Strengthening Cyber Resilience for a Digital Agriculture Ecosystem

About the Customer

The customer is a central public sector organization focused on enhancing agricultural productivity, farmer welfare, and rural development. With a mission to improve the livelihood of millions across rural India, the organization manages a wide array of digital platforms for subsidy distribution, crop insurance, procurement systems, and beneficiary management. Operating at the intersection of policy implementation and digital governance, it processes and safeguards vast volumes of personal, financial, and geospatial data across multiple states and stakeholder groups.

The Challenge

As the organization expanded its digital services to increase accessibility and transparency, it encountered several security and operational risks:

Securing farmer-centric portals and mobile apps that manage subsidies, insurance claims, and landholding records.	**Protecting sensitive personal and Aadhaar-linked data** from unauthorized access and misuse.	**Preventing cyber fraud in direct benefit transfers (DBT)** through real-time monitoring of transactions.
Addressing vulnerabilities in legacy applications developed across different departments over the years.	**Ensuring high availability and integrity** of procurement and warehouse monitoring systems during peak seasons.	**Complying with national data protection mandates** and sectoral audit requirements from regulatory bodies.

The scale of its digital outreach—serving over 150 million farmers—demanded a cybersecurity platform that could offer centralized visibility, automated threat response, and scalable protection.

Threat Deception with XDR+

Deception was deployed across sensitive digital services to:

- Detect misuse of admin credentials and simulate DBT fraud scenarios.
- Divert automated scripts and bots targeting subsidy portals to deception assets.
- Reduce false-positive incidents by 48% enabling faster triage during seasonal program rollouts.

Security Compliance Enablement with GSOS

The GSOS module supported the team in:

- Aligning internal controls with national public sector audit guidelines.
- Generating audit-ready reports across subsidy programs and payment platforms.
- Creating a security policy framework consistent with MeitY and NIC best practices.

CTEM in Action CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Mapped 5,400+ digital assets, including DBT APIs, mobile apps, cloud storage buckets, and admin portals.
Discovery	Detected 72 critical vulnerabilities, including API exposure, insecure session tokens, and unpatched CMS plugins.
Prioritization	Flagged 31 issues with potential to impact farmer payments and real-time data accuracy.
Validation	Simulated attacks on 3 mobile apps and 4 DBT integrations, confirming risks related to session hijacking and input tampering.
Mobilization	Enabled 90% patch implementation within 21 business days through automated workflows and patch validation with Invinsense teams.

Executive Quote

"Delivering secure and timely services to farmers is our top priority. Invinsense has helped us build a strong cybersecurity foundation while maintaining trust in our digital infrastructure."

– CISO, Central Government Entity for Agriculture and Rural Welfare

Solutions Used

To safeguard its critical infrastructure and ensure secure delivery of citizen services, the organization deployed:

- **Invinsense XDR** to unify detection across citizen service portals, DBT APIs, and state-level integrations.
- **Invinsense XDR+** to add deception capabilities across subsidy portals and backend systems to trap malicious activity early.
- **Invinsense OXDR** to identify vulnerabilities in crop insurance platforms, mobile applications, and administrative tools.
- **Invinsense GSOS** to align data handling and control policies with MeitY guidelines and internal audit expectations.

Key Results

- **90% remediation** of critical exposures in under a month.
- **48% reduction** in false-positive alerts.
- **100% alignment** with internal and regulatory audit requirements.
- Enhanced protection of **personal and financial data of** over 150 million citizens.
- Improved service uptime and incident visibility during **peak agriculture seasons.**

Infopercept | INVINSENSE

About Infopercept - Infopercept is one of the fastest growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Contact
sos@infopercept.com
www.infopercept.com/knowledge/casestudy