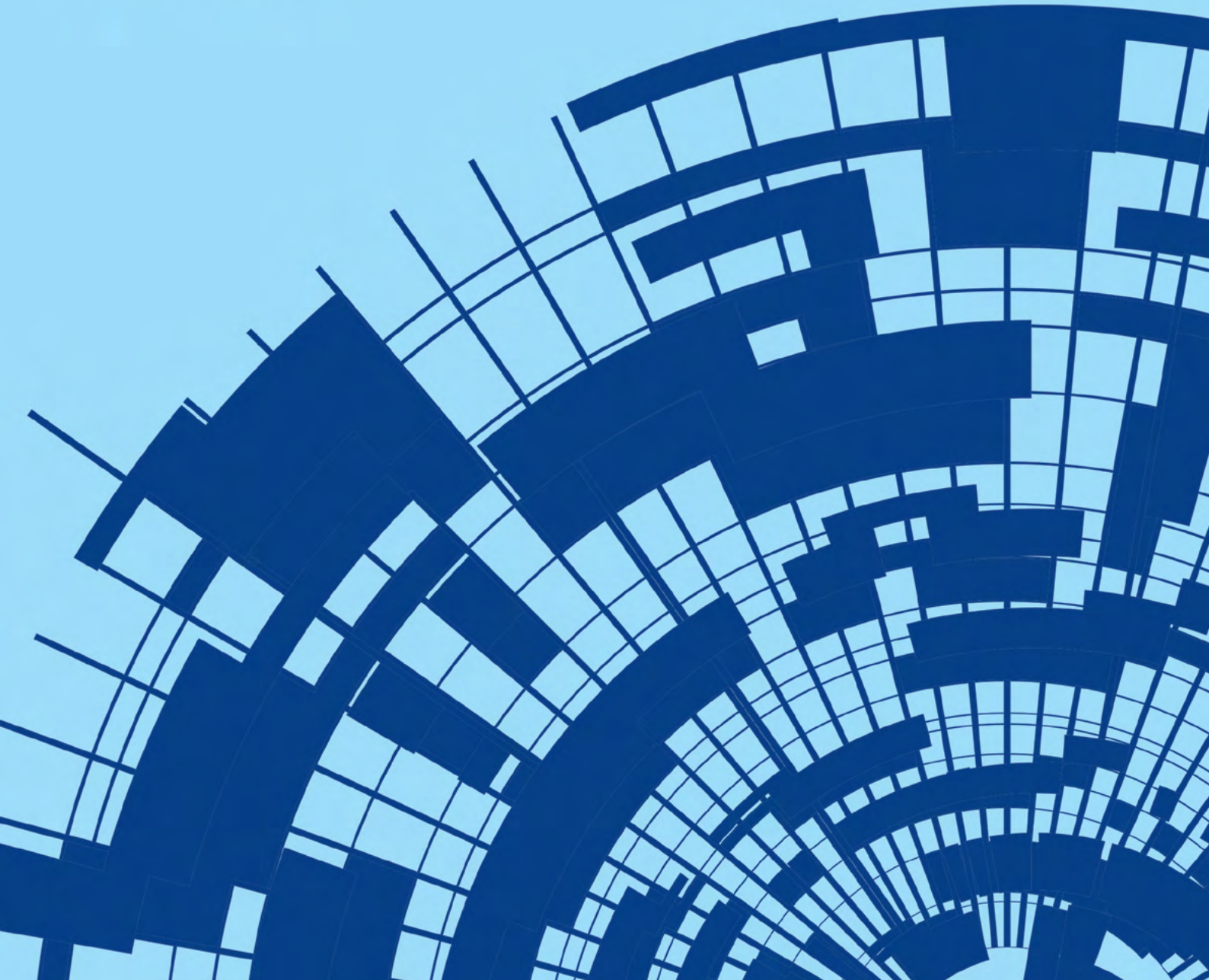
DSCI
PROMOTING DATA PROTECTION

Honeywell

OPERATIONAL TECHNOLOGY

SECURITY OPERATIONS CENTRE



Contents

Executive Summary

In this context, the OT Security Operations Centre (OT SOC) has emerged as a strategic capability to move from reactive, audit-driven practices to continuous, risk-based monitoring and response. This report outlines three pragmatic OT SOC operating models: Separate, Hybrid, and Converged.

Industrial sectors in India, especially power, manufacturing, oil & gas, transport, and utilities, are rapidly digitizing to improve operational efficiency, reliability, and remote management. As a result, **Operational Technology (OT) environments are getting interconnected with Information Technology (IT) and cloud systems**, dissolving traditional air-gaps and expanding the cyber-attack surface across critical infrastructure. While modernization unlocks productivity, it also heightens exposure to ransomware, supply chain compromise, credential abuse, and targeted cyber-physical attacks that can disrupt production or endanger safety.

In this context, the **OT Security Operations Centre (OT SOC)** has emerged as a strategic capability to move from reactive, audit-driven practices to continuous, risk-based monitoring and response. This report outlines **three pragmatic OT SOC operating models: Separate, Hybrid, and Converged**. It also defines the building blocks of a secure OT SOC foundation, including Secure Architecture and Network Segmentation, Asset Inventory, Vulnerability Management and sector-specific Threat Intelligence.

The report further examines the **critical challenges organizations encounter during OT SOC implementation**. Where possible, it highlights practical solutions, including the role of AI and automation in bridging analyst skill gaps, reducing alert noise, and supporting faster, safer response at the operational layer.

Finally, the report provides a **way forward** for utilities, plant operators, technology vendors, and regulators. This includes aligning regulatory requirements with capability building, improving cross-sector knowledge sharing, establishing clear governance models between IT and OT teams and enabling international collaborations in OT cybersecurity.

Introduction

OT devices and systems spanning power, manufacturing, utilities, transportation, and critical infrastructure are vital to India's industrial ecosystem. Once isolated, these systems now converge with IT networks, Industrial IoT (IIoT), and cloud platforms, dramatically expanding cyber-attack surfaces. As digitalization accelerates, securing OT systems has become a board-level risk management priority, not just a regulatory requirement. Unlike IT, OT demands 24/7 uptime, involves legacy systems, and manages safety-critical processes, requiring specialized SOCs.

OT SOCs provides real-time monitoring, intrusion detection, threat hunting and incident response but must address unique challenges: decentralized architectures, heterogeneous devices, skills gaps, and extended maintenance cycles. As Indian organizations pursue digital transformation under **Central Electricity Authority (Measures Relating to Cybersecurity in Power Sector) Directions, 2021[1], National Critical Information Infrastructure Protection Centre (NCIIPC), Computer Emergency Response Team – India (Cert-In) and Computer Security Incident Response Team (CSIRT) mandates**, understanding OT SOC models, architecture, and solutions is essential for operational resilience and safety.

OT Security Landscape

India's OT security landscape is undergoing rapid change as power, manufacturing, and transport systems converge with IT and cloud platforms under national digitization programs. While this integration improves efficiency and remote operations, it also expands the attack surface across critical infrastructure.

Foundation	Legacy Systems in OT	A sizeable proportion of OT assets are legacy and unsupported (industry analyses commonly cite a multi-decade device lifespan and high legacy prevalence; with estimates in literature range in the tens of percent).
	Foundational Readiness	Low adoption maturity amongst utilities and large manufacturers; the most targeted sector was manufacturing at 17% as both nation-state actors and Ransomware-as-a-Service (RaaS) cybercriminals continue to capitalize on vulnerabilities.[2]
Attack Landscape	Prominent Threat Vectors in OT/ICS Attacks	Removable-media scans across India's OT/ICS environments detected a wide spectrum of malware including ransomware, credential-stealers, remote-access trojans, lateral-movement frameworks, worms, and ICS-reconnaissance tools highlighting the diverse and evolving threat surface industrial systems face.[3]
Organizational Capability	Cybersecurity Talent Shortage	A severe shortage of OT-specialist practitioners exists; industry estimates for cybersecurity talent gaps are large (India estimates discuss shortfalls in the hundreds of thousands to ~1M cybersecurity professionals overall), and OT roles routinely show extended hiring timelines (often many months).
	SOC Adoption in India	Large central utilities have been early adopters/pilots of OT SOCs; many state DISCOMs and smaller operators lag in SOC capability (survey evidence suggests a small minority of smaller utilities have mature SOC capabilities)

Operational	Visibility Across OT Assets	As more security solutions are applied and combined IT and OT teams collaborate, there is also a decline in those identifying 75% visibility within the organization's central cybersecurity operations.[4]
Advanced Technology	AI & Automation	Many organizations are deploying AI/ML-based tools in SOC operations. For example, 59% of respondents in a 2025 survey reported that their SOC's efficiency had been moderately or significantly boosted by AI[5].
Governance	Regulatory Directions/ Frameworks and Standards	CEA 2021 Directions: SOC monitoring, IT/OT segregation, periodic audits; adoption uneven across utilities; ISA/ IEC 62443; ISO 27001; ISA 95; CSIRT guidelines, Cert-In guidelines.

In 2025, global ransomware extortion incidents rose by 46% compared to 2024[6], with India emerging as the most targeted country in Asia, particularly across manufacturing, technology, and healthcare sectors[7].

The talent gap amplifies these risks. India faces a severe shortage of OT cybersecurity professionals, mirroring global trends. Although the NCIIPC and the Ministry of Power are training engineers through sectoral programs, the supply of qualified OT security practitioners remains limited, with most organizations relying on system integrators or managed service providers.

Regulatory efforts are gaining strength, but adoption remains uneven. However, **implementation maturity varies significantly** between central generation utilities, state DISCOMs, and private players. While large entities have begun establishing centralized OT SOCs, smaller utilities often view compliance as a checkbox exercise rather than a risk management priority. India's OT security posture reflects an ecosystem in transition: from awareness to capability-building.

Three Key Limitations of OT Security

OT environments face unique constraints that make their cybersecurity posture fundamentally different from IT. These limitations span financial, human resource, and operational dimensions, and together they shape the challenges of establishing effective OT SOCs in India.

Financial Challenges

- OT security receives a disproportionately small share of the cybersecurity budget (typically <20%).
- Investments are often project-specific (audit/compliance-driven) rather than programmatic.
- Limited funding for advanced OT SOC capabilities, such as AI-enabled monitoring or integrated threat intelligence.
- Capital approval processes prioritize operational upgrades or equipment modernization over cybersecurity.

Personnel Challenges

- Shortage of specialists with dual expertise in industrial control systems and cybersecurity.
- Hiring cycles for OT security professionals extend 9–12 months on average.
- Existing IT security personnel often lack OT domain knowledge, requiring reliance on system integrators or managed services.
- Training initiatives are time-intensive, limiting the company's ability to scale its OT SOC.

Operational Challenges

- OT infrastructure cannot accommodate rapid changes without risking production downtime.
- Industrial equipment operates 24/7, with long maintenance windows and high tolerance constraints.
- Security measures (firmware updates, network segmentation) require extensive planning and coordination.
- Difficult for OT SOCs to standardize detection, enforce controls uniformly, and coordinate incident response across plants because decentralized sites run equipment from multiple OEMs.

These challenges highlight the need for **dedicated OT SOCs, process-aware monitoring, and a risk-based approach** to secure critical industrial operations while maintaining continuity and safety.

The Evolving Threat Landscape and Digitization Pressures

IT-OT convergence is reshaping India's industrial cybersecurity, driving efficiency while expanding attack surfaces. Digitalization initiatives in power, manufacturing, and infrastructure integrate cloud analytics, AI optimization, and remote monitoring.

Globally, there's a shift from compliance-driven to resilience-focused strategies emphasizing risk-based OT SOCs, real-time monitoring, and joint IT-OT governance. While India's large utilities and manufacturers pilot centralized SOCs and AI-driven monitoring, most industrial sites, especially smaller DISCOMs and medium manufacturers, remain reactive and compliance-focused, vulnerable to evolving threats. Effective defense demands holistic strategies combining real-time asset visibility, proactive threat intelligence, and industrial-grade incident response, failing to integrate these risks of operational disruption, safety incidents, financial losses, and regulatory non-compliance.

Over 40 distinct malware families were detected and blocked through USB scanning across Indian critical infrastructure environments, including ransomware, credential-stealers, OT-pivoting frameworks, and ICS reconnaissance tools.[3]

Trojans were the most dominant malware class observed in India's OT/ICS environments, with variants like Wacatac, Ghanarava, Phak, and Crypren frequently detected on engineering and SCADA systems signalling sustained attacker interest in gaining persistence and remote control within industrial networks.[3]

OT SOC Models and Architecture

OT systems are responsible for physical processes such as manufacturing, energy distribution, and water management that requires continuous uptime and have historically been isolated from the internet. The increasing integration of IT systems, cloud analytics, and Industrial IoT has eroded this isolation, making OT SOCs indispensable for real-time visibility and incident response across industrial control networks.

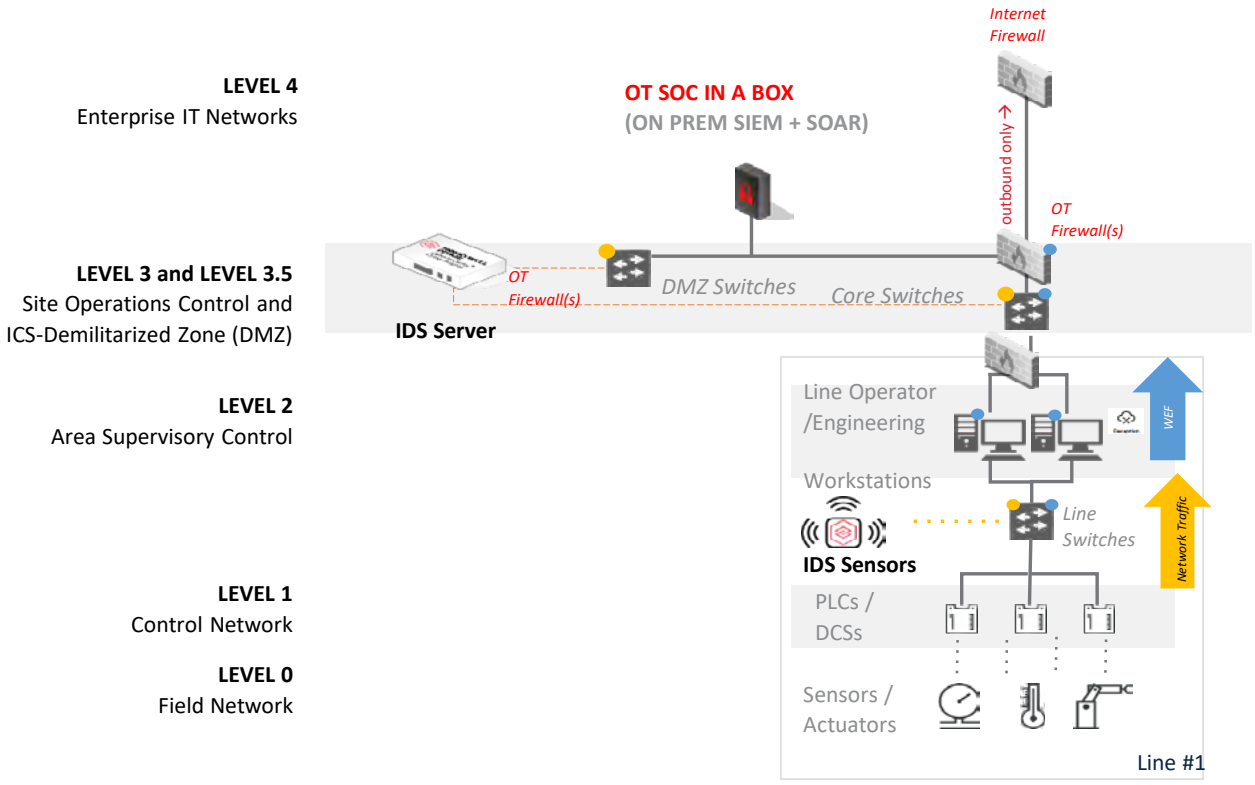
OT SOC Models

On-Prem OT SOC-in-a-Box

Operates independently from IT SOCs with dedicated analysts, infrastructure, and OT-specific monitoring tools for SCADA, DCS, and PLC networks.

Typically adopted by critical infrastructure sectors (oil and gas, power, transportation) requiring operational safety isolation, it provides maximum control and risk separation but incurs high capital and staffing costs.

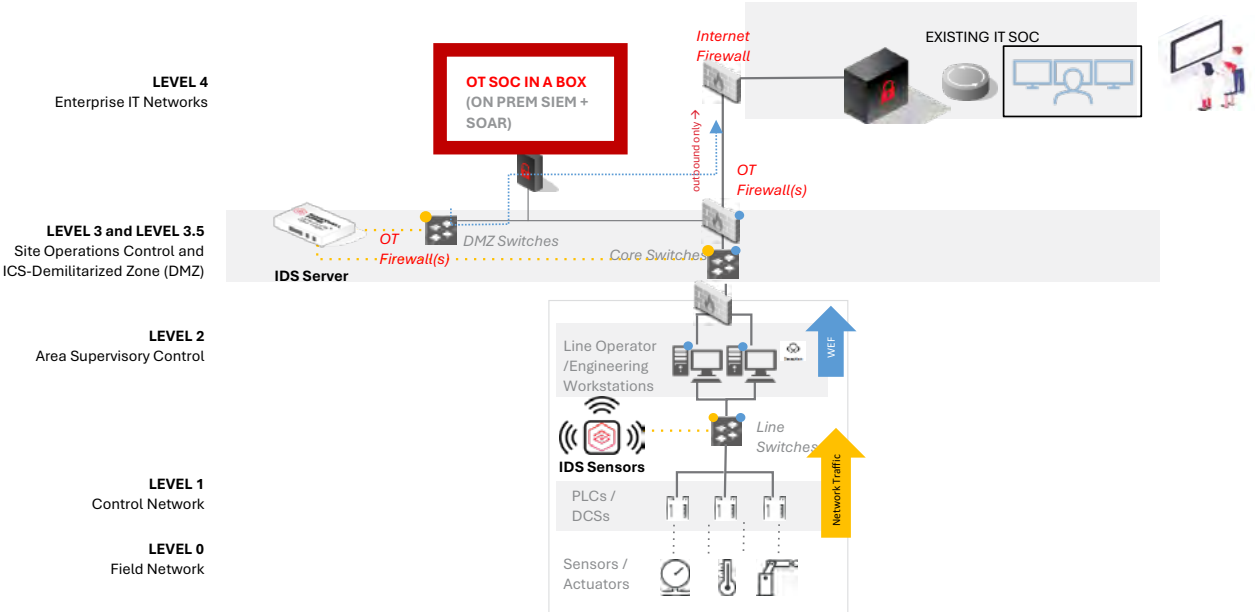
Design Architecture



Hybrid Integrated IT-OT SOC

Combines an existing IT SOC with a parallel OT SOC (internal or managed service provider) under shared governance but separate monitoring environments due to differing tooling, data formats, and response timelines. This enables phased convergence, maintaining operational safety while fostering shared visibility, knowledge exchange, aligned incident correlation, risk dashboards, and reporting as OT-specific playbooks develop.

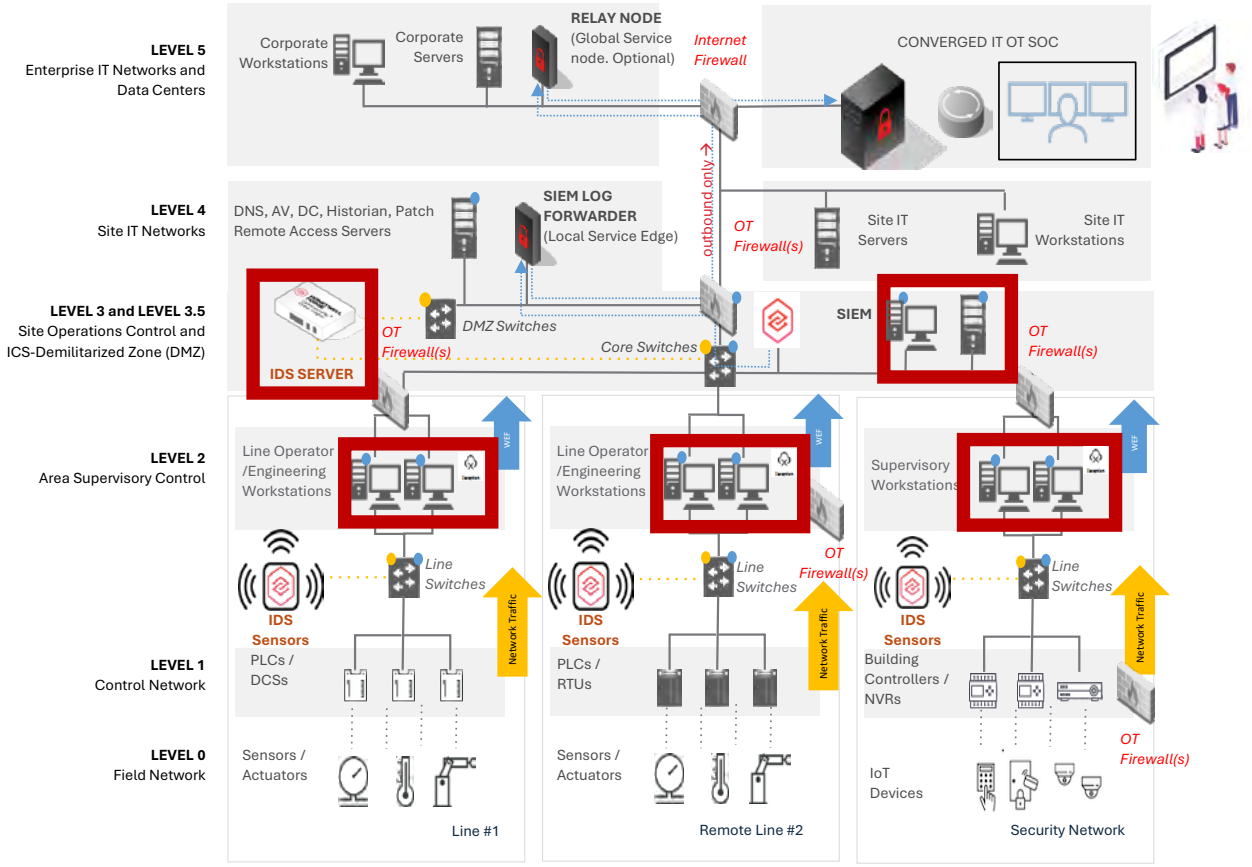
Design Architecture



Converged Managed SOC

The Converged SOC unifies IT and OT monitoring under single governance, process, and technology frameworks while maintaining logical separation between visibility layers. It centralizes incident triage, analytics, and threat hunting, enabling end-to-end situational awareness and correlation of attacks crossing IT-OT boundaries (e.g., ransomware spreading from IT email to industrial networks). Increasingly adopted by large manufacturers pursuing enterprise-wide cyber resilience, but may prove challenging to govern as the IT and OT technological frameworks, playbooks and incident management are converged.

Design Architecture: Automated Flow of Incident Response



Building Blocks of OT SOC (Secure Foundation)

1. Secure Architecture and Network Segmentation

At the heart of OT SOC infrastructure is a **secure network architecture** that enforces segmentation between different layers. This segmentation prevents lateral movement of threats between IT and OT environments while allowing controlled data flows through **Demilitarized Zones (DMZs)** and **firewalled conduits**.

- **Implementation Aspects:**
  - Segregate control, supervisory, and enterprise networks using VLANs, firewalls, and industrial demilitarized zones (iDMZs).
  - Deploy **Industrial Intrusion Detection Systems (IDS)** and **Network Monitoring Tools** within Level 2–3 networks for continuous visibility.
  - Enforce r**ole-based access control (RBAC)** and **least privilege policies** to restrict access to OT assets.
- **Outcome:** This segmentation ensures that even if an enterprise network is compromised, attackers cannot directly access control systems or programmable logic controllers **(PLCs).**

2. Asset Discovery and Vulnerability Management

A comprehensive OT SOC must maintain **real-time visibility of all connected assets** including **PLCs, HMIs, SCADA servers, RTUs, and sensors** across all Purdue layers. OT environments often include legacy devices with long operational lifespans and limited security features, making **asset inventory and vulnerability management crucial**.

- **Implementation Aspects:**
    - Employ **passive discovery tools** to map assets and communication patterns without disrupting production.
    - Integrate **vulnerability databases** and **vendor advisories** into SOC threat intelligence workflows.
    - Conduct **regular patch assessments** and deploy updates during controlled maintenance windows to minimize downtime.
- **Outcome:** Enables proactive detection of outdated firmware, unpatched systems, and unauthorized devices, significantly reducing the attack surface.

3. Threat Intelligence and Defence-in-Depth

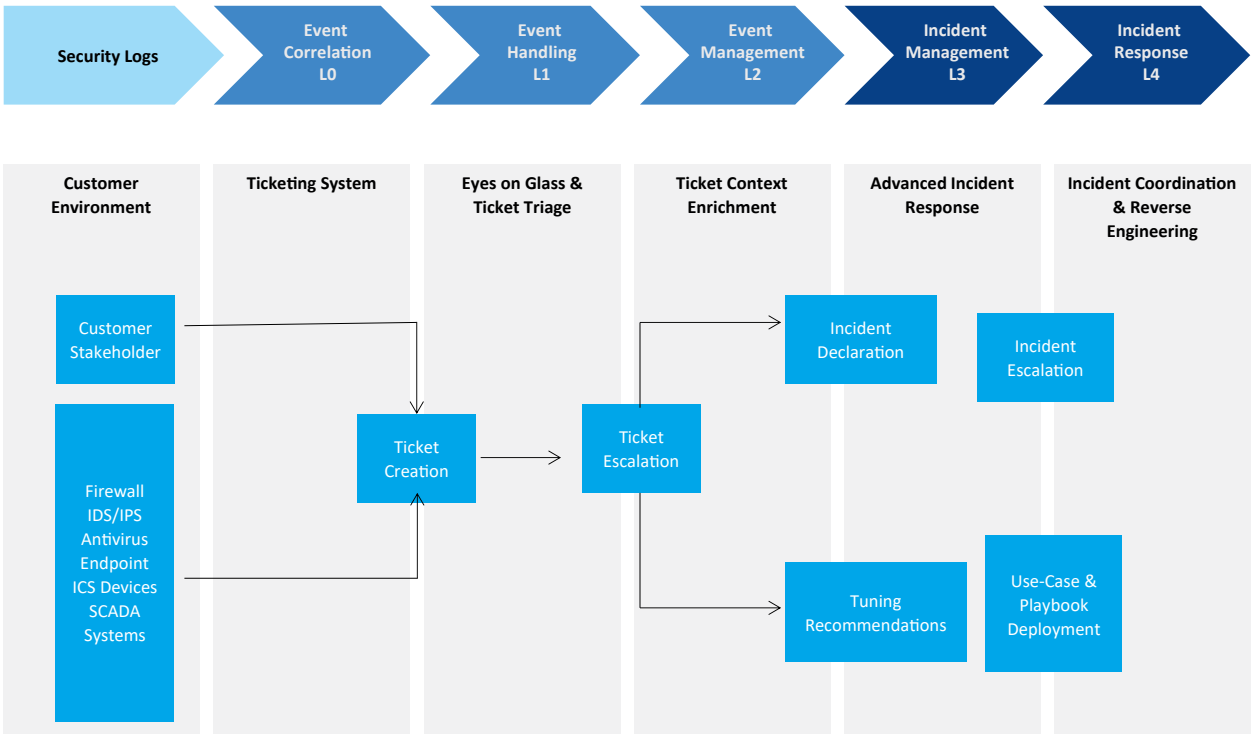
The **defence-in-depth** approach within an OT SOC ensures that multiple, overlapping security layers protect the environment. By integrating **threat intelligence** specific to industrial control systems, the SOC can identify early indicators of compromise and contextualize them within the OT process.

- **Implementation Aspects:**
    - Ingest **ICS-specific threat feeds** (e.g., from CERT-In, or industry partners) and correlate them with real-time alerts.
    - Deploy **behavioural analytics and anomaly detection** powered by AI/ML models that leverage predictable OT network patterns.
    - Establish **incident playbooks** tailored to OT attack scenarios such as ransomware propagation, firmware tampering, or remote access abuse.
- **Outcome:** Strengthens predictive and preventive capabilities, allowing faster containment and minimizing operational disruption during security incidents.

Each building block works in tandem to provide **resilience, situational awareness, and operational continuity**. This structured foundation ensures that the OT SOC not only monitors but also fortifies critical industrial systems against the evolving landscape of cyber threats.

In OT security operations, incident response must be fast, accurate, and safe for ongoing industrial processes. Manual workflows are no longer sufficient as threats can spread quickly across converged IT–OT networks. To keep pace, industrial SOCs are adopting automated and semi-automated response models that streamline alert triage, enrichment, escalation, and remediation. This reduces analyst burden, improves detection quality, and ensures responses are consistent and aligned with operational constraints, enabling faster containment and stronger resilience across distributed plants and critical infrastructure.

Diagram: Automated Flow of Incident Response



OT SOC Implementation
Challenges and Solutions

Building an OT SOC is not a purely technological pursuit, it is a socio-technical transformation that demands new governance, cross-domain skills, and real-time operational resilience. While convergence with IT SOCs promises unified visibility and faster response, the journey to establishing a functional OT SOC is fraught with structural, human, and technical challenges.

	Challenges	Solution
Single SPOC	80% of OT incidents require on-site action, but central SOC analysts lack authority and visibility. Undefined site contacts cause containment delays and extended response times.	Designate trained site personnel as SPOCs. Deploy AI-powered orchestration to auto-route alerts by asset location, incident type, and risk score for IT-OT coordination.
Governance & Decision-Making	Blurred boundaries between IT, OT, and vendors create confusion over incident approval, patching, and modifications. Vendors may delay response, creating blind spots.	Develop site-specific decision matrices within central governance defining authority levels, vendor escalation, and emergency workflows. Use AI to map asset-vendor-process dependencies and flag conflicts.
OT Knowledge Gap	IT-trained analysts lack OT protocol exposure, safety constraints, and asset criticality understanding, causing alert misinterpretation (e.g., benign PLC restart vs. process disruption).	Establish OT training programs with shop-floor shadowing. Hire analysts with plant experience. Deploy AI-powered virtual simulators, digital-twin environments, and knowledge graphs linking process variables to security alerts.
Monitoring & Visibility	IT tools miss OT-specific telemetry. Legacy protocols create 20x asset discovery gaps. Many plants lack Industrial IDS, leaving control systems opaque.	Deploy Industrial IDS with deep-packet inspection for Modbus, DNP3, PROFINET. Use AI-based anomaly detection and time-series analysis for behavioral deviations and low-and-slow threats. Test in OT labs first.

	Challenges	Solution
Log Quality & Access	OT architectural diversity prevents consistent log collection. Non-critical data floods SOCs while PLCs, RTUs, HMIs lack standardized logging. Poor signal-to-noise overwhelms analysts.	Implement edge-level data cleaning pre-forwarding. Fine-tune Industrial IDS for coverage-manageability balance. Use AI filtration and prioritization learning from historical patterns.
Response Playbooks	Generic IT playbooks ignore OT constraints like safety interlocks, manual overrides, and downtime risks, causing uncoordinated responses endangering safety or production.	Develop OT-specific playbooks detailing procedures, contact hierarchy, isolation/rollback, vendor communication, and restoration. Use AI automation for containment execution, playbook recommendations, and workflow refinement.
Leadership & Budget	Leaders underestimate OT cyber risk as operational vs. strategic. Limited cross-departmental budget pooling delays in SOC implementation.	Position OT security as business resilience, not just compliance. Conduct CISO shop-floor sessions contextualizing vulnerabilities. Aggregate departmental budgets and use AI risk quantification expressing threats financially with ROI and loss projections.

Role of AI in Overcoming OT SOC Challenges

AI has emerged as a key enabler for addressing the resource, capacity, and skill bottlenecks plaguing OT SOCs.

- **Skill Augmentation:** AI-driven simulation labs and adaptive training engines accelerate upskilling of SOC analysts in OT protocols and process safety.
- **Operational Efficiency:** Predictive analytics, anomaly detection, and automated response tools reduce analyst workload and improve detection accuracy.
- **Capacity Building:** AI-based orchestration allows smaller or resource-constrained industries to operate hybrid or "SOC-in-a-Box" models effectively, democratizing industrial cybersecurity readiness.

Technology and Best Practices for OT SOC Operations

A robust OT SOC must be designed to address both technological and operational maturity gaps, particularly at the L1 (Monitoring) and L2 (Analysis and Response) levels.

Technology Practices

1. **Mandatory Tooling:** Industrial IDS are the cornerstone of OT monitoring. They passively observe industrial protocols (Modbus, DNP3, OPC-UA, etc.), detect deviations in expected communications, and correlate them with known attack signatures.
2. **Integration of AI/ML for Prioritization and Automation**
    - **Predictive Insights:** Detect anomalies that deviate from expected PLC-to-HMI communications.
    - **Alert Prioritization:** Rank alerts by operational criticality (e.g., a network anomaly affecting a safety PLC will automatically be flagged higher).
    - **Automated Correlation:** Merge IDS alerts, engineering logs, and maintenance events to identify whether an incident is benign (maintenance-related) or malicious.
    - **Outcome:** Reduces analyst fatigue and accelerates root cause analysis while maintaining process safety.
3. **Testing in an OT Laboratory Before Deployment:** Before implementing any new security tools or patches, testing them in a simulated OT environment or cyber range is essential.
    - **Capability Building:** Lab environments double as training grounds for SOC analysts and engineers to simulate real-world attack and defence scenarios.
4. **Capability Building and Addressing L1–L2 Gaps:**

L1 Gaps: Limited contextual understanding of industrial processes; analysts often misclassify alerts due to lack of operational awareness.

L2 Gaps: Difficulty in conducting root cause analysis because of unfamiliarity with proprietary protocols, PLC programming logic, and safety implications.

Capability Building Measures

- **Cross-Skilling**: Upskill IT SOC analysts with OT process knowledge and basic engineering concepts (PLC operation, SCADA logic).
- **Hands-On Labs**: Use OT testbeds for experiential learning.
- **Joint Response Teams**: Establish integrated IT–OT response groups where cybersecurity analysts work closely with control engineers.
- **Vendor-Agnostic Training**: Encourage training programs aligned to standards like **IEC 62443, NIST SP 800-82**, and **ISA/IEC 61511**.

AI's Role in Bridging Gaps

- **L1 Augmentation:** AI-enabled alert triage systems can reduce the cognitive load on analysts by automatically classifying alerts into high, medium, or low operational impact categories.
- **L2 Assistance:** AI-driven incident reasoning engines can contextualize alerts by referencing historical events, asset criticality, and PLC communication logs,helping L2 analysts identify root causes faster.
- **Knowledge Transfer:** AI chat-assistants integrated within SOC platforms can provide real-time procedural guidance to junior analysts based on playbook recommendations.

Developing a high-functioning OT SOC requires a combination of **fit-for-purpose technologies** (IDS, AI-driven analytics, testbeds) and **structured capability enhancement** (cross-training, simulation, playbook refinement).

Best Practices Framework

The following framework outlines how the human, procedural, technological, and communication dimensions must align to sustain continuous monitoring, rapid incident handling, and long-term security maturity within OT environments.

People

- **Dedicated Training:** SOC analysts must be trained not only in cybersecurity fundamentals, but also in OT domains, plant process operations, and the specific cybersecurity requirements of OT environments.
- **Strong SOC-to-Site Communication:** A SOC cannot operate in isolation. Site engineers, maintenance teams and plant operations must have clear communication channels with the SOC, including defined SPOCs and escalation lists.
- **Engineering Background Preference:** When staffing an OT SOC, preference should be given to individuals with plant/automation experience (e.g., control system engineers) who understand process safety, operational constraints and industrial protocols. The unique nature of OT demands this combination of cybersecurity skill and domain knowledge.

Process

- **Dedicated OT Procedures:** OT environments cannot simply reuse IT SOC playbooks. Procedures must reflect OT realities like safety constraints, maintenance windows, process dependencies.
- **Cross-Site Knowledge Sharing:** For organizations with multiple plants or sites, SOC workflows must include cross-site incident sharing, threat-intelligence dissemination and lessons-learned databases to reduce repeat incidents.
- **Systematic Fine-Tuning:** Industrial IDS, AI/ML models, detection rules and alert thresholds must be regularly fine-tuned based on feedback from the SOC and site engineers. As noted by Automation.com in their article on OT/ICS cybersecurity, continuous configuration and monitoring of change-data integrity is a best practice.

Technology

- **Industrial IDS & OT-Specific Tools:** The monitoring stack must include sensors tailored for OT (protocol decoding, process anomaly detection), edge collectors for telemetry normalization, and integration into central SOC workflows.
- **Clean Data at Source:** OT telemetry is often voluminous and noisy, the framework should therefore deploy data-cleaning closer to the plant (edge preprocessing) so that the SOC receives high-value, normalized events rather than raw flood of logs. Trout Software emphasizes the need for filtering and originating data close to production.

Communication

- **IT - OT/Engineering:** One of the key friction points in OT SOCs is the misalignment between IT security teams and OT engineering/operations. TechTarget highlights the need to place OT cybersecurity under the CISO's remit to ensure unified strategy.
- **Cross-Site Incident Sharing:** Alert and incident information from one site may be relevant elsewhere. The SOC should operate as a knowledge hub, enabling peer learning and threat-intelligence transfer among sites.
- **Industry Peer Collaboration:** Beyond internal communication, organizations should engage in industry-sector ISACs, share threat intelligence, and collaborate on OT-specific cyber exercises. Security Boulevard highlights the value of collective intelligence in the OT SOC context.

Conclusion and Path Forward

Modern OT SOCs serves as industrial resilience nerve centres, integrating situational awareness, incident response, and cross-domain coordination beyond detection to encompass strategic intelligence, business continuity, and national critical infrastructure protection. As sophisticated threats like state-sponsored attacks, supply-chain intrusions and industrial ransomware escalate, countries are repositioning OT cybersecurity as integral to national security doctrine.

Strategic Positioning of SOCs for Global and India's Resilience

Globally, **SOCs are becoming the first line of defense in the cyber-physical battlespace**.

A Security Operations Centre for India's future should be envisioned as a **three-tiered ecosystem**:

- **Sectoral SOCs** (Energy, Transport, Manufacturing, etc.) acting as coordination hubs.
- **Regional SOC Nodes** providing shared monitoring for small and mid-sized utilities.
- **National Cyber Fusion Centre**, integrating situational awareness, analytics, and coordinated response across all sectors.

Positioned strategically, it can **fortify India's industrial competitiveness** by ensuring reliability, safety, and trust.

Operational and Collaboration Recommendations for Stakeholders

Operational Recommendations

- Deploy **industrial-grade IDS**, asset discovery tools, and passive monitoring for visibility across PLCs, SCADA, and HMIs.
- Implement **AI-based analytics and correlation engines** that can distinguish between normal industrial process fluctuations and genuine cyber anomalies.
- Develop domain playbooks for IT and OT incident response, with clear escalation paths and site-level engagement procedures.
- Introduce **continuous training, shadowing, and joint drills** between SOC analysts and plant engineers to build operational fluency across domains.

Collaboration Recommendations

- Mandating **cyber resilience audits** for critical OT infrastructure, with tiered compliance maturity models.
- Incentivizing the creation of **sectoral OT SOC testbeds and simulation labs**, under public–private partnerships led by MeitY, CERT-In, and NCIIPC.
- Launching National Skill Development Mission in OT Security.

Regulatory Alignment

Effective OT SOC implementation not only strengthens cyber-physical resilience but also directly supports enterprises in meeting India's evolving regulatory obligations across the critical infrastructure sectors.

- **Enables continuous monitoring required by CEA 2021 Directions**, including real-time visibility of SCADA, substation automation, and plant-level control systems.
- **Supports mandatory IT–OT segregation controls**, ensuring secure data flow and network zoning as outlined by CEA and NCIIPC guidelines.
- **Provides structured detection and response workflows**, fulfilling CERT-In and CSIRT expectations for timely identification, escalation, and containment of cyber incidents.
- **Delivers audit-ready logs and evidence**, including centralized event correlation and long-term retention, essential for regulatory compliance and periodic security audits.
- **Ensures timely incident reporting to CERT-In/NCIIPC**, by integrating alerting, classification, and communication mechanisms aligned with mandated timelines.
- **Implements preventive and resilience-focused controls** recommended by NCIIPC, such as anomaly detection, baseline behavior monitoring, and critical asset protection.
- **Strengthens governance and accountability**, enabling clear roles between IT, OT, OEMs, and plant teams that is critical for meeting regulatory expectations on responsibility and decision-making.
- **Provides sector-wide readiness**, supporting utilities and critical infrastructure operators in standardizing cyber hygiene and aligning with India's national cyber incident response ecosystem.

Path Forward for Market Enablement

The road ahead for OT SOCs in India involves translating operational, and technological readiness into market maturity. The ecosystem is poised for rapid growth driven by:

- **Regulatory mandates** (from CERT-In and CSIRT and sectoral regulators such as CEA, etc.).
- **Growing domestic capability** through Indian cybersecurity startups innovating in industrial monitoring and anomaly detection.
- **Integration of AI and automation**, enhancing alert prioritization and predictive threat modelling.
- **Enable international cooperation** in OT cybersecurity through strategic dialogues with the global players, focusing on joint research, certification frameworks, and talent exchange programs.

In the long run, a resilient OT SOC ecosystem will serve not only as a defensive measure but as a competitive differentiator for India's industrial economy by enhancing investor confidence, ensuring production reliability, and reinforcing the country's status as a global hub for secure manufacturing and critical infrastructure innovation.

References

1. *Central Electricity Authority (Measures Relating to Cybersecurity in Power Sector) Directions, 2021*
2. *2025 State of Operational Technology and Cybersecurity, Fortinet*
3. *Honeywell GARD(Global Analysis, Research, and Defense) Data*
4. *2025 State of Operational Technology and Cybersecurity, Fortinet*
5. *When Should You Trust AI For Mission-Critical Tasks in the SOC, Splunk*
6. *2025 Cyber Threat Report, Honeywell*
7. *Ransomware Statistics for 2025, Ransomware.live*

Acknowledgement

Honeywell

Pranav Bhopatkar
Director – Cybersecurity
META, India

Ashdin Bharucha
Sales Manager – India

Luke Tasker
Global Customer Marketing Manager –
OT, ICS & IoT Cybersecurity

DSCI

Anuprita Singh
Senior Associate Research

Neha Mishra
Lead – DSCI Insights and Research

Bhupesh Janoti
Senior Program Manager – Business Transformation & Security

Contributor:

Mridushi Bose
Senior Associate, Marketing & Communications, DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives.

Honeywell

Honeywell provides industry leading, end-to-end OT cybersecurity technology and services. Honeywell operates 7 regional hubs: the Cybersecurity Center of Excellence in Dubai, Singapore, Atlanta and Bucharest, which support threat detection, rapid response, and advisory services; and Honeywell Managed Security Services Center in Dammam, Houston, and Bucharest which focuses on training, testing, and managed services. These centers deliver advanced MDR, support localization, and build regional cybersecurity capabilities.

DATA SECURITY COUNCIL OF INDIA

Nasscom Campus, Fourth Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

+91-120-4990253 | info@dsci.in | www.dsci.in

DSCI_Connect dsci.connect dsci.connect data-security-council-of-india dscivideo