CYWARE™ | Datasheet

Cyware Compromised Credential Management

Credential Exposure Intel Operationalized for Real-Time Detection and Rapid Response

Overview

Cyware Intel Exchange has now been enhanced with the new Compromised Credential Management (CCM) capability to enable seamless domain monitoring, analysis, and enables swift responses through automation and manual interventions.

As part of the new Exposure Management module in Cyware Intel Exchange, the CCM capability is also integrated with Identity and Access Management (IAM) applications to gather intelligence about the risks associated with any compromised credentials. With this new capability, security teams can define actions and automate responses to detected breaches across various security technologies, such as cloud security, forensics, malware analysis, vulnerability and risk management, data enrichment, threat intelligence, incident response, endpoint security, and more.

About Cyware Intel Exchange

Cyware Intel Exchange is a fully automated Threat Intelligence Platform (TIP) designed to operationalize the entire threat intelligence lifecycle. It enables ingestion, enrichment, correlation, analysis, and dissemination of threat data across tools, teams, and ecosystems—now enhanced with Exposure Management capabilities like CCM.

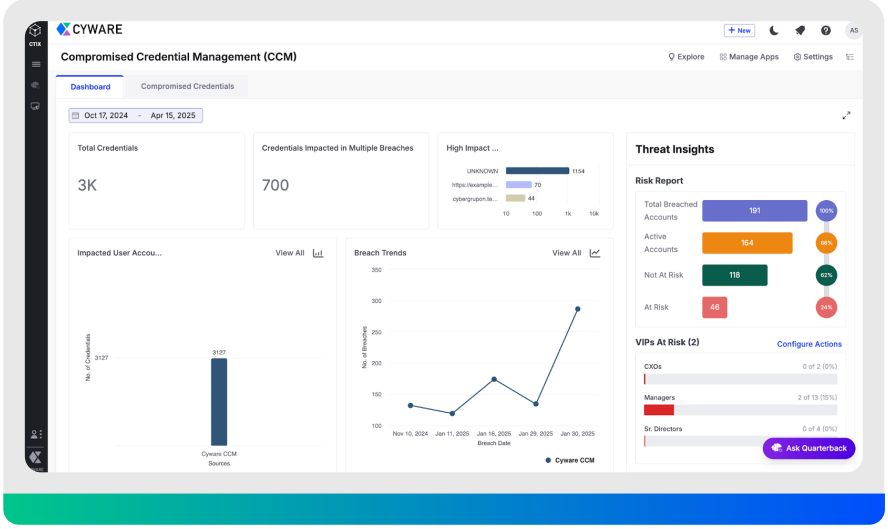

Fig 1. *Cyware Compromised Credential Management Dashboard*

Key Capabilities

Automated Domain Monitoring

Security teams are automatically notified when compromised credentials linked to monitored domains are discovered, allowing for a quick response to potential threats.

Integration with IAM

The Exposure Management module seamlessly integrates with IAM applications to gather real-time insights on compromised credentials. This empowers users to categorize breaches based on risk severity, streamlining incident management.

Automated and Manual Response

The module supports automated corrective actions across integrated applications using playbooks while also allowing users to perform quick manual actions for immediate threat mitigation.

CYWARE™

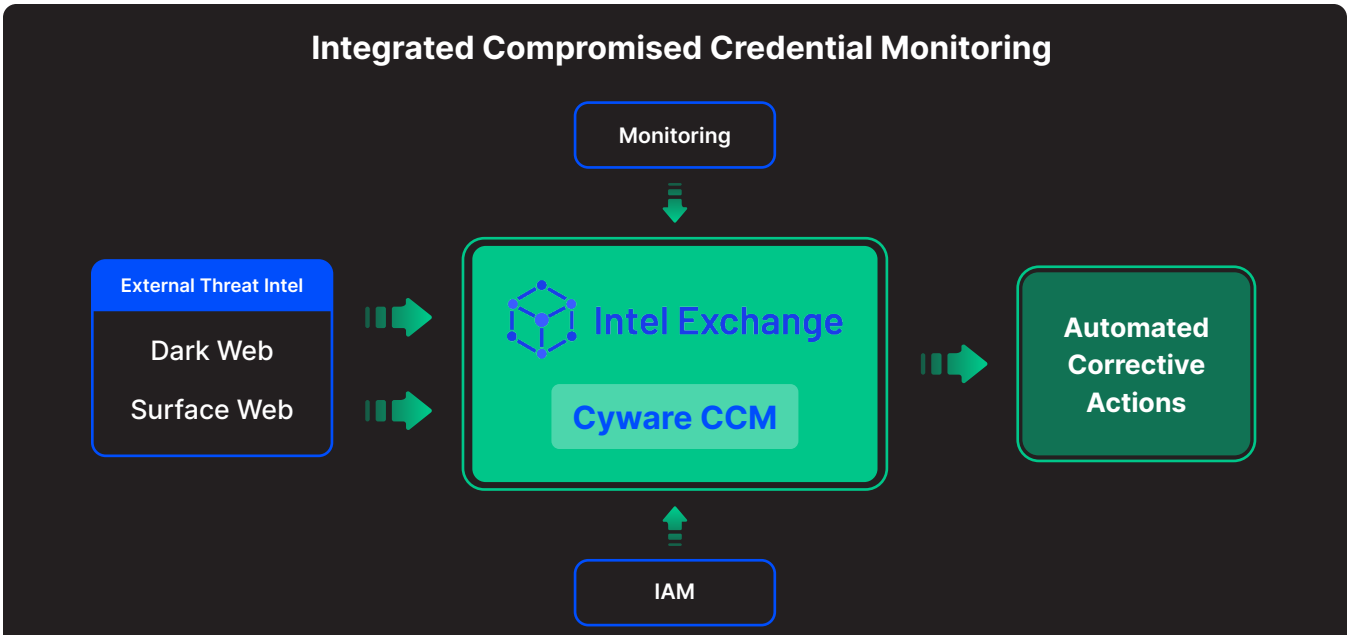

Fig 2. *Compromised Credential Management Workflow in Cyware Intel Exchange*

Exposure Management Use Cases

Compromised Credentials Management

Compromised login credentials and access information are prime targets for threat actors. Exposure Management solutions continuously monitor the web and Darkweb for references to leaked credentials.

Infostealer Malware Detection

Exposure Management solutions help protect sensitive information stored on devices or networks by enabling the early detection of stealer malware, mitigating the risk of data exfiltration.

Account Takeover Prevention

By detecting compromised credentials, stealer malware, and suspicious attempts to access sensitive accounts, the DRP module helps prevent unauthorized account takeovers.

Credential-Aware Threat Investigations

Leverage credential exposure data along with other threat intelligence sources to uncover related IOCs, actors, and campaigns.

Extending Threat Intel Operationalization Through the Cyware Ecosystem

Orchestrate

Drive threat intel operationalization and orchestrate security workflows across the cloud and on-premise using Cyware Orchestrate.

Collaborate

Enable secure collaboration and bidirectional intel sharing across trust boundaries for collective defense using Cyware Collaborate.

About Cyware

Cyware helps enterprise cybersecurity teams build platform-agnostic cyber fusion centers by delivering cyber threat intelligence and next-generation security orchestration and automation solutions. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout. Cyware's Cyber Fusion solutions enable secure collaboration, information sharing, and enhanced threat visibility for MSSPs, enterprises, government agencies, and sharing communities (ISAC/ISAO/CERTs and others) of all sizes and needs.

cyware.com

sales@cyware.com

111 Town Square Place Suite 1203,
#4 Jersey City, NJ 07310