IBM Security

X-Force Active Threat Assessment Services

Between scanning and testing, you know you have vulnerabilities. But how do you know if any have been exploited? Or, if you have identified and remediated malicious activity, how can you affirm a clean bill of health? If you are acquiring a company, how do you know an attacker isn't already in your acquiree's environment? When you deploy new tools, if an active threat is already inside your environment, it may get baked into what's considered "normal behavior." Your tools wouldn't flag the attacker because nothing would seem unusual.

Active Threat Assessments can answer those questions and should be the baseline for your security program. They involve threat hunters analyzing forensic artifacts and correlating data from endpoints, logging tools, intelligence, and human knowledge of attacker behavior, to uncover potential exposures and active threats.

X-Force Active Threat Assessment Services

X-Force Active Threat Assessment Services is a data-driven analysis of your environment based on how adversaries may operate in a network. The services can identify threat exposures and active attacks and affirm your remediation status:

Data Collection & Analysis

– Deploys endpoint tooling to the in-scope endpoints and networks to collect forensic artifacts, including indicators of past intrusions. Data is collected from EDR, proprietary and logging tools.

– Inside a forensic lab, X-Force analysts ingest data into its data processing engine, review data sources and develop and test various hypotheses, driven by knowledge of attackers' behaviors.

Threat Hunting

– Identifies and investigates anomalous outliers and behaviors such as unusual processes, user activity and user connections.

– Searches for evidence of attacker techniques executed in the environment. Techniques are aligned to the MITRE ATT&CK framework.

Reporting & Recommendations

– Provides a report of findings and recommendations to reduce risk. The team walks you through which changes should be made and why.

Why Choose X-Force

X-Force has threat hunters, hackers, researchers and responders in twenty-two countries, and has a proven track record of helping organizations across all industries, of all sizes, minimize the impact of a breach.

Predictable Pricing

– Pre-negotiated pricing for all services based on average market rate.

– No overtime pricing, or license fees.

Expertise

– Diverse backgrounds including law enforcement, government, and industry leading digital forensics & incident response (DFIR) firms.

– Expertise spans at least a dozen security domains.

– Multiple industry certifications held by majority of team.

– Builds custom scripts, and forensic and hacking tools to support testing, investigations, preparedness and data analysis.

Portfolio of Services

– Access to the IBM Security services portfolio, under one contract and retainer:

  – Penetration Testing

  – Vulnerability Management Services

  – Adversary Simulation Services

  – Incident Response Preparedness and Retainer Services

  – Risk Quantification