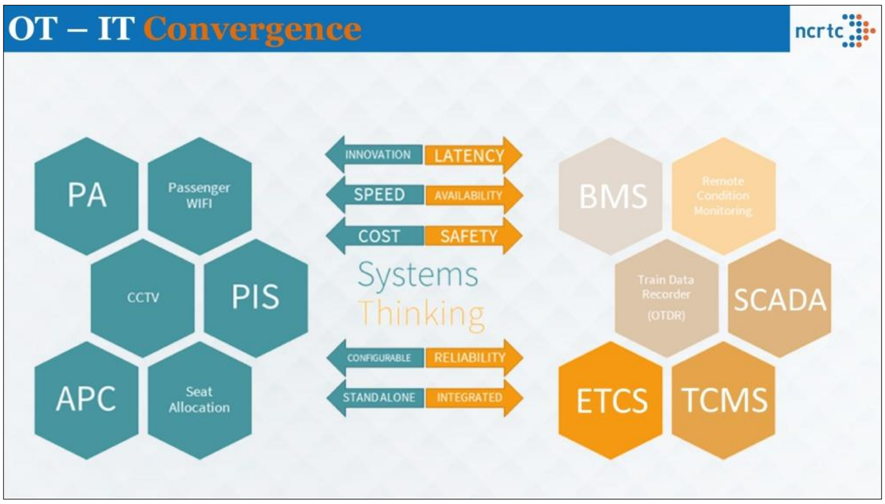
- IT and OT converge for digitalization
- Cyber-attack surface expands
- Exposing critical operations to potential cyber threats

Solution:

- NCRTC integrating IT systems (ticketing, websites, mobile apps, etc.) OT systems (signalling, SCADA, rolling stock control, etc.)
- Unidirectional Gateways
- OT-IT Convergence promises operational efficiency and real-time data benefits

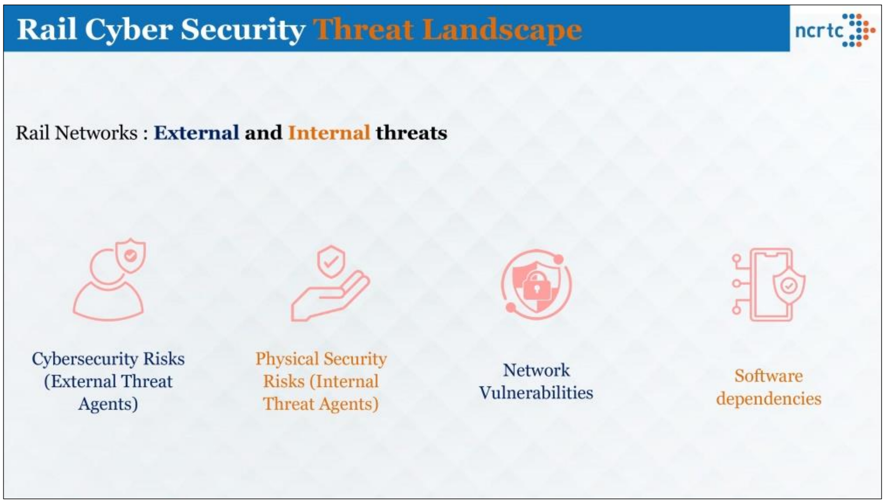
Emphasis:

Make In India Innovation, **cost-effectiveness**, **scalability**
Customer centric services and risk mitigation
Securing India's fastest trains operations Network the "NaMo Bharat" project



OT – IT Convergence

ncrtc



Rail Cyber Security Threat Landscape

ncrtc

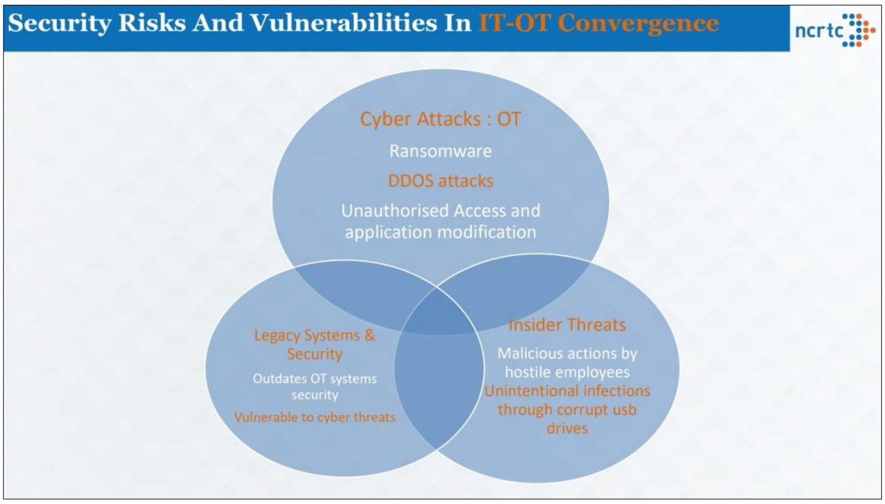
Rail Networks : **External and Internal threats**

Cybersecurity Risks (External Threat Agents)

Physical Security Risks (Internal Threat Agents)

Network Vulnerabilities

Software dependencies



Security Risks And Vulnerabilities In IT-OT Convergence

ncrtc

Cyber Attacks : OT

Ransomware

DDOS attacks

Unauthorised Access and application modification

Legacy Systems & Security

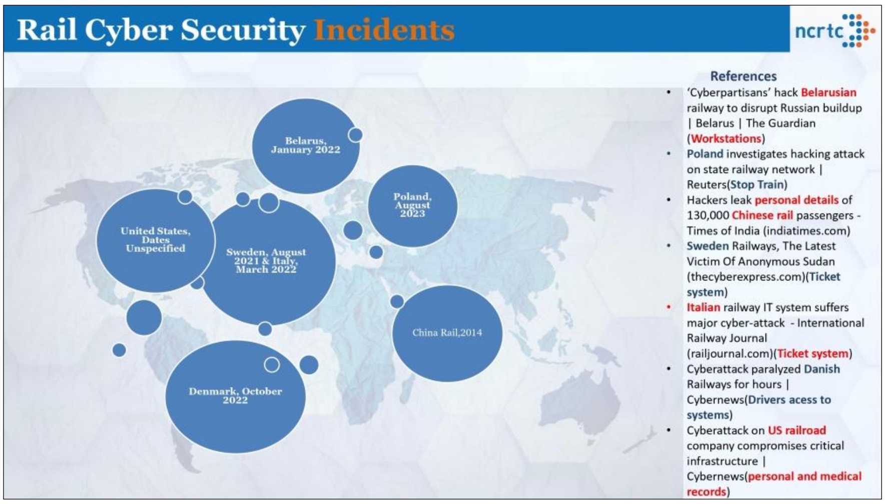
Outdates OT systems security

Vulnerable to cyber threats

Insider Threats

Malicious actions by hostile employees

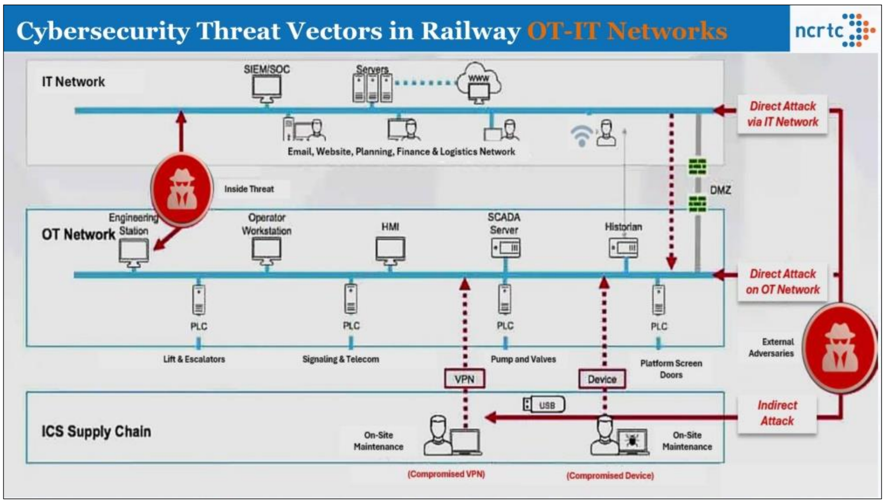
Unintentional infections through corrupt usb drives



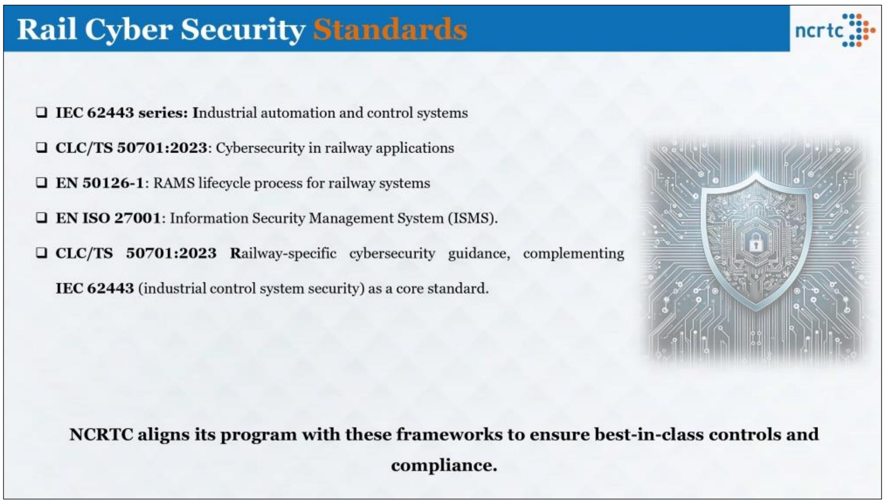
Rail Cyber Security Incidents

References

- ‘Cyberpartisans’ hack **Belarusian** railway to disrupt Russian buildup | Belarus | The Guardian (**Workstations**)
- **Poland** investigates hacking attack on state railway network | Reuters(**Stop Train**)
- Hackers leak **personal details** of 130,000 **Chinese rail** passengers - Times of India (indiatimes.com)
- **Sweden** Railways, The Latest Victim Of Anonymous Sudan (thecyberexpress.com)(**Ticket system**)
- **Italian** railway IT system suffers major cyber-attack - International Railway Journal (railjournal.com)(**Ticket system**)
- Cyberattack paralyzed **Danish** Railways for hours | Cybernews(**Drivers acess to systems**)
- Cyberattack on **US railroad** company compromises critical infrastructure | Cybernews(**personal and medical records**)



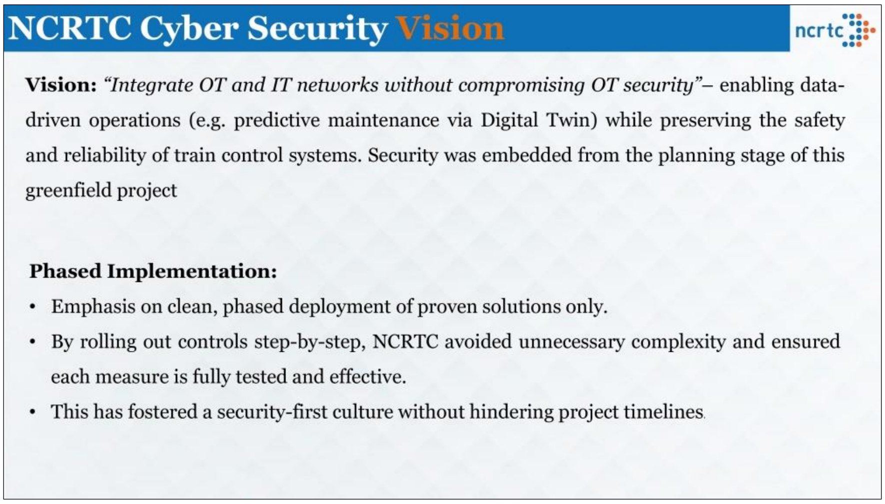
Cybersecurity Threat Vectors in Railway OT-IT Networks



Rail Cyber Security Standards

- ❑ **IEC 62443 series:** Industrial automation and control systems
- ❑ **CLC/TS 50701:2023**: Cybersecurity in railway applications
- ❑ **EN 50126-1**: RAMS lifecycle process for railway systems
- ❑ **EN ISO 27001**: Information Security Management System (ISMS).
- ❑ **CLC/TS 50701:2023** Railway-specific cybersecurity guidance, complementing **IEC 62443** (industrial control system security) as a core standard.

NCRTC aligns its program with these frameworks to ensure best-in-class controls and compliance.

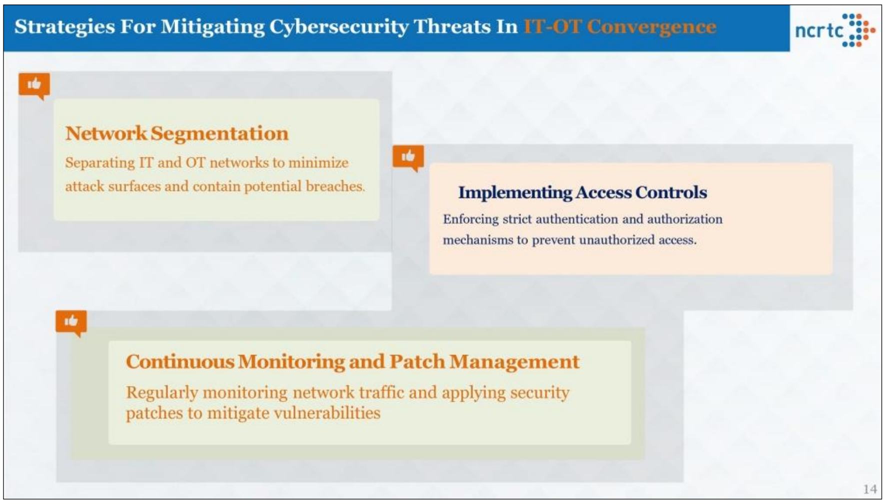


NCRTC Cyber Security Vision

Vision: *"Integrate OT and IT networks without compromising OT security"*– enabling data-driven operations (e.g. predictive maintenance via Digital Twin) while preserving the safety and reliability of train control systems. Security was embedded from the planning stage of this greenfield project

Phased Implementation:

- Emphasis on clean, phased deployment of proven solutions only.
- By rolling out controls step-by-step, NCRTC avoided unnecessary complexity and ensured each measure is fully tested and effective.
- This has fostered a security-first culture without hindering project timelines.



Strategies For Mitigating Cybersecurity Threats In IT-OT Convergence

Network Segmentation

Separating IT and OT networks to minimize attack surfaces and contain potential breaches.

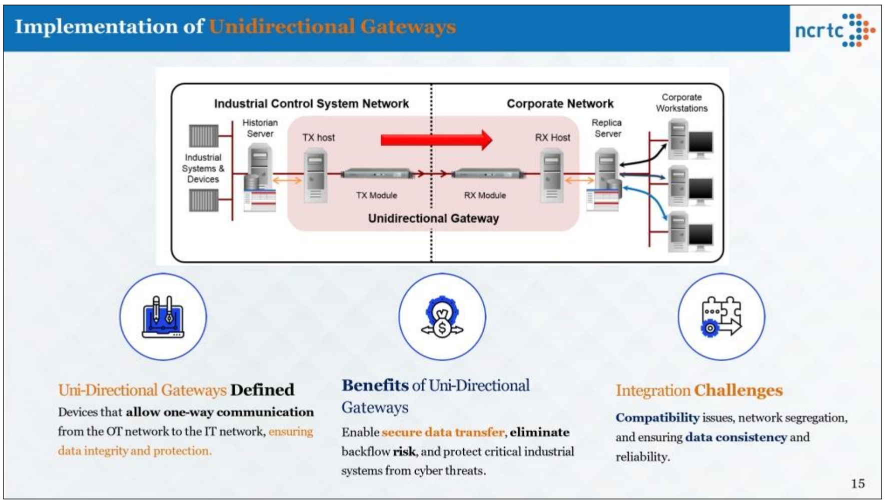
Implementing Access Controls

Enforcing strict authentication and authorization mechanisms to prevent unauthorized access.

Continuous Monitoring and Patch Management

Regularly monitoring network traffic and applying security patches to mitigate vulnerabilities

14



Implementation of Unidirectional Gateways

Uni-Directional Gateways Defined

Devices that **allow one-way communication** from the OT network to the IT network, ensuring data integrity and protection.

Benefits of Uni-Directional Gateways

Enable **secure data transfer**, **eliminate** backflow **risk**, and protect critical industrial systems from cyber threats.

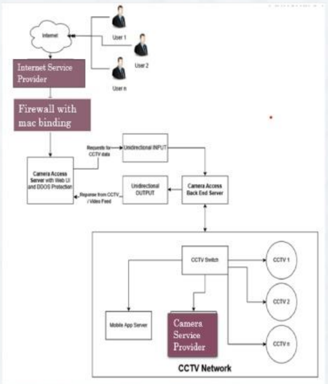
Integration **Challenges**

Compatibility issues, network segregation, and ensuring **data consistency** and reliability.

15

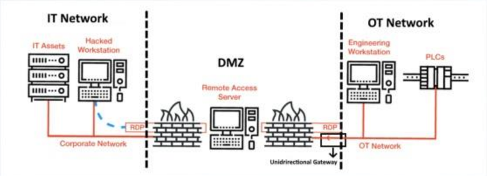
Case Study: Unidirectional gateway ~ CCTV System

ncrtc



Outbound Interface: Connects to the CCTV system and allows the transfer of video data out of the network.

Security Controls: Implements security measures to ensure that data can only flow in one direction.
Protocol Conversion to break communication and remove any embedded scripts for OT access



16

IT Cybersecurity Solutions

ncrtc

XDR:

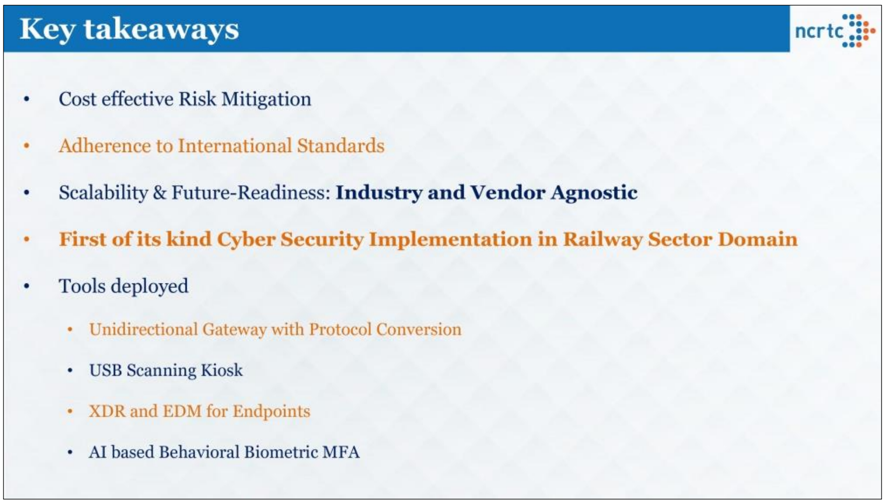
- Secured all endpoints with an XDR (Extended Detection & Response) solution.
- "Virtual SOC," correlating signals and stopping attacks in real time with minimal human intervention.
- **Cloud based XDR Implementation is Cost and Time effective compared to traditional SoC implementations.**

Next-Gen MFA:

- **Behavioural biometric multi-factor authentication** across employee portals.
- Persistent authentication beyond one-time logins, greatly reducing risk of account takeover or insider impersonation.

NCRTC is among pioneers in India to use AI-driven continuous authentication in rail operations.

NCRTC Cyber Security Initiave Bridging the divide- IT-OT Integration



Key takeaways

ncrtc

- Cost effective Risk Mitigation
- Adherence to International Standards
- Scalability & Future-Readiness: **Industry and Vendor Agnostic**
- **First of its kind Cyber Security Implementation in Railway Sector Domain**
- Tools deployed
  - Unidirectional Gateway with Protocol Conversion
  - USB Scanning Kiosk
  - XDR and EDM for Endpoints
  - AI based Behavioral Biometric MFA

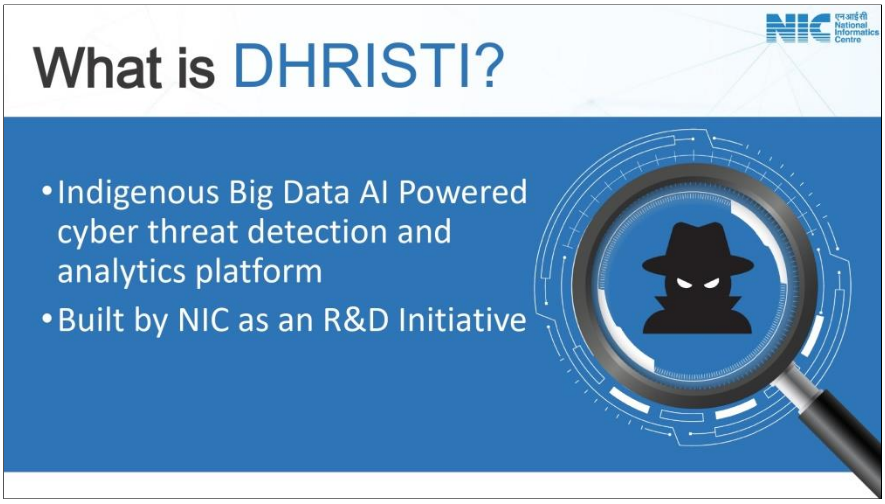
ncrtc

Thank You

4.2. Presentation by Shri M.Hariharan, Joint Director (IT), NIC

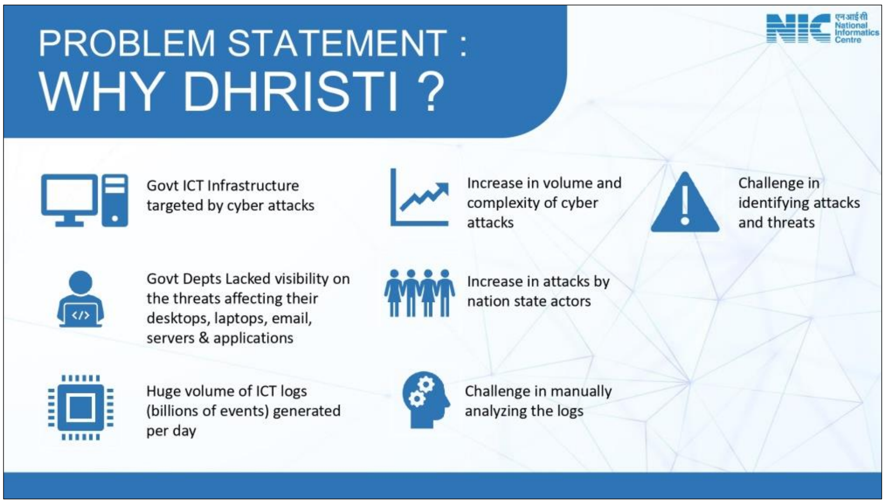
DHRISTI

Data Harmonization for Risk Insights & Security Threat Intelligence



What is DHRISTI?

- Indigenous Big Data AI Powered cyber threat detection and analytics platform
- Built by NIC as an R&D Initiative



PROBLEM STATEMENT : WHY DHRISTI ?

Govt ICT Infrastructure targeted by cyber attacks

Increase in volume and complexity of cyber attacks

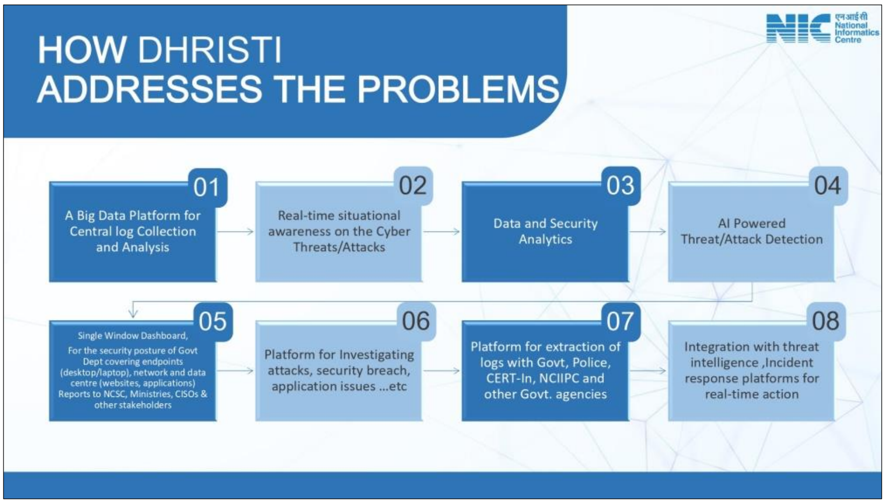
Challenge in identifying attacks and threats

Govt Depts Lacked visibility on the threats affecting their desktops, laptops, email, servers & applications

Increase in attacks by nation state actors

Huge volume of ICT logs (billions of events) generated per day

Challenge in manually analyzing the logs



HOW DHRISTI ADDRESSES THE PROBLEMS

01 A Big Data Platform for Central log Collection and Analysis

02 Real-time situational awareness on the Cyber Threats/Attacks

03 Data and Security Analytics

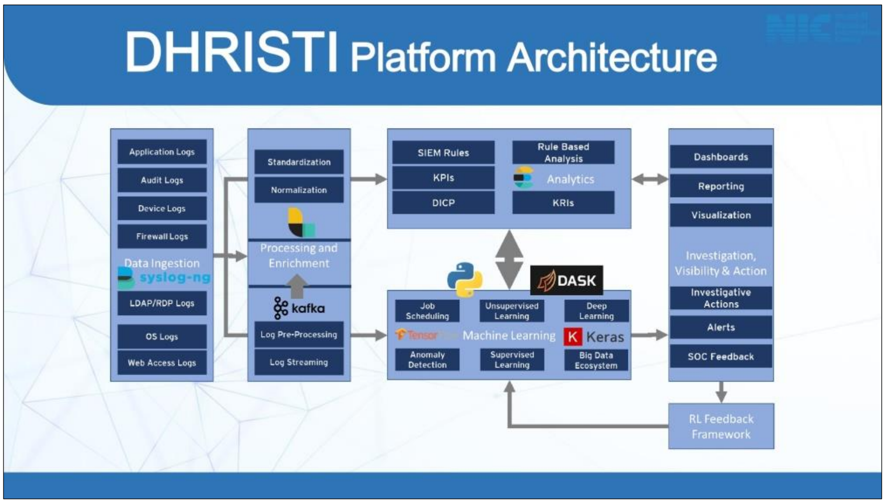
04 AI Powered Threat/Attack Detection

05 Single Window Dashboard, For the security posture of Govt Dept covering endpoints (desktop/laptop), network and data centre (websites, applications) Reports to NCSC, Ministries, CISOs & other stakeholders

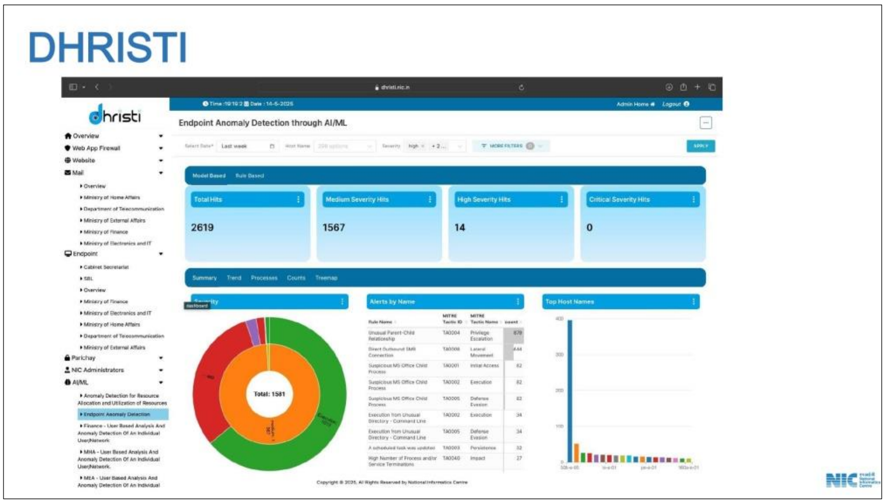
06 Platform for Investigating attacks, security breach, application issues ...etc

07 Platform for extraction of logs with Govt, Police, CERT-In, NCIIPC and other Govt. agencies

08 Integration with threat intelligence ,Incident response platforms for real-time action



DHRISTI Platform Architecture



DHRISTI

dhristi.nic.in
dhristi
Overview
Web App Firewall
Website
Mail
Overview
Ministry of Home Affairs
Department of Telecommunication
Ministry of External Affairs
Ministry of Finance
Ministry of Electronics and IT
Endpoint
Cabinet Secretariat
SBL
Overview
Ministry of Finance
Ministry of Electronics and IT
Ministry of Home Affairs
Department of Telecommunication
Ministry of External Affairs
Parichay
NIC Administrators
AI/ML
Anomaly Detection for Resource Allocation and Utilization of Resources
Endpoint Anomaly Detection
Finance - User Based Analysis And Anomaly Detection Of An Individual User/Network
MHA - User Based Analysis And Anomaly Detection Of An Individual User/Network
MEA - User Based Analysis And Anomaly Detection Of An Individual
Admin Home
Logout
MORE FILTERS
APPLY
Model Based
Rule Based
Summary
Trend
Processes
Counts
Treemap
Severity
Total: 1581
Top Host Names
400
300
200
100
0

Time :19:19:2 Date : 14-5-2025

Endpoint Anomaly Detection through AI/ML

Select Date* Last week

Severity high + 2...

Total Hits 2619

Medium Severity Hits 1567

High Severity Hits 14

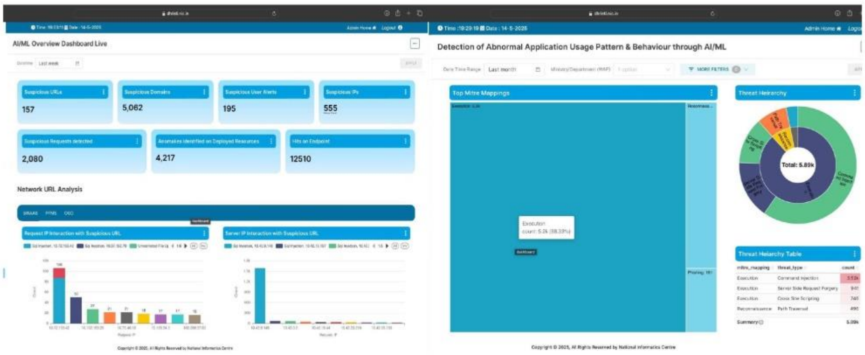
Critical Severity Hits 0

Alerts by Name

Rule Name	MITRE Tactic ID	MITRE Tactic Name	count
Unusual Parent-Child Relationship	TA0004	Privilege Escalation	879
Direct Outbound SMB Connection	TA0008	Lateral Movement	444
Suspicious MS Office Child Process	TA0001	Initial Access	82
Suspicious MS Office Child Process	TA0002	Execution	82
Suspicious MS Office Child Process	TA0005	Defense Evasion	82
Execution from Unusual Directory - Command Line	TA0002	Execution	34
Execution from Unusual Directory - Command Line	TA0005	Defense Evasion	34
A scheduled task was updated	TA0003	Persistence	32
High Number of Process and/or Service Terminations	TA0040	Impact	27

Copyright © 2025, All Rights Reserved by National Informatics Centre

DHRISTI



dhristi.nic.in

Time :19:23:11 Date : 14-5-2025

AI/ML Overview Dashboard Live

Duration: Last week

Suspicious URLs	Suspicious Domains	Suspicious User Alerts	Suspicious IPs
157	5,062	195	555

Suspicious Requests detected	Anomalies identified on Deployed Resources	Hits on Endpoint
2,080	4,217	12510

Network URL Analysis

Request IP Interaction with Suspicious URL

Server IP Interaction with Suspicious URL

Copyright © 2025, All Rights Reserved by National Informatics Centre

dhristi.nic.in

Time :19:29:19 Date : 14-5-2025

Admin Home Logout

Detection of Abnormal Application Usage Pattern & Behaviour through AI/ML

Date Time Range: Last month

Ministry/Department (WAF)

MORE FILTERS

Top Mitre Mappings

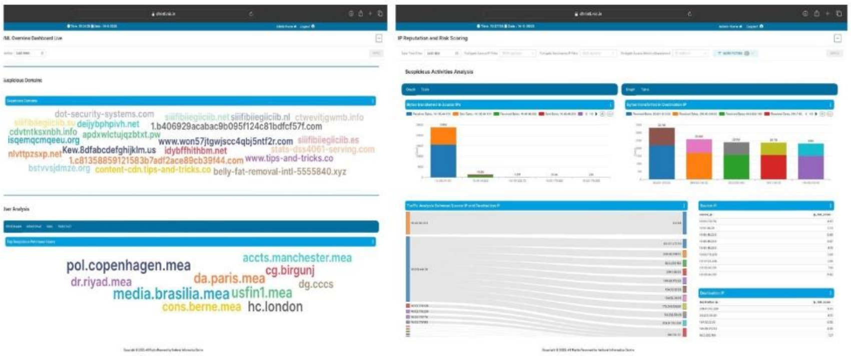
Threat Heirarchy

Threat Heiarchy Table

mitre_mapping	threat_type	count
Execution	Command Injection	3.53k
Execution	Server Side Request Forgery	941
Execution	Cross Site Scripting	740
Reconnaissance	Path Traversal	490
Summary		5.89k

Copyright © 2025, All Rights Reserved by National Informatics Centre

DHRISTI



dhristi.nic.in

AI/ML Overview Dashboard Live

Suspicious Domains

User Analysis

dhristi.nic.in

IP Reputation and Risk Scoring

Suspicious Activities Analysis

Bytes transferred in Source IPs

Bytes transferred in Destination IP

Traffic Analysis Between Source IP and Destination IP

Source IP

Destination IP

DHRISTI KEY METRICS

01 Total volume of data handled by the platform : 2.5 Petabytes

02 Size of the DHRISTI Platform cluster : 150+ data nodes

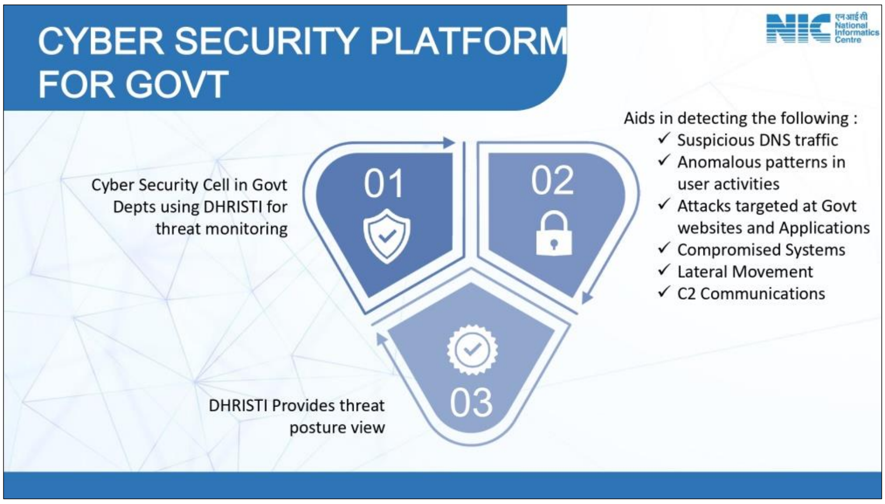
03 Critical Ministries using DHRISTI Platform :

- PMO
- Cabsec
- MHA
- MEA
- MoD

04 Total cyber threats detected during Operation Sindoor : 2.5 Lakhs

05 Total anomalies detected during last 3 months : 15 Lakhs

06 Total pre-threats detected during last 3 months : 8500

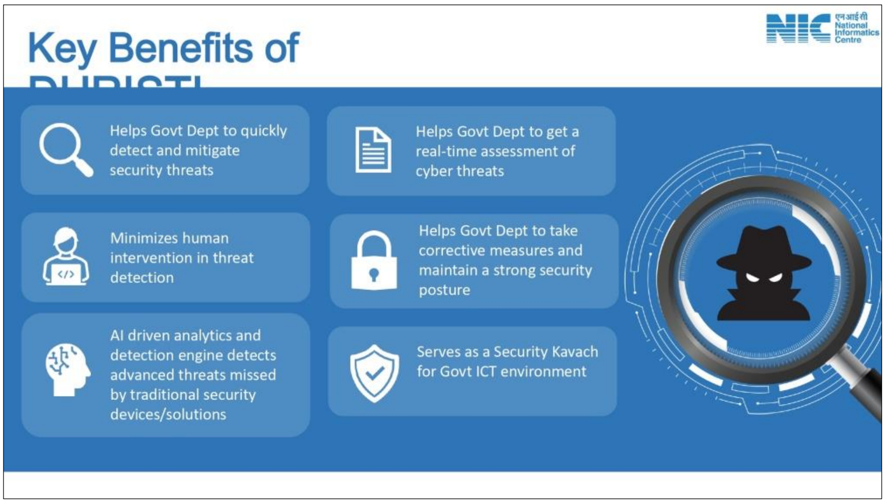


CYBER SECURITY PLATFORM FOR GOVT

Cyber Security Cell in Govt Depts using DHRISTI for threat monitoring

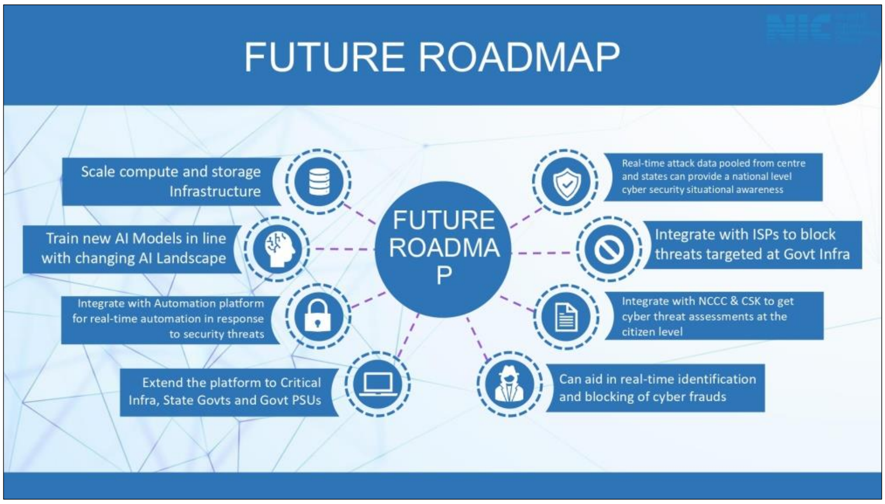
Aids in detecting the following :
- ✓ Suspicious DNS traffic
- ✓ Anomalous patterns in user activities
- ✓ Attacks targeted at Govt websites and Applications
- ✓ Compromised Systems
- ✓ Lateral Movement
- ✓ C2 Communications

DHRISTI Provides threat posture view



Key Benefits of DHRISTI

- Helps Govt Dept to quickly detect and mitigate security threats
- Minimizes human intervention in threat detection
- AI driven analytics and detection engine detects advanced threats missed by traditional security devices/solutions
- Helps Govt Dept to get a real-time assessment of cyber threats
- Helps Govt Dept to take corrective measures and maintain a strong security posture
- Serves as a Security Kavach for Govt ICT environment



FUTURE ROADMAP

- Scale compute and storage Infrastructure
- Train new AI Models in line with changing AI Landscape
- Integrate with Automation platform for real-time automation in response to security threats
- Extend the platform to Critical Infra, State Govts and Govt PSUs
- Real-time attack data pooled from centre and states can provide a national level cyber security situational awareness
- Integrate with ISPs to block threats targeted at Govt Infra
- Integrate with NCCC & CSK to get cyber threat assessments at the citizen level
- Can aid in real-time identification and blocking of cyber frauds

THANK YOU!

एन आई सी
National Informatics Centre

4.3. List of Participants

S. no.	Participant's Name
1	KIPHIRE NAGALAND
2	Social Welfare Deptt. A&N islands
3	25132880685
4	A&N Islands
5	A. K. Bhattacharya
6	ABHISHEK DUBE
7	ABHISHEK KUMAR
8	AC (G) Jalandhar
9	AC to DC Chamba
10	AC to DC Solan
11	AC(G) JALANDHAR
12	AC(G) SBS Nagar
13	ADC RD S.A.S Nagar Mohali
14	ADM JSG
15	ANANTNAG
16	ANI Fisheries
17	AR - WEST SIANG
18	Addl EO ,Khordha
19	Addl CIT R1 Noida
20	Adesto gonda
21	Admfr
22	Administration Charkhi Dadri
23	Ajeet Kumar
24	Akrati Raghuvanshi
25	Amar
26	Amit Bandekar
27	Amit Bandekar - DITE&C, Goa
28	Andaman
29	Arpit Mathur
30	Arun
31	Arun K Markam
32	Ashok Kumar
33	Ashwani Kumar IAS
34	Asish Mohanty
35	Assistant Secretary (AR)
36	Astha Thakur
37	Ayush Tripathi, Executive/Cyber Security, NCRTC
38	BH-BEGUSARAI
39	BLMEENA
40	BRM

41	BS US
42	Bhadradri
43	Bhawana
44	Bikiran Mohapatra, SeMT, Mizoram
45	Budha Ram
46	C Raja Sekhar, D S, GAD, Andhra Pradesh
47	CCPS Vellore
48	CDO Bijnor
49	CDO LALITPUR
50	CEO XP CHITTORGARH
51	CHARKHI DADRI-HR
52	CONTROL ROOM J&K
53	CPO Kurnool
54	CPO Medchal
55	CTM AMBALA
56	CTM FATEHABAD
57	CTM HISAR
58	Collector Rajkot , Gujarat
59	Cyber Cell Karauli
60	D Lato
61	D S S Joshi
62	DAH&VO RIBHOI NONGPOH
63	DARPG STC BOARD ROOM
64	DC - WEST SIANG
65	DC ATP
66	DC CHARKHI DADRI
67	DC OFFICE CHAMBA
68	DC West Siang
69	DDF Ferozepur
70	DDO Basti UP
71	DDeGS
72	DEPUTY COLLECTOR LA SOUTH GOA
73	DHQ DUNGARPUR
74	DHS, A&N Admn.
75	DIO DHUBRI
76	DIO Fatehabad
77	DIO Gwalior
78	DIO KRISHNA
79	DIO KRNAP
80	DIO Kathua
81	DIO NIC Leh
82	DIO Tirap, Arunachal Pradesh
83	DIT

84	DIT Pdy
85	DIT Sikkim
86	DLO JAIPUR
87	DM DHAR
88	DM Dhalai
89	DM OFFICE PATNA
90	DM SOUTH EAST
91	DM UNAKOTI
92	DM West Tripura District
93	DOIT BARMER
94	DOITC Ajmer
95	DOP, Sikkim
96	DPO Begusarai
97	DPO, SHEIKHPURA
98	DPRO Medchal
99	DR SHEEL ASTHANA, JOINT DIRECTOR ARD
100	DSEO Ambala
101	DTC FAZILKA
102	DTDO, Medchal
103	DYSO medchal
104	Damodhar Reddy Yerva
105	DeGM Ashoknagar
106	Deepak (DIO Hisar)
107	Department of Information Technology Govt. of Bihar
108	Dept ITE&C, Govt of Goa
109	Deputy Secretary, GAD, UT Ladakh
110	District Jind
111	District Moga
112	District Sirohi
113	Dr Yuvraj Singh
114	Dr. Tasaduq Hussain
115	Dr.Aruna, ADIT, Daman and Diu
116	Dr.Manjulata Rao, Principal, TGCE
117	Dy.Collector, O/o The Sub-COllector,Panposh
118	EDM BAPATLA
119	EE
120	G kanthamma CEO MEDCHAL MALKAJGIRI
121	GA AR Dept A.P. Secretariat
122	GA Faridkot
123	GAD Off 2
124	GAD,Bihar
125	GM DIC Medchal
126	GOA

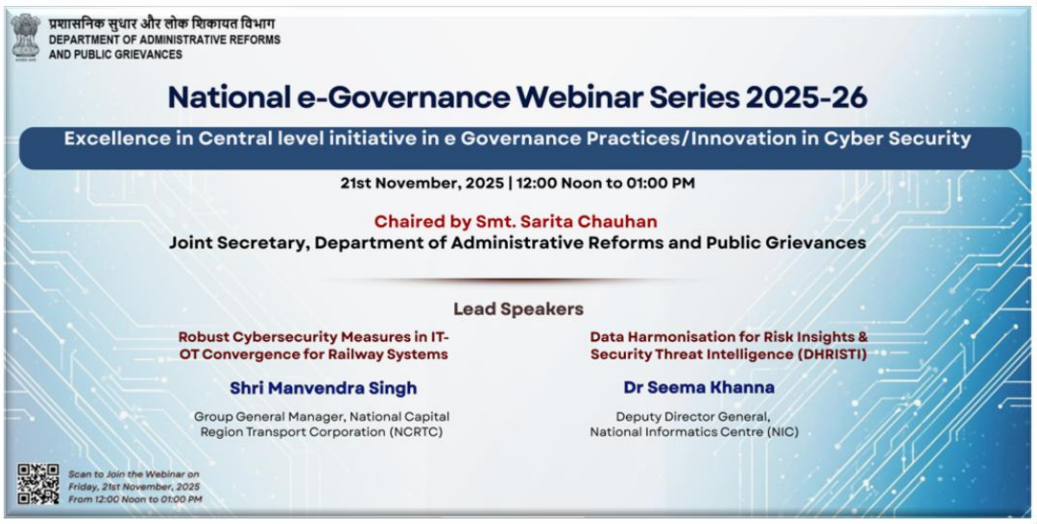
127	Godda
128	Gopinath Narayan (Pr. Secy - IT - Assam)
129	Guest
130	Gurugram - Haryana
131	HARYANA-PANCHKULA
132	HR-BHIWANI
133	HS Nagra
134	Hari Haran M - NIC
135	Head SeMT GNCTD
136	Himanshu Agarwal DoIT Chandigarh
137	IT & C Dept Arunachal
138	IT Branch FGS
139	IT Branch, Rupnagar
140	IT Dept Assam
141	IT ludhiana
142	ITPTK
143	JAMMU - NIC
144	JAP-IT
145	JSG
146	Jaspreet Kaur DTC Malerkotla
147	Jaswant Singh
148	Jhalawar Collectorate
149	Jt. Secy.AR, GoHP
150	Jyoti Gupta
151	KanpurDehat
152	Karimnagar -Telangana
153	Kasturibala Jena
154	Khairthal-Tijara Collectorate
155	LOHARDAGA
156	MAYANK
157	Mahendragarh Haryana
158	Mahima Kaul
159	Maitrayee
160	Malkangiri-OD
161	Malvika DOITC
162	Malvika DOITC Alwar
163	Mandi
164	Mansoor
165	Manvendra Singh GGM/S&T NCRTC
166	Mawkyrwat
167	Mayank Prabha
168	Mayurbhanj-Odisha
169	Md Mukhtar Ali (telangana

170	Medchal Malkajgiri-Telangana
171	Meelu_Senior Fellow (SAS Nagar)
172	Megha Khajuria-J&K
173	Mukhtar Ali (Telangana)
174	Mungeli DMC
175	NAVEESH Y B
176	NIC
177	NIC
178	NIC - KRISHNA - AP
179	NIC Bijnor
180	NIC CHARKHI DADRI
181	NIC Chengalpattu
182	NIC DIO Jammu
183	NIC Dhalai
184	NIC ETAH
185	NIC KANPUR DEHAT UP
186	NIC Keonjhar
187	NIC LALITPUR
188	NIC Ludhiana
189	NIC Medchal-Malkajgiri
190	NIC Narnaul
191	NIC PTA
192	NIC Panna
193	NIC Pathankot
194	NIC Pratapgarh
195	NIC Prayagraj
196	NIC SERCHHIP
197	NIC SHRAVASTI
198	NIC Shravasti
199	NIC Sikar
200	NIC West Singhbhum Jharkhand
201	Naina Khatik
202	Narinder Singh
203	Nic Rampur
204	Nic ludhiana
205	Nodal officer social Welfare Andaman
206	Nongpoh-Meghalaya
207	O/o DMWO
208	OD-Boudh
209	PM HPSDC
210	PS
211	Panchayat Samiti Office, Lephripara
212	Panchkula Haryana

213	Patiala
214	Patna
215	Payal goyal
216	Planning Office
217	Prangshu Deb, SeMT Tripura
218	Pranshuta
219	Pratapgarh-Rajasthan
220	R.L. Solanki
221	RAJBAHADUR
222	Rajat, ADIO Gwalior
223	Ramkesh saini
224	Ranchi
225	Ranjeet Mourya
226	Ratan Kumawat
227	Ravipati Ramanjaneyulu
228	Rinku meena
229	Rinku meena
230	Rohit QCI
231	Rohit salodia dpmu rajsamand
232	Roushan Kumar
233	Rucha Mahale, Head SeMT MP
234	SAHIBGANJ
235	SDM HQ, South-West Delhi
236	SDM Panipat
237	Sadhabi Dehuria,Deputy Collector,Panposh
238	Sanjay Sharma
239	Sdm Rajsamnd
240	Sekhar, SeMT
241	ShO Cyber Crime Kaithal
242	Shankar
243	Shri.Vitthal Shinde GAD Maharashtra
244	Shruti
245	Sikar-Rajasthan
246	Sonali Gupta
247	Sonipat
248	Special Secretary ARI
249	Sundargarh-OD
250	Suraj Kujur
251	Suresh Kumar
252	TN-KANCHEEPURAM
253	TN-Vellore
254	TNeGA
255	TR-SouthTripura

256	Taha
257	Tehniya Abf
258	Tnega
259	Transport Dept AN
260	UK- BAGESHWAR
261	Umsning CRD Block
262	VC Coordinator, DARPG
263	Vivek Sharma, IT Cell J&K
264	Webex
265	West-Tripura
266	ZP,Angul
267	Zilla Parishad, Mayurbhanj
268	adseto aligarh
269	bhuv
270	ccps
271	cpo udaipur
272	drda medchal
273	eDM Prayagraj
274	kavita kumari khichar
275	kavita sharma
276	mainority wellfare
277	nic mirzapur
278	pragati joshi
279	pragya lahoti
280	puneet
281	rajesh kumar m addl secty e&itd GoK
282	samastipur
283	shilpa
284	zp chittorgarh

4.4. Gallery



प्रशासनिक सुधार और लोक शिकायत विभाग
DEPARTMENT OF ADMINISTRATIVE REFORMS
AND PUBLIC GRIEVANCES

National e-Governance Webinar Series 2025-26

Excellence in Central level initiative in e Governance Practices/Innovation in Cyber Security

21st November, 2025 | 12:00 Noon to 01:00 PM

Chaired by Smt. Sarita Chauhan
Joint Secretary, Department of Administrative Reforms and Public Grievances

Lead Speakers

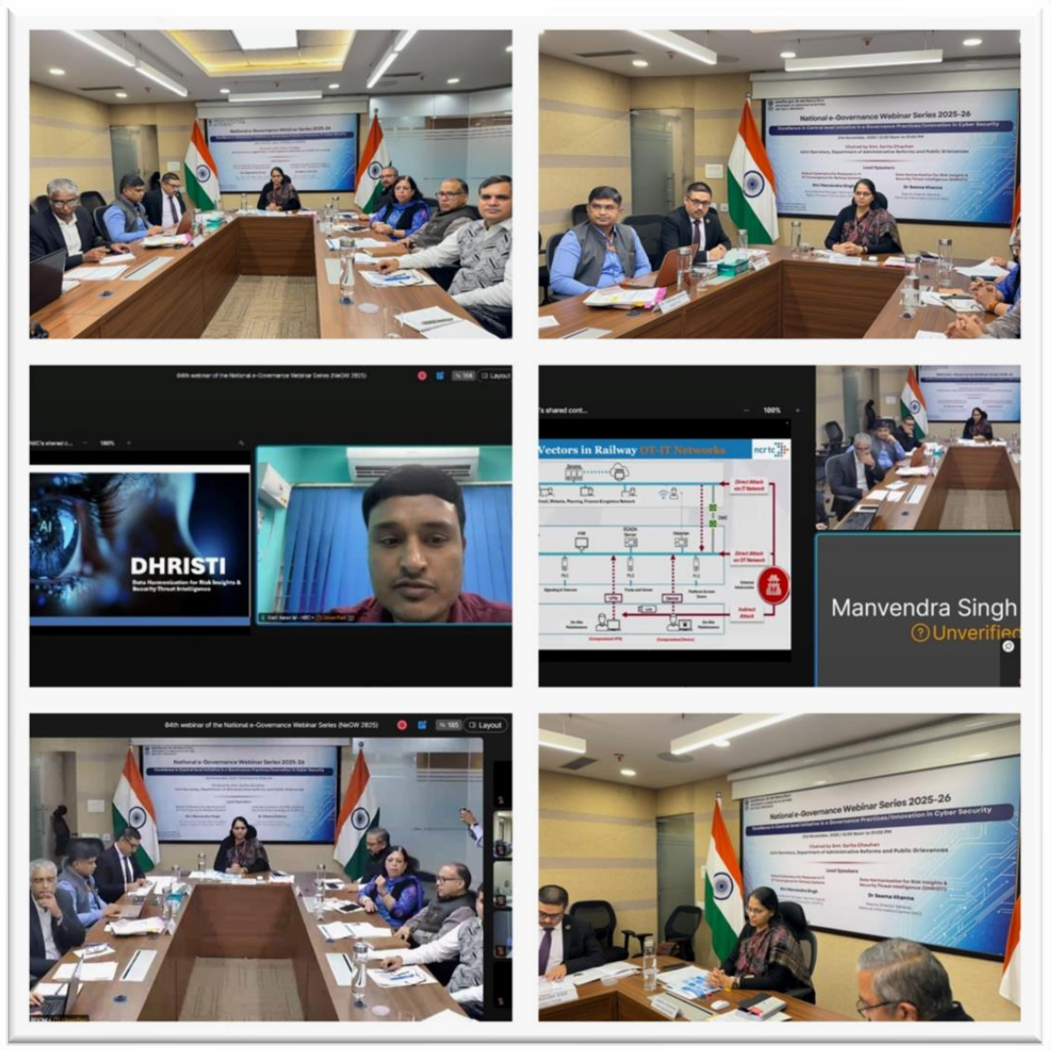
Robust Cybersecurity Measures in IT-OT Convergence for Railway Systems

Shri Manvendra Singh
Group General Manager, National Capital Region Transport Corporation (NCRTC)

Data Harmonisation for Risk Insights & Security Threat Intelligence (DHRISTI)

Dr Seema Khanna
Deputy Director General,
National Informatics Centre (NIC)

Scan to Join the Webinar on
Friday, 21st November, 2025
From 12:00 Noon to 01:00 PM


64th webinar of the National e-Governance Webinar Series (NeGW 2025)
DHRISTI
Data Harmonisation for Risk Insights & Security Threat Intelligence
Vectors in Railway OT-IT Networks
ncrtc
Manvendra Singh
Unverified
National e-Governance Webinar Series 2025-26

सत्यमेव जयते

Department of Administrative Reforms & Public Grievances
Ministry of Personnel, Public Grievances & Pensions
Government of India