IBM Security

IBM

X-Force® Threat Management Services

A smarter security solution to manage the full threat lifecycle

When properly implemented and integrated, a standards-based threat management solution can provide the following critical business outcomes:

Transparency	Uncovering all connected devices and providing an open book solution
Speed	Automation increases speed to action
Consistency	Prescriptive action increases consistency
Quality	Enriched investigation results in higher quality
Collaboration	Joint development of security maturity roadmap and execution
Governance	Routine advisory service and continuous optimization

IBM X-Force Threat Management Services is an end-to-end, integrated threat management program that provides services across each phase of the NIST cybersecurity framework. An intelligent mix of cognitive tools, automation, orchestration and human guidance accelerates and enhances each phase of the threat management lifecycle. X-Force Threat Management Services brings the NIST framework to life using advanced technologies and capabilities from the IBM Security Services portfolio to provide coverage across the entire threat management lifecycle.

IBM X-Force Threat Management Services helps to identify and protect critical assets, detect advanced threats, and respond and recover from disruptions. The comprehensive program provides a single workflow for threat management across multiple technology domains, including traditional IT, Operational Technology (OT), Internet of Things (IoT) and Internet of Medical Things (IoMT) bringing visibility into unmanaged devices.

The IBM Security Services mobile app increases transparency of the program with real-time updates and allows clients to access events, escalations, response teams and Watson®. Our solution supports cloud, hybrid cloud and on-premises environments and helps provide a reliable, repeatable framework for managing security.

1. Insight

- Maturity baseline
- Asset discovery
- Offensive services
- Threat intelligence

2. Protection

- Vulnerability management
- Policy management
- Protection technology
- Policy optimization

3. Detection

- 24x7 monitoring
- Patented artificial intelligence
- SIEM Rule optimization
- Alert enrichment

4. Response

- Prescriptive runbooks
- Incident response retainer
- Cyber range simulations
- Crisis communication

5. Recovery

- Remediation plans
- Business continuity
- Disaster recovery
- After action review