Qintel

PMI

PMI™

Patch Management Intelligence (PMI) Reporting on Actively Exploited Common Vulnerabilities and Exposures

Prioritizing patching is a challenge in any organization. Qintel's Patch Management Intelligence (PMI) product simplifies the process by providing vital context around reported Common Vulnerabilities and Exposures. PMI is a repository of exploited vulnerabilities that are known by Qintel to be leveraged by adversaries of all stripes.

WHAT SETS PMI™ APART?

Qintel just doesn't just follow cyber underground conversations. We use our advanced tracking and visibility into criminal and nation-state infrastructure to see which vulnerabilities are actively being exploited. Data is added on a real-time basis, meaning you see a vulnerability when we do.

PMI™ HIGHLIGHTS

Qintel offers clients high-fidelity reporting of actively exploited Common Vulnerabilities and Exposures (CVEs) that can be utilized to help prioritize patch management processes as well as help threat hunters look for threats against internal systems.

Qintel identifies the targeted CVEs based on its proprietary collections, which include intelligence related to nation-state and criminal activity, as well as exploit kits and public tools like Metasploit.

As part of the service, Qintel includes available context around attacks or tools associated with the CVE information provided in PMI. Qintel also produces indicator arrays related to nation-state groups.

Culture at Qintel

More than a job - a family, excitement, reward, and a sense of meaning and accomplishment.

Contact Us

Qintel has a security solution for all types of organizations. Please reach out to learn more about how our products can help you combat cyber-enabled fraud and attacks.

Qintel

What We Do

Our Data

- The Data Lake
- Integrations

Success Stories

Products

- CrossLink
- QWatch
- QSentry
- QAuth
- PMI

Services

Trust & Security

About Us

Culture

Careers

Contact

Privacy Policy