DCM Infotech

CASE STUDY · MANAGED SECURITY OPERATIONS

Delivering 24×7 managed security operations for a mission-critical government platform

How a multi-tier Managed Security Operations Centre has protected a high-profile public portal for four years

>10,000
Visits to the portal every day

24×7
Security monitoring, 365 days a year

4 years
Of continuous cyber defence

01 · EXECUTIVE SUMMARY

A government portal under constant threat needed security operations, not just tools

Government digital platforms have become some of the most targeted assets in cyberspace. A leading government regulatory organisation, responsible for critical economic and regulatory activities across the country, operates a public-facing portal that receives more than 10,000 visits every day from businesses, investors, professionals, government agencies and citizens. Because of its strategic importance, it has consistently been on the radar of threat actors ranging from cybercriminal groups and hacktivists to sophisticated adversaries.

Recognising that cybersecurity could no longer be treated as a technology deployment exercise alone, the organisation established a 24×7 Managed Security Operations Centre (SOC). It combines IBM QRadar SIEM, IBM X-Force threat intelligence, Tenable, Fortinet, Cisco, identity controls, and Data Centre and Disaster Recovery oversight with dedicated Level 1, 2 and 3 security professionals and formal service, SLA and change governance.

Over four years, the Managed SOC has protected the platform against a wide variety of cyber threats and maintained uninterrupted security operations.

02 · CUSTOMER BACKGROUND

The portal is now a mission-critical national digital asset

The customer is a prominent government institution that administers and regulates critical economic processes affecting organisations and stakeholders across the country.

Any disruption, degradation or security compromise of its website could affect public services, business processes, stakeholder confidence and wider economic activity. The platform has evolved beyond a traditional website into a mission-critical national digital asset that needs enterprise-grade protection and operational oversight.

The platform is the primary gateway for

- Regulatory services
- Statutory information
- Public disclosures
- Citizen interactions
- Enterprise compliance
- Government-to-business communications

03 · BUSINESS CHALLENGES

Four pressures called for an integrated security operation

Protecting a high-profile platform

Attacks on public-sector portals often aim beyond financial gain: to disrupt services, damage citizen trust, influence public perception, interrupt regulatory activity or create economic uncertainty.

Managing security around the clock

Threats don’t keep office hours. Attacks can come at weekends, on national holidays, outside business hours or across several vectors at once, so vigilance had to be 24 hours a day, 365 days a year.

Increasing threat complexity

Security data came from networks, appliances, operating systems, authentication platforms, applications, databases, scanners and endpoint tools. Without centralised visibility, attack patterns were hard to spot.

Maintaining operational discipline

Tools alone cannot guarantee security. The customer needed incident, change and escalation management, SLA compliance, governance reporting and continuous improvement.

> **The requirement was not simply for security tools, but for an integrated security operations capability.**

04 · SOLUTION OVERVIEW

A managed security programme, not a standalone implementation

The engagement was designed as a comprehensive managed security services programme. Together, its components created a sustainable and scalable cybersecurity operating model:

- Advanced cybersecurity technologies
- Skilled security personnel
- Well-defined operational processes
- Service governance
- Performance management
- Continuous monitoring

05 · THE 24×7 SECURITY OPERATIONS CENTRE

Three tiers give every incident the right level of expertise

The SOC is the central command centre for cybersecurity operations, monitoring, investigating and responding to events across the customer environment with continuous visibility into its security posture.

L1	**Level 1 operations** The first line of defence	Around-the-clock monitoring across all shifts: security event monitoring, alert triage, initial investigation, event categorisation, incident logging, ticket creation, escalation and monitoring dashboard management. Every event entering the SOC is reviewed and prioritised.
L2	**Level 2 specialists** Deep technology expertise	Technology-specific experts for IBM QRadar SIEM, IBM threat intelligence, Tenable, Fortinet, Cisco and identity systems. They handle incident investigation, troubleshooting, platform optimisation, correlation rule tuning, performance management, security configuration and upgrades.
L3	**Level 3 security experts** Complex threat scenarios	Advanced incident response, cross-technology investigations, root-cause analysis, threat hunting, security architecture reviews, major incident management and strategic remediation planning, for attacks that span multiple systems and domains.

06 · TECHNOLOGY FOUNDATION

An integrated technology stack provides defence-in-depth

IBM QRadar SIEM

The central analytics platform: real-time monitoring, log management, event correlation, threat prioritisation, investigation workflows and security analytics.

IBM X-Force Threat Intelligence

Global feeds on malicious IP addresses, emerging campaigns, indicators of compromise, threat actor activity and attack trends, for faster, more accurate decisions.

Vulnerability management

Continuous assessment with Tenable finds security weaknesses, configuration risks, missing patches and critical exposures before they can be exploited.

Identity security

Active Directory and multi-factor authentication (MFA) strengthen access controls and reduce the risk of unauthorised access.

Network and perimeter security

Fortinet security infrastructure and Cisco networking technologies, with firewall security and network segmentation.

Infrastructure protection

Security appliance monitoring, web application security, Disaster Recovery security oversight and DDoS mitigation controls.

07 · SERVICE GOVERNANCE

Governance and discipline keep the operation accountable

Many cybersecurity programmes fail not because of poor technology but because of inconsistent operational discipline. A structured governance framework addresses that risk.

Dedicated delivery management

A Delivery Manager oversees service delivery, team coordination, customer engagement, escalations, SLA compliance and reporting, bridging operations and business stakeholders.

SLA-driven operations

Defined service levels for alert response times, incident response timelines, resolution targets, escalation commitments and platform availability.

Structured change management

Every change passes impact assessment, risk evaluation, approval, implementation planning, validation and rollback preparation.

Continuous service improvement

Regular reviews of incidents, emerging risks, technology effectiveness, processes, capacity and the threat landscape.

08 · RESULTS AND BUSINESS BENEFITS

Four years of continuous cyber defence kept the platform resilient

Since it was established, the Managed SOC has continuously monitored, detected, investigated and responded to security events while maintaining operational stability, and the environment has remained resilient despite ongoing attempts to compromise or disrupt services.

Enhanced security visibility	Centralised visibility across systems, applications, security appliances and infrastructure has improved situational awareness and decision-making.
Faster detection and response	SIEM analytics, threat intelligence and skilled analysts let potential threats be analysed, escalated and addressed before they become major incidents.
Stronger operational resilience	Data Centre monitoring, Disaster Recovery oversight and 24×7 support have strengthened business continuity.
Reduced risk	Continuous monitoring of risk indicators and suspicious activity enables earlier intervention and reduces exposure.
Governance and accountability	Service management, SLA monitoring and formal change management bring consistent reporting, transparency and accountability.
Trusted long-term partnership	The customer has renewed the engagement annually, reflecting confidence in the technology, expertise, responsiveness and service delivery.

09 · CONCLUSION

Security became a mature operational capability, not a technology deployment

Cybersecurity for mission-critical government platforms cannot be achieved through technology alone. The integrated framework of IBM QRadar, threat intelligence, vulnerability management, identity security, multi-layer infrastructure protection and a dedicated L1, L2 and L3 team has created a resilient defence ecosystem. Over four years it has defended the platform against evolving threats while maintaining service availability, and the customer's continued trust reflects both the solution and the partnership behind it.