Explore the IBM X-Force Threat Intelligence Index

Estimated time: 30 minutes

What is the IBM X-Force Threat Intelligence Index?

The IBM X-Force Threat Intelligence Index, an annual report created through extensive analysis of security events, provides insights into the current cybersecurity landscape. The report tracks changes, analyzes security trends and patterns, identifies emerging threats and vulnerabilities, and provides strategic guidance to help organizations strengthen their security posture and defend against cyberattacks.

The IBM X-ForceThreat Intelligence Index 2024 is based on insights and observations from examining over 150 billion security events per day in over 130 countries. In this activity, you will research and review the IBM X-Force Threat Intelligence Index 2024 to gain insights into cybersecurity trends and the threat landscape.

Learning objectives

After completing this activity, you will be able to:

- Identify the components of the IBM X-Force Threat Intelligence Index 2024
- Identify key cyber threat trends highlighted in the report

Instructions

1. Review the X-Force Threat Intelligence Index 2024 here.
   (***Note:** Right-click the link and select "Save link as" to download the X-Force Threat Intelligence Index 2024 PDF*.)

2. Familiarize yourself with the report's structure. Ensure to pay close attention to the data gathering and analysis methodologies.

3. Identify key cyber threat trends highlighted in the report and note any changes or emerging patterns since the previous index.

4. Compare the findings outlined in the index with current cybersecurity events and analyze their correlation with real-world occurrences.

What is the IBM X-Force Threat Intelligence Index?

The IBM X-Force Threat Intelligence Index 2024 gives a solid look at what's really going on in cybersecurity right now. The report is based on more than 150 billion daily security events across over 130 countries. It pulls in data from actual incident responses, network sensors, honeypots, and even dark web monitoring. What I appreciated most is that this isn't just a numbers report—it's a practical breakdown of how attackers operate and what that means for organizations trying to stay ahead of threats.

Phishing is still the most common way attackers get in, which isn't surprising. But the increase in attacks using stolen or valid credentials stood out. It shows how important identity management and multi-factor authentication really are. Another major issue is unpatched vulnerabilities. Even with all the awareness around patching, attackers are still finding open doors. That tells me that basic controls still aren't being followed in a lot of environments.

The report also called out which industries are being hit the hardest. Manufacturing is the top target again, mostly because it runs older systems that are hard to secure. Finance and healthcare are close behind. With healthcare, the impact goes beyond data, it directly affects people's lives. That's a strong reminder that cybersecurity isn't just technical, it's ethical.

What's also changing is how attacks are being carried out. Ransomware-as-a-Service is making it easier for even inexperienced hackers to launch attacks. At the same time, more advanced groups are using legitimate tools already on a system (called Living Off the Land techniques) to avoid detection. And with more companies moving to the cloud, misconfigured APIs and storage are now common weak points.

The data collection methods in this report are worth noting. IBM uses a mix of managed security services, threat hunting, honeypots, and OSINT. This multi-layered approach gives the findings real credibility and makes the report useful not just for security teams, but for anyone working in compliance or risk.

Reading this, I couldn't help but compare it to real-world incidents. In 2024 alone, we've seen hospitals taken offline by ransomware, major credential leaks, and nation-state actors trying to interfere in elections. Everything the report highlights is playing out in real time.

For someone like me, transitioning from criminal justice into cybersecurity with a focus on compliance and digital forensics, this kind of analysis is valuable. It helps bridge the gap between threat intelligence and decision-making. Whether I'm reviewing policies, building risk reports, or tracking incidents, I want to make sure those actions are grounded in what's actually happening in the field, not just theory.