IBM Security X-Force IRIS Threat Intelligence

Global intelligence experts guiding clients with industry-leading analysis

Highlights

- Know your adversary and how they can compromise your network
- Simplify and automate your threat intelligence management programs
- Share threat information within your organization and industry peers
- Contextual, prioritized, and actionable threat intelligence
- Get time back for more high-value detection and analysis work

Organizations today face an unprecedented set of pressures that can compromise cybersecurity. From a global skills shortage to an increase in the number and sophistication of threats, it's clear that the same forces that have driven growth (e.g. mobile, cloud, open source), have also created the conditions for security lapses. Organizations need accurate, up-to-the-minute information on threats and attackers, how they work, and how to defend against them.

Threat intelligence services can help security teams better understand their adversary. The most effective threat intelligence solution can support organizations at tactical, operational, and strategic-levels to turn intelligence into actionable insights to be shared across your organization industry, and communities. It should come from a trusted source with unique security expertise and data that integrates seamlessly with existing security tools to simplify and strengthen real-time decision-making.

IBM Security X-Force® IRIS Threat Intelligence

IBM Security X-Force Incident Response and Intelligence Services (IRIS) Threat Intelligence simplifies your intelligence management while improving detection and response with experts who can design, build, deliver, and operate an automated cyber threat platform. This solution provides accurate, up-to-the minute cyber threat data from both common and unique sources and the ability to share the information with your organization, industry, and communities. X-Force IRIS threat intelligence sources combined with our incident response services can help you stay ahead of attacks and better understand the risks.

IBM Security X-Force IRIS analysts curate contextual threat intelligence from real world IBM Security incident response investigations, IBM Managed Security Services operations, IBM Security research, and both open and closed sources. It delivers machine and human readable actionable information and integrates with security workflow applications via pre-built Application Program Interfaces (APIs) including Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Endpoint Detection and Response (EDR), case management, ticketing and more. Capabilities also include bi-directional communication for intel and systems improvement updates, and a secure threat intelligence sharing capability for internal and external use.

IBM Security X-Force IRIS Threat Intelligence delivers two threat intelligence offerings to help improve your cybersecurity posture:

Premier Threat Intelligence

To expand beyond indicators of compromise (IOC), Premier Threat Intelligence provides organizations access to the latest threat information findings via IBM curated, human and machine-readable threat intelligence extracted from real-time IBM security operations, investigations, and research. The service includes finished intelligence reports on threat activity, malware, threat actor groups, and industry assessments to sophisticated organizations. This high quality, prioritized, actionable threat intelligence, delivered at both tactical and strategic levels, allows for the security story to be understood by your operations, analysts, and executive leadership.

Enterprise Intelligence Management

Building on the capabilities of Premier Threat Intelligence, organizations can further improve the prioritization of events and enrich investigations by utilizing Enterprise Intelligence Management to operationalize internal and external data sources through an ecosystem of security technologies, integrations and open source intelligence (OSINT) feeds to deliver it into your security tools. This service provides the tactical structure to automate and optimize the exchange of threat data and fuse intelligence efficiently with your existing security systems. Your organization can use Enterprise Intelligence Management to facilitate threat intelligence sharing across your security operations, with IBM, and with other permissioned enclaves and communities by helping teams proactively make decisions faster.

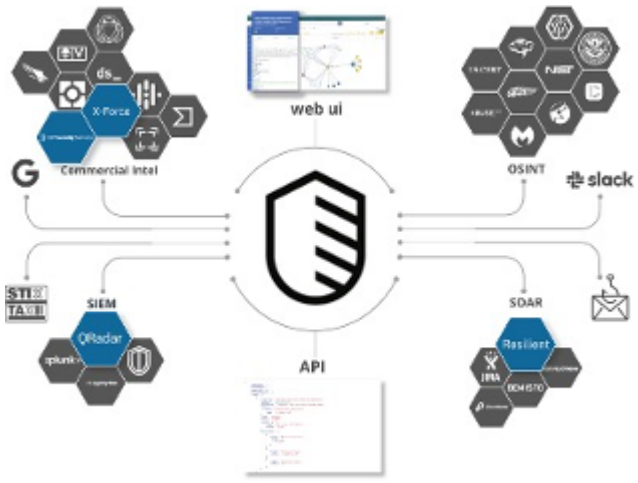

Figure 1: Enterprise Intelligence Management Impact to Client

Together, X-Force IRIS Threat Intelligence delivers a holistic enterprise intelligence management program, helping organizations operationalize, automate, optimize, and exchange threat information between contributors and making intelligence sharing more efficient and secure.

Add-On Services: Threat Intelligence Consulting Services

Cyber Threat Intelligence Program Assessment

The X-Force IRIS team can perform a threat analysis to understand the characteristics of the threat actor and how they used their capabilities to infiltrate the organization. Using industry best practices for evaluating threat information data sources, products, policies, and processes, the Cyber Threat team delivers a gap analysis, project roadmap, report of malicious activity, and recommendations to improve the organization's security posture.

X-Force Strategic Threat Assessment

The X-Force IRIS team can develop a comprehensive report examining the threat attackers likely to target an organization and the infection vectors, techniques and procedures they employ. This report provides organizations with an understanding of strategic risks to key business assets and can help senior leaders to make better decisions about organization-wide security programs, investment decisions, security requirements, and monitoring strategies. The team's unique understanding of adversaries and their tactics is derived from fusing information gathered from incident response investigations, telemetry data, dark web research, IBM spam traps, and open source research.

X-Force Dark Web Analysis Services

The X-Force IRIS team can deliver services to search the dark web, including TOR nodes, hacker forums, IRC channels, and paste sites, for specific areas of interest to the organization to warn them about leaks of their confidential information using key words (e.g. the organization's brand). They will sort through the results to turn raw data into actionable information to help improve your security posture.

Malware Reverse Engineering

The X-Force IRIS team can work with your organization to provide industry-leading malware analysis for advanced cyber threat incidents to put attacks into context by understanding TTPs. The team completely reverse-engineers malware to discover variants and understand every component.

Why IBM?

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 security research, development and delivery organizations, monitoring greater than 60 billion security events per day in more than 130 countries, and holds more than 3,700 security patents.

Next steps

→ IBM X-Force IRIS Threat Intelligence Webpage

→ City of Los Angeles Case Study

→ Threat Intelligence Index Report

→ Destructive Malware Report

For more information

Visit the IBM X-Force IRIS Threat Intelligence web page to learn more

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM Security X-Force® IRIS Threat Intelligence

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.