mastercard

Cyber Front

Automatically and continuously test the ability of your security systems to detect and protect your production environment against the latest threats.

Breaches happen every day – but most are not zero-day attacks. Many are configuration mistakes and other preventable errors. Targeting exploitable misconfigurations helps address the most urgent gaps. This, in turn, enables you to reduce cyber risk costs by focusing on issues that can readily cause cyber incidents and breaches.

Cyber Front executes frequent, ongoing attack simulations to validate and improve security infrastructure and operations:

Is my organization prepared to respond to a potential cyber threat?

- ✓ Assess your organization's cyber readiness against the latest emerging threats with a threat library which provides more than 4,000 real-world threats, comprising more than 20,000 TTPs covering all major OS families (Windows, Linux, macOS)
- ✓ Reduce opportunities for attackers by validating your security controls continuously

Did preventative and detective controls work as anticipated against known cyber threats?

- ✓ Validate your security controls to provide the protection you need to defend against the latest cyber threats.
- ✓ Cyber Front maps simulation results to MITRE ATT&CK framework and unified kill chain to understand gaps in your controls in greater detail

Does the security operations center (SOC) have the capabilities and processes to respond to detected alerts?

- ✓ Detect and respond to threats and security gaps with increased efficiency.
- ✓ Continuously supply quantifiable metrics to measure effectiveness, reduce risk and demonstrate ROI.
- ✓ An intuitive user interface provides complete visibility over your posture with options for quick reporting

How should my organization address exploits that were neither prevented nor detected?

- ✓ Boost detection capabilities by validating logs and alerts generated through simulation activities.
- ✓ Mitigate identified gaps quickly by providing insights and recommendations specific to your technology stack with a frequently reviewed library of mitigation actions

HOW IT WORKS

Through agents deployed on your network, Cyber Front utilizes various modules to simulate threats with no disruption to your operations and allows visibility over entire unified kill chain of attacks.

Attack Modules cover:

- ✓ Network Infiltration
- ✓ Endpoint Systems
- ✓ Email Security
- ✓ Web Applications

Cyber Front also allows organizations to see if their detection tools logged and alerted these attacks. **By improving detection and responding to current threats, organizations can improve their cyber resiliency.**

Attack Simulation Needs		Cyber Front Solution
Identify whether technology configurations are set up correctly to defend against emerging threats.	→	Validate that security infrastructure, configuration settings and prevention technologies are operating as intended.
Scan frequently and quickly to keep up with continuous operational changes in the technology infrastructure.	→	Continuously test existing security infrastructure, without the need to wait for vulnerability scanning windows.
Go beyond identifying vulnerabilities to also understand potential exploitability.	→	Understand the probability of a threat by identifying threats and attack vectors.
Provide effective guidance to address incidents, rather than generic response scenarios.	→	Ensure security operations staff and incident responders can detect attacks and respond accordingly during cyber response exercises.

COMPETITIVE DIFFERENTIATION

Mastercard has unmatched expertise and extensive hands-on experience securing our own worldwide network

Industry Leadership

Founding member of Cyber Readiness Institute and co-founded the PCI Council

First-hand Expertise

Mastercard has been applying our cybersecurity principles to secure a global payments network for the past 50 years

Dynamic Adjustment

Mastercard's methodology accounts for the **changing environment** of **cyber threats** and responds to **new attacks**