Security

Thought Leadership White Paper

April 2018

Help defuse IT security risks with advanced IBM X-Force Threat Management Services

Achieve better security through a holistic, managed approach to protecting enterprise systems, networks and data

Introduction

Enterprises of all sizes are adopting a range of security-as-a-service offerings, or managed security services (MSS), for greater efficiency and simplicity. By offloading specialized labor- and data-intensive security tasks such as incident detection and post-problem recovery to a managed security service provider (MSSP), an organization can focus more on core abilities and business purpose.

At the same time, to maintain a consistent security program and align internal and service provider resources, enterprises are adopting the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Adopting such a standards-based framework, especially in concert with the services provided by a leading MSSP, can offer organizations advantages in experience, staffing, scope and access to data and tools.

The NIST framework outlines five core tasks that security personnel must undertake:

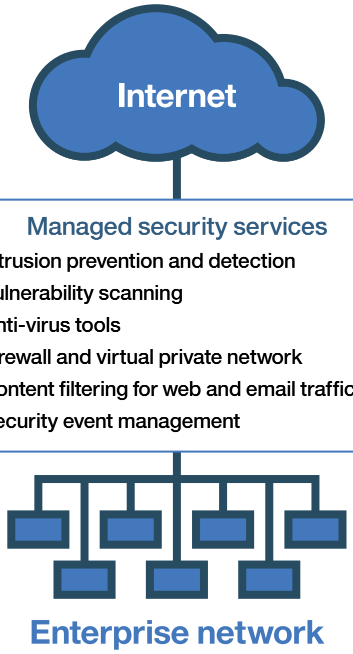
- **Identify** organizational systems, assets, data and capabilities—and the risks each one faces.
- **Protect** assets with a mix of technology, policies and practices.
- **Detect** security events, anomalous activity and undesired behavior.
- **Respond** to detected events and suspected incidents.
- **Recover** by restoring affected systems and data, and by planning for resilience in the event of future attacks.

Within each of these core functions, the framework is further divided into nearly 100 detailed categories of security outcomes and controls, such as governance, maintenance and response planning. Using a standardized approach such as the NIST CSF helps organize the activities of a security or incident team by outlining a logical, practical approach to incident management. For organizations that adopt a security-as-a-service model, a reasonable expectation is that their MSSP can orchestrate actions based on such a security-response framework.

Conventional MSS

Though details vary by provider and service level, MSSPs are typically expected to undertake several tasks that would otherwise be handled in-house by IT or dedicated security teams. In such a scenario:

- **Monitoring** of networks, core systems and valuable data stores (on-premises or in the cloud) are designed to detect intrusion attempts, data breaches, and the presence of malware or exploitable bugs—and to bring these to the attention of IT personnel. An often-used tool for this is an on-premises, or cloud-based, security information and event management (SIEM) system.
- **Management** and use of security tools (also on-premises or in the cloud) the MSSP utilizes can range from dedicated firewalls to malware-detection software.
- **Mitigation** of detected security problems as required can provide a passive or reactive approach. These functions require MSSP personnel to respond as security issues are detected by the underlying security tools, such as firewalls or malware-alerting systems. Response mitigation tools can include endpoint detection and response (EDR), firewalls or web proxies, as an example.
- **Reporting** and internal auditing tasks include those needed for consumption-based billing and those designed to demonstrate compliance with incident management and service requirements.


Internet
Managed security services
• Intrusion prevention and detection
• Vulnerability scanning
• Anti-virus tools
• Firewall and virtual private network
• Content filtering for web and email traffic
• Security event management
Enterprise network

MSSPs help enterprises by providing security expertise with a common pool of resources and specialized knowledge that an enterprise may not want to acquire and maintain.

This conventional, scope-limited approach to MSS benefits organizations by providing security resources the firm may not have—for example, by allowing dedicated, around-the-clock coverage. The variety of MSS offerings available can free up internal resources to concentrate on other security demands, rather than ones that can be covered by day-to-day routines. Regardless of size, virtually any organization can benefit from the cross-client visibility that MSS can bring to the table.

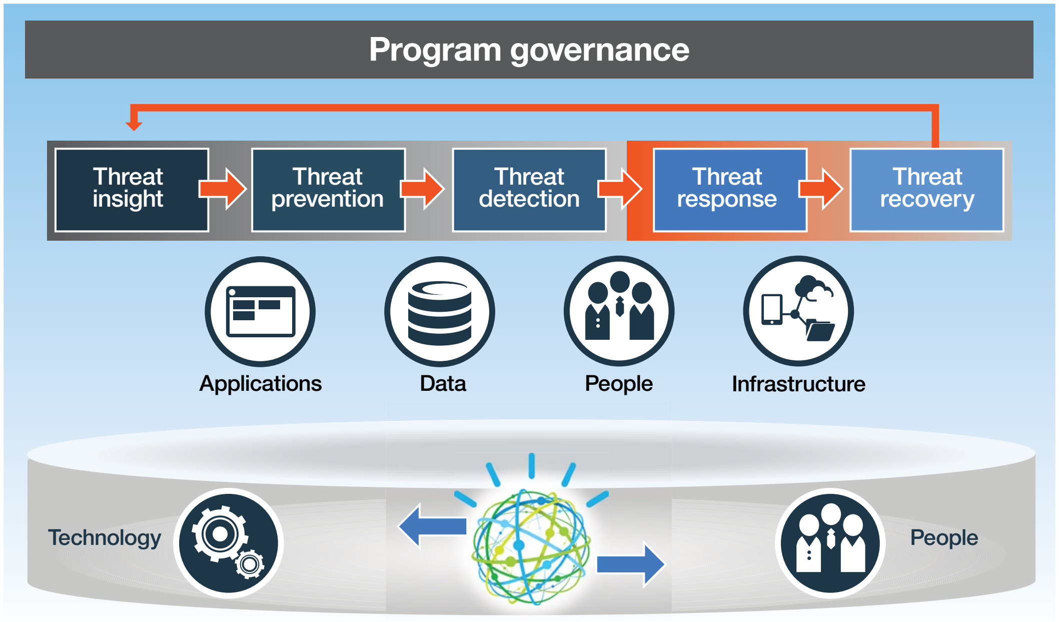
However, sourcing security activities to a managed security provider does not guarantee consistency across the enterprise. An enterprise can have critical gaps that must be overcome to achieve greater security.

MSS, for instance, does not eliminate the problem of protecting data silos within an enterprise. Different threat vectors (such as applications, databases, and user authentication and system access systems) may be managed separately, or divisions within the enterprise may not share tools even when protecting similar data stores. Situations such as these demonstrate that simply allowing a third party to manage security tools does not automatically unify an organization's security approach.

More importantly, while a conventional MSSP offers convenience and simplicity in staffing even when a large security team is required, greater insights into the bigger picture of an enterprise's security posture are not always obtained using this traditional sourcing strategy.

Next-generation MSSPs: Beyond monitoring and notification

Besides system monitoring, tool management and as-needed issue mitigation—the set of common minimum expectations covered by a service provider—an MSSP can deliver greater value to the enterprise by using artificial intelligence (AI) and data analytics to provide next-generation threat management. With a more comprehensive MSS strategy, insights derived by employing AI together with active threat hunting can better protect the enterprise from threats—not only as they emerge, but before they do harm. Enterprises can be proactive by integrating knowledge about security issues across the MSSP client portfolio into prevention strategies for each individual client, not just into generic mitigation plans.



IBM X-Force Threat Management Services offers a standards-based, structured approach to facing security threats across the entire threat lifecycle.

The next generation of MSS therefore requires a provider that is not limited to notifying clients of detected events, but instead approaches security events as part of a larger picture. Such a provider recognizes that intrusion attempts, malware and other security issues must all be addressed cohesively. Key traits of an MSSP that can extend security tools in this manner include:

- Employment of an overarching *standards-based programmatic approach* (such as NIST), rather than a proprietary methodology, to prevent and detect undesired activity. A standards-based approach provides a reliable, repeatable framework for managing multiple types of security incidents, and encourages transparency, a shared vocabulary and predictable outcomes in responding to threats.
- Implementation of *information lifecycle management* (ILM) and *information security management* (ISM) practices to put both threats and the data they could affect into context. Viewing security incidents in isolation may cause a lack of adequate business context for proper prioritization and duplication of effort that can be reduced by instead putting each threat into a management framework.
- Emphasis on the development of *ongoing insights* using visualization and analysis tools (including AI-based tools), so experiences with previous, current or anticipated threats can be used to inform ongoing security resiliency across the enterprise.
- Integrated *monitoring and management functions* for managed systems with *consulting and system integration* for more extensive coverage, rather than approaching each phase of security maturity as an isolated need.

- An *aggressive approach to the security perimeter*, extending that perimeter to encompass widely distributed endpoints. Enterprise security must be built with an understanding that valuable data may originate from (or be stored in) not just centralized databases, but throughout the IT environment.
- *Intelligent use of automation* and orchestration to enable necessary scaling without the need for large personnel shifts.

Introducing IBM X-Force Threat Management Services

IBM is combining a framework-based approach with next-generation MSSP capabilities to deliver the five-part IBM® X-Force® Threat Management Services. This offering is built on a platform that provides threat management delivered as a service, as well as consulting services and systems architecture and integration, to allow fully integrated threat and incident lifecycle management. The solution enables an intelligent mix of cognitive tools, automation and orchestration and human guidance to accelerate and enhance each phase of the threat management lifecycle. These services are delivered through IBM X-Force Protection Platform that includes, but is not limited to, IBM QRadar® SIEM, IBM QRadar Vulnerability Manager, IBM Resilient®, AI and machine-learning technologies, plus third-party EDR tools to extend to the endpoint. Additionally, robust IBM security associated integration allows tools like Carbon Black, Blue Coat, Palo Alto and FireEye—among others—to seamlessly contribute to threat management service delivery.

X-Force Threat Management Services aligns with and expands on the NIST CSF using mature products and capabilities from the IBM Security Services portfolio to provide coverage across the entire threat management lifecycle. This IBM solution also incorporates innovative response techniques such as threat hunting with real-time forensic detail designed to quarantine suspect code before it enters an organization's network, or to help isolate an infected host. Information is transparently shared between the X-Force Threat Management team (operating as an MSSP) and the client organization throughout the duration of any security incident using both automated client notifications and human-driven responses—so clients know exactly what's happening and what's being done.

X-Force Threat Management Services is designed to eliminate or reduce the uneven protection inherent to data-security silos by emphasizing shared tools and responses, and to incorporate enterprise IT decision making throughout the security continuum. The goal is to collect all relevant data about the threat management lifecycle within an organization, from detecting threats to responding to them at the endpoints, and to use that data to repeatedly generate insights to help reduce future security problems.

There are five major capabilities of X-Force Threat Management Services derived from integrated services that feed collected data into a central integrated platform. This helps provide for seamless orchestration, automation and visibility, allowing granular control of security events and incidents through their entire lifecycle. They include:

- **Threat insight** utilizes IBM X-Force Incident Response and Intelligence Services (X-Force IRIS), IBM X-Force Red offensive testing and vulnerability management, and X-Force Research and Threat Intelligence, with support from machine learning (with IBM Watson®) for mining of data within each client environment as well as across the IBM Security client portfolio.
- **Threat prevention** utilizes managed network security tools and X-Force data plays to define threats, identify suspicious behavior patterns and make policy recommendation at any point in the threat management lifecycle.

- **Threat detection** (including threat monitoring, validation, threat analysis and modeling) uses client technologies such as SIEM tools integrated with X-Force Protection Platform to provide capabilities such as searching for known malware. Increasingly, it also encompasses anomaly detection by analyzing user, network, asset and transaction behavior using cognitive technologies. A contemporary mobile experience provides clients access to the information they need, when they need it.
- **Threat response** utilizes the incident response capability of X-Force Protection Platform integrated with IBM Resilient, supporting enrichment as well as dynamic orchestration based on incident variables to affect threat response actions. To speed the response to threats, it also offers patented risk scoring and automation based on policy.
- **Threat recovery** utilizes X-Force IRIS to help return affected systems to their previous state post-incident, and IBM X-Force IRIS Incident Planning for pre-incident resiliency preparation.

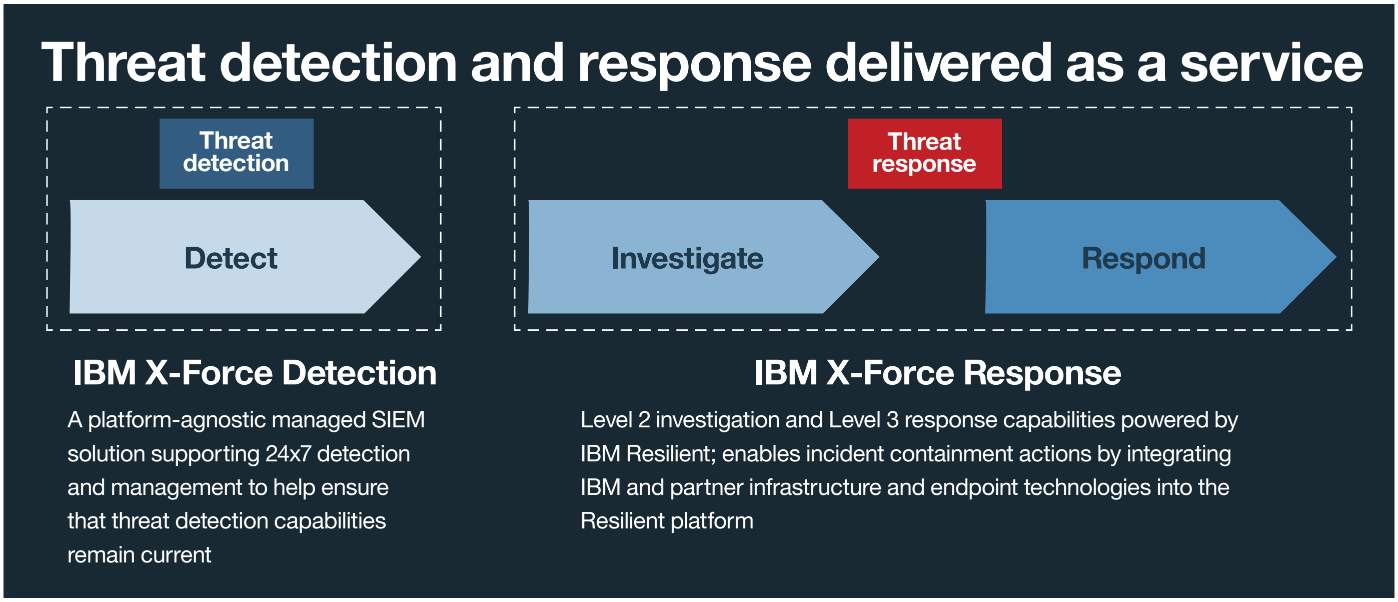
For the core operational capabilities of detection and response, three scalable levels of threat management are globally available, so security needs can be addressed more efficiently for client organizations of virtually any size, practically anywhere in the world:

- **Level 1** provides threat monitoring and detection, security issue verification with automated client notifications, and possible automated mitigation responses. Level 1 processing is highly influenced by cognitive processing, augmented by human analysis and intervention. Due to the time-intensive nature of monitoring, always-on expert monitoring is a chief reason for any enterprise to adopt MSS. And because not all security events or alerts represent actual threats, verifying the validity of alerts before spending time on investigation and mitigation helps conserve valuable time.
- **In Level 2**, experienced security analysts investigate suspicious activities, analyzing confirmed security problems, enriching the understanding of the incident, and making recommendations for further action based on the severity of the threat, the business context of the incident, and the relative priority of all other open incidents.
- **Level 3** security analysts act on the intelligence that has been gathered and the recommendations of Level 2 personnel to mitigate or contain the threat and hunt down potentially parallel issues that may have gone undetected in other parts of the environment. These IBM security operations center (SOC) analysists use both IBM and IBM-associated technologies at the endpoint or network layer to respond to incidents. All response actions are orchestrated through predefined procedures and include client communication and involvement to help reliably deliver desired outcomes.

Conventional MSS offerings usually focus on network traffic and core data stores. In contrast, X-Force Threat Management Services considers the enterprise information environment as a whole—addressing security implications of the application layer; the data held throughout the enterprise; people (including employees, administrators and other system users); and infrastructure (both hardware and architecture).

Its platform-agnostic design provides integration with products from an extensive ecosystem of partner solutions including Carbon Black, Crowdstrike, Palo Alto, Cisco, Checkpoint and more.

X-Force Protection Platform integrates capabilities to address each phase of the threat management lifecycle—and the global presence of IBM, which is staffed by empowered, skilled IBM Security employees. Because of these strengths, X-Force Threat Management Services can deliver a better experience for enterprise clients by addressing the entire threat ecosystem with continually updated service offerings and features.



Threat detection and response delivered as a service

Threat detection

Detect

Threat response

Investigate

Respond

IBM X-Force Detection

A platform-agnostic managed SIEM solution supporting 24x7 detection and management to help ensure that threat detection capabilities remain current

IBM X-Force Response

Level 2 investigation and Level 3 response capabilities powered by IBM Resilient; enables incident containment actions by integrating IBM and partner infrastructure and endpoint technologies into the Resilient platform

Components of X-Force Threat Management Services help prevent, detect, respond to and recover from threats by leveraging the best features and capabilities of other X-Force offerings.

This next-generation approach can provide security expertise in threat identification, prevention, detection, response and recovery, whether IBM delivers all these capabilities or the client organization performs some of them in-house. Critically for organizations that have already deployed security monitoring tools from other vendors such as Splunk or ArcSight, the IBM approach to security as a service adopts a vendor-agnostic viewpoint and can link smoothly with these SIEM products. Additionally, IBM already integrates IBM-associated technologies, easing the adoption of these next-generation services.

X-Force Threat Management Services offers consumption-based pricing along with pricing, packaging and options suitable for midsized and large enterprises. This enables organizations with smaller security demands to tailor their spending while getting the same expertise as the most demanding enterprises. Integral to this delivery are IBM X-Force Command Centers around the world, which enable IBM specialists to provide nonstop threat management services.

For more information

To learn more about IBM X-Force Threat Management Services, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security/services/threat-management

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest and deepest security research, development and delivery organizations; monitors more than two trillion events per month in more than 130 countries; and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
April 2018

IBM, the IBM logo, ibm.com, Resilient, QRadar, X-Force, and Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

♻ Please Recycle