XM Cyber

Protect Your Business From Stolen Credentials Before They Are Exploited

XM ECM
Exposed Credentials Management

Leverage near real-time alerts of external breaches that compromise your employees' credentials and digital identities and understand how they can threaten your critical business assets with the holistic end-to-end XM Attack Graph Analysis™.

Compromised credentials - stolen usernames, password, or cookies - are a favorite breach strategy for attackers. According to the Verizon Data Breach Investigation Report (DBIR), 80% of basic application attacks in 2024 were attributed to stolen credentials. Once company credentials are leaked, there is a short window until it is sold off to threat actors who exploit them to gain access to the organization's network. Attackers can then use lateral movement to compromise business critical assets and access sensitive data.

Existing solutions detect stolen credentials after weeks or even months, which may be too late in some cases. Early detection within hours of the breach is the best way to stay ahead of attackers and prevent breaches. Proactive infostealer threat intelligence enables near real-time detection of compromised credentials and infected devices, providing timely alerts to help mitigate threats before they are exploited.

Detect

infected devices in hours instead of weeks

Alert

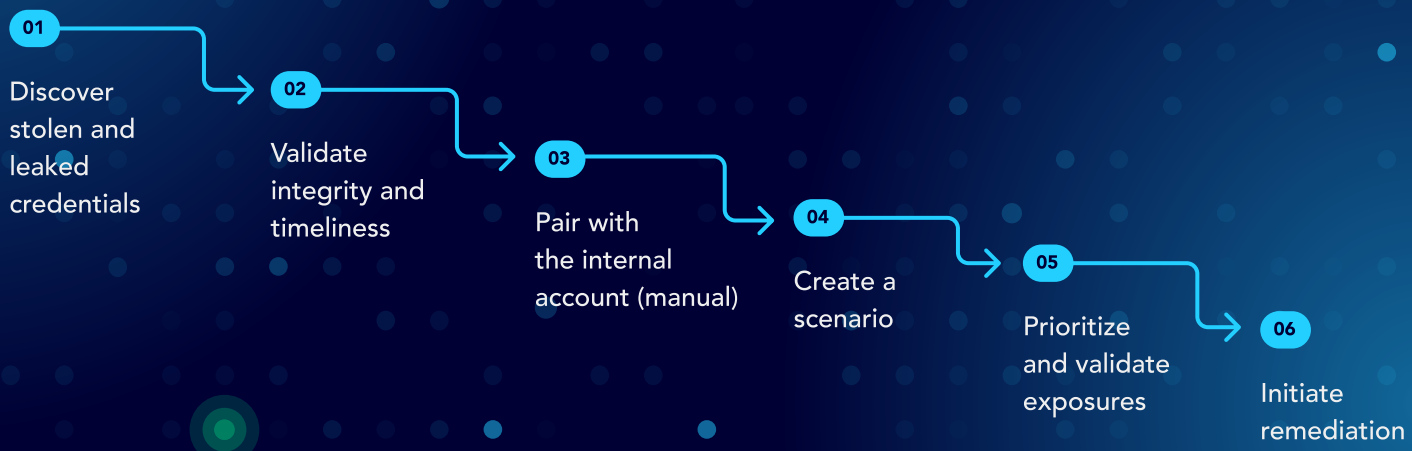
on stolen credentials before they are exploited

Validate

how leaked credentials compromise your business

Visualizing

The End-To-End Attack Path



Near Real-Time Breach Detection

XM ECM continuously monitors the primary infostealers, identifying infected machines and leaked credentials within hours instead of weeks or months. Early detection of your organization's exposures on the dark web allows you to prevent data breaches, unauthorized access, financial losses and brand damages.

Immediate Actionable Alerts

XM ECM generates near real-time alerts, empowering you to swiftly trigger password reset, revoke the account, or add multiple authentication measures. A rapid reaction to stolen credentials is the key to stay ahead of attackers and protect your business from ransomware attacks and data leaks.

Proactive Exposure Management

XM Cyber allows visualizing how leaked credentials can be used to compromise critical assets. Customers can identify the compromised accounts, classify them as a breach point, and visualize the attack path to critical assets in the XM Attack Graph Analysis™. This allows validating and prioritizing the exposed credentials and how to address them.

XM Cyber

XM Cyber is a leader in hybrid cloud exposure management that's changing the way organizations approach cyber risk. XM Cyber transforms exposure management by demonstrating how attackers leverage and combine misconfigurations, vulnerabilities, identity exposures, and more, across AWS, Azure, GCP and on-prem environments to compromise critical assets. With XM Cyber, you can see all the ways attackers might go, and all the best ways to stop them, pinpointing where to remediate exposures with a fraction of the effort. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, Asia Pacific and Israel.