Cyber Observer Technology Partners

CYBER OBSERVER

CROWDSTRIKE

Solution Brief

Cyber Observer and CrowdStrike Falcon Integration

End-to-end cybersecurity management and awareness

Challenge

Today's challenging cybersecurity landscape offers an over-abundance of cybersecurity tools. As the number of breaches proliferates, so have the solutions and technologies designed to stop them. The state of cybersecurity is not getting easier to manage, despite enterprises and organizations worldwide spending more money than ever on new technologies and solutions.

Designed for CISOs and senior InfoSec managers (such as CIOs, C-level managers, risk officers, SOC managers and IT Infrastructure personnel), Cyber Observer empowers leadership with a **unified dashboard** of their entire cybersecurity ecosystem. Cyber Observer can be fully deployed within an enterprise in a few hours, enabling easy **identification** of **weaknesses**, **reduction of mean-time-to-detect (MTTD)**, **prevention of breaches**, and advancement of your organization's **cybersecurity posture** and **maturity**.

Solution

Cyber Observer's partnership with CrowdStrike enables CISOs to better manage their cybersecurity ecosystem. They receive alerts from Cyber Observer on the key aspects and issues in CrowdStrike Falcon such as **configuration**, **incident** and **investigation management**, **access control**, **password policies**, **user** and **role administration** and more. This joint effort helps enterprises manage their cybersecurity environment and **continuously monitor their cybersecurity ecosystem posture**.

KEY FEATURES

- Identifies cybersecurity tools that are misconfigured, malfunctioning, or missing
- Finds security gaps and provides recommendations for fixing
- Builds an ongoing security program to ensure alignment with new threats
- Uses continuous analytics to send alerts when there are deviations from normal behavior
- Automatic reporting

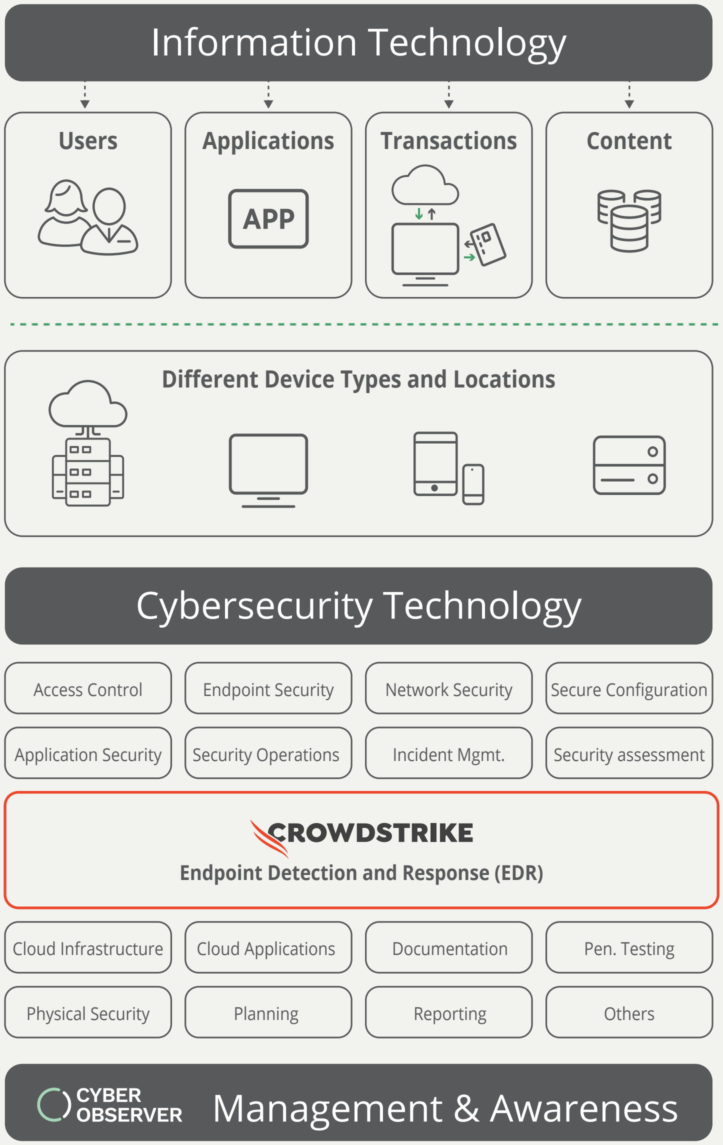
The integration between Cyber Observer and CrowdStrike offers CxOs powerful and effective **resilience visibility** along with **compliance validation** and **controls**, to secure and monitor Tenable. SC in an unprecedented manner.

Cyber Observer deploys to the corporate network automatically, in a matter of a few hours, predefined with security domains and CSC measurements to deliver three unique cybersecurity ecosystem views:

- First, it provides organizations with the best indicators of the cybersecurity tools that may be **misconfigured**, **malfunctioning**, or **missing** and should be added to provide complete cybersecurity protection.
- It then **reveals the security gaps** that exist in each security domain and **delivers continuous proactive recommendations to close these gaps**.
- Finally, Cyber Observer's machine learning analytics engine continuously calculates online measurements that represent normal behavior, and then **alerts when a deviation from normal behavior is detected**.

Fast and Secure Deployment

The Cyber Observer connector for CrowdStrike receives security and configuration data from the CrowdStrike server via a secure REST API.



CYBER OBSERVER

CROWDSTRIKE

Key Features & Benefits of This Integration

- **Cyber Hygiene Analysis and Reporting for Managers:**
  Alerts and reporting regarding CrowdStrike Falcon current configuration implementation status based on vendors' and security standards best-practices, including security configuration issues, incidents and investigations management, admins and roles administration, and more.
- **Reduced Incident Analysis Time:**
  Cyber Observer provides continuous alerts on deviation from normal behavior in terms of CrowdStrike Falcon implementation and effectiveness as well as continuous monitoring of relevant security issues in near real-time.

Continuous Incident Response:

- Provides the CISO and other relevant managers in the organization, as well as the CrowdStrike Falcon technical owners with continuous mitigation recommendations and steps to improve, for securing and monitoring CrowdStrike Falcon implementation, effectiveness, maturity and resilience from a management perspective in an unprecedented manner.

Customizable Views and Reports

- Cyber Observer is highly customizable – all views and reports could be modified to the organization's needs and structure. The integration between Cyber Observer and CrowdStrike Falcon offers CxOs powerful effectiveness and resilience visibility, as well as compliance validation and controls.

Key Use Cases

1 Immediate alerts and detailed information regarding high severity detections and incidents

- New High-risk severity incidents
- Hosts with more than X incidents
- Hosts with more than X incidents
- Detections with process blocked
- Detections with process killed or operation was blocked
- Detections with falcon overwatch tactic attacks found
- Detections with process not killed

2 Immediate alerts and detailed information regarding various MITRE Attacks found

- Detections with MITRE Initial Access tactic attacks
- MITRE Execution tactic attacks
- MITRE Persistence tactic attacks
- MITRE Privilege Escalation tactic attacks
- MITRE Credential Access tactic attacks
- MITRE Command and Control tactic attacks
- MITRE Exfiltration tactic attacks

3 Detailed information regarding mis-configured and insecure policies found

- Windows prevention policies without unknown executables
- Windows prevention policies without sensor anti-malware detection\prevention
- Windows prevention policies sensor anti-malware detection machine learning not set to aggressive
- Windows prevention policies without cryptowall prevention
- Windows prevention policies without file encryption prevention

About CrowdStrike

CrowdStrike® Inc.(Nasdaq: CRWD), a global cybersecurity leader is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform’s single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network.

About Cyber Observer

Cyber Observer is the premier critical controls monitoring (CCM) solution that simplifies the way cybersecurity tools are monitored and managed. Cyber Observer integrates hundreds of popular cybersecurity tools into a single intuitive interface that enables security and risk management executives to continuously monitor their security tools and improve their cybersecurity posture in alignment with cybersecurity, business, and regulatory frameworks.
Learn more at **cyber-observer.com**.