Looking into Your Cyber Risk Future

Highlights

- A leader in the Forrester Wave™: External Threat Intelligence Service Providers, Q3 2023
- 200K+ hours responding to attacks per year
- Digital asset discovery and digital footprinting
- Service offering to provide a composite picture of the most relevant cyber threats to you and how they will most likely target you
- Monitor for keywords on 200+ card shops, forums, marketplaces and ransomware sites across open, deep and dark web sources
- 285+ active checks available to confirm vulnerabilities, misconfigurations, and exposures

Multiple avenues of insight with digital risk protection

Cyber criminals prepare for their attacks. This preparation leaves evidence across the internet. If you know where to look or have the right access, these clues can provide enough early warning to ready cyber defenses for the attack.

Digital risk protection gives you visibility into your global attack surface and dark web activity. This enables you to neutralize threat actor campaigns before any organizational impact, such as damaged brand reputation, lost customer trust and digital exposure across the extended enterprise infrastructure. Digital risk protection gives security professionals the ability to identify:

- High-risk attack vectors
- Malicious orchestration from the deep and dark web
- Campaign execution on the open web
- Threat actor groups and the tactics, techniques and procedures (TTPs) they are currently using

Armed with this information, organizations can prepare for attacks, use resources more efficiently and reduce response time.

Visibility into external exposure and targeting

Having visibility is good. Knowing when and where to look is a game-changer. Digital risk protection draws from threat intelligence to know where to look across the open, deep and dark web for malicious chatter and targeting.

Threat analysis and risk identification

To protect against imminent attacks, you need to start by answering three questions:

Who's targeting you?

What are they targeting?

How are they planning to compromise you?

You answer these questions, by monitoring the open, deep, and dark web for chatter, understanding the motivation of the threat actors targeting you, and seeing which externally facing systems look the most vulnerable. Digital risk protection helps identify the threats most relevant to the organization. This in turn helps you to know the attacker and their playbook, and adjust your security tools accordingly.

Cyber threat intelligence-driven prioritization

The next step is to gather threat intelligence you can have confidence in. Digital risk protection draws on threat intelligence to help you understand threat actor methods and the tools they will use against you. You can use this knowledge to prioritize and proactively adjust your defenses.

How Mandiant delivers digital risk protection

To properly address the requirements of digital risk protection, Mandiant offers both products and services depending on your needs and requirements. The product offering includes Mandiant Advantage Threat Intelligence, Mandiant Advantage Digital Threat Monitoring and Mandiant Advantage Attack Surface Management and the services offering includes Managed Digital Threat Monitoring and Cyber Threat Profile. All of these offerings draw on industry-leading, nation-grade Mandiant threat intelligence.

Digital Threat Monitoring and Attack Surface Management provide the visibility needed to anticipate attacks. By using the knowledge within Threat Intelligence, Digital Threat Monitoring knows where to look on the open, deep and dark web for malicious chatter. It monitors forums, paste sites, social media, marketplaces and more to anticipate an attack. Paired with Attack Surface Management you get the added visibility across your vulnerable, external-facing assets and cloud resources. Individually these are powerful products, but together they enable you to see further and protect your organization well in advance of a possible attack.

For example, if Attack Surface Management identifies a vulnerability on a device hosted by a third party, you can search the deep and dark web for chatter about exploiting this vulnerability using Digital Threat Monitoring. Mandiant can automate the recognition of this chatter, attributing it to a threat group through the Mandiant Indicator Confidence Score. Based on attribution, you can learn the TTPs of the threat actor to ensure your organization is prepared to mitigate the impact of a pending attack.

Another scenario: Digital Threat Monitoring sees activity targeting an executive in your organization. You can use details of this activity to help identify the threat actor and other TTPs they commonly use. Awareness of the increased likelihood of a possible attack and the attack vectors that will be used, you can scan your external attack surface to see if any externally facing vulnerabilities need patches or adjustments.

Validate the adjustments

A central value of digital risk protection products and services from Mandiant is the ability to get ahead of attacks and make data-driven and proactive improvements to your security effectiveness. Mandiant Advantage Security Validation helps ensure the efficacy of your security controls and your ability to block, detect and alert on anticipated threats. Automated and continuous, Security Validation offers you visibility into how your security controls behave under attack to pinpoint gaps, misconfigurations and areas for improvement across your security architecture. Security Validation arms your security team with the ability to continuously test and optimize your cyber defenses and increases stakeholder confidence in your ability to defend against targeted attacks.

Digital risk protection from Mandiant is backed by industry-leading threat intelligence to help cut through the noise, understand the threats relevant to your organization and prioritize your resources. It provides visibility across your global external attack surface and the open, deep and dark web to give you the knowledge to prepare for attacks.