SOLUTION BRIEF

Gain Contextual Insights on Imminent and Current Threats With FortiRecon Adversary-Centric Intelligence

Executive Summary

Threat intelligence is a key requirement for every security operations center (SOC). But rather than receiving curated intelligence, often security teams must do their own time-consuming analysis to extract what's actionable and meaningful for their organizations.

Part of the Fortinet Digital Risk Protection (DRP) solution, FortiRecon Adversary-Centric Intelligence (ACI) is a result of intelligence from FortiGuard threat experts who monitor and assess the dark web, underground adversary forums, and open-source intelligence (OSINT) sources, curating intelligence pertinent to a company, geography, or sector. They gather information on imminent threats and illegitimately acquired data on an organization's behalf.

> "The more we know about attackers, the better we can respond to their actions."[1]

Curated Threat Intelligence Is Key

The volume of what is considered threat intelligence has ballooned astronomically in recent years, leaving security teams overwhelmed. Receiving custom, truly actionable information and enabling swift and effective protection is extremely difficult, if not impossible. The key to solving this growing issue is to receive curated intelligence from an outside source. This source must have the bandwidth and expertise to find and deliver the critical information security teams must focus on. This not only lessens the volume for teams to process but enables swifter action to protect an organization from imminent threats.

FortiRecon Adversary-Centric Intelligence Delivers Much-needed Insights

FortiRecon ACI provides contextual insights into imminent threats to organizations. This allows faster response to incidents, a better understanding of attackers, and the ability to safeguard assets.

ACI provides comprehensive coverage of:

- The dark web and other underground and invite-only forums
- Open-source intelligence sources
- Technical threat indicators from dominant and emerging threats
- Multi-language sources in over 10 languages

The intelligence includes threat-actor insights to help organizations proactively assess risks; look for vulnerabilities in existing on-premises, cloud, and remote presence; and increase the security awareness of staff.

ACI includes the results of human intelligence (HUMINT) gained by researchers' direct engagement in invitation-only, closed forums, dark web, open source, and other sources. Engaging in human intelligence collection, our analysts also assess and curate the intelligence for relevance to the given customer and assign Admiralty or NATO System confidence ratings for the reliability of the source and the assessed level of confidence in the information.

Intelligence provided to an organization is collected and can be filtered for:

- Sector-specific threats, such as a threat actor targeting VPN and RDP access in financial services organizations
- Geography-specific threats
- Threats to a specific organization, which are also sent as immediate alerts

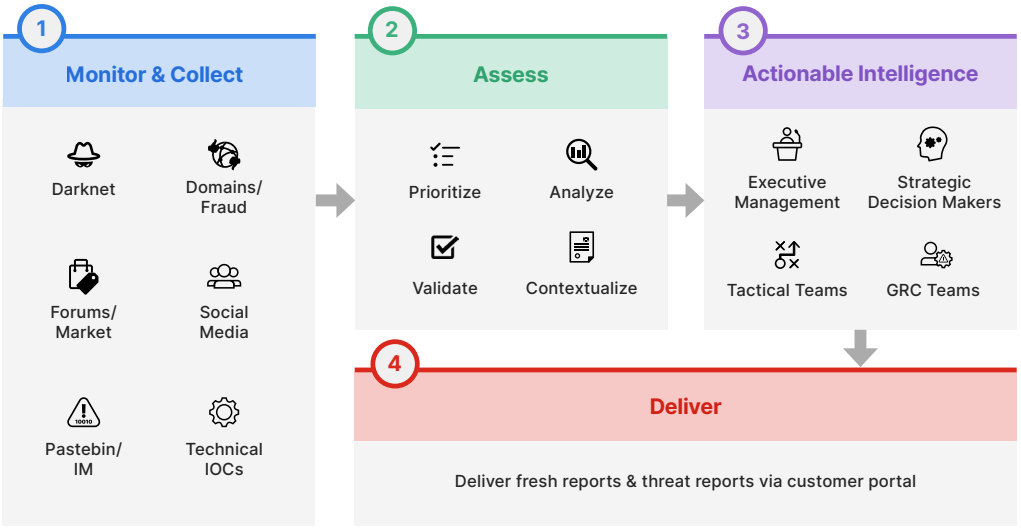
Threats to organizations can include, but are not limited to:

- Credential exposures
- Other leaked data
- Active vulnerability exploits in the wild
- New attack vectors
- New tactics, techniques, and procedures (TTPs)

Examples of such threats have included:

- Publicly exposed S3 buckets
- A threat actor selling access to an employee's system on the dark web

For the financial services industry, ACI can also include credit card BIN monitoring, with alerting on the first sign of a leaked credit card number.



FortiRecon ACI Results

Having such a highly skilled, experienced threat-intelligence team helps organizations:

- Directly and swiftly address immediate and imminent threats
- Reduce overall risk with knowledge of threat actor TTPs
- Alleviate threat intelligence overload
- Focus limited resources on what's most relevant
- Outsource access to, and engagement with, underground forums, not typically done by corporate SOC teams

Among other insights, intelligence is delivered via:

- Threat reports providing detailed information assessing the threat, along with recommendations to implement a proactive approach to defend against advanced threats
- Threat alerts providing timely information and initial findings about security issues, vulnerabilities, exploits, and darknet advertisement posts discovered by FortiRecon sources

FortiRecon Digital Risk Protection

FortiRecon ACI can be licensed with both FortiRecon Brand Protection and FortiRecon External Attack Surface Management (EASM). The full FortiRecon solution with Brand Protection, EASM, and ACI includes the following features:

- A breadth of coverage that includes digital asset discovery, data leak detection on underground and open forums, and brand attacks for swift action
- Takedown service for accounts, websites, and rogue mobile applications
- Licensing flexibility, for "outside-in" visibility when it's needed
- Executive to technical-level views with an intuitive graphical user interface (GUI)
- Threat and incident expertise access from additional FortiRecon analyst time to incident response and assessment services

Top FortiRecon ACI Benefits

- Curated intelligence to minimize organization's analysis time-to-respond
- Intelligence on threats specific to the organization, its industry, and region
- Broader intelligence collection from both OSINT and closed sources
- Increased knowledge of threat tactics, actors, and exploits, leaked data

Fortinet Delivers Comprehensive Security and Services

The Fortinet Security Fabric delivers end-to-end security across every stage of the attack lifecycle with FortiGuard threat intelligence for up-to-date protection. We also provide on-demand analysis, assessments, readiness services, and exercises. The FortiGuard Labs threat-research team is skilled at collecting, analyzing, and discerning the relevance of billions of threat events worldwide. We bring together this wealth of expertise, skilled dark web researchers, multi-language intelligence collection, and human intelligence specialists. This enables unrivaled access to threat intelligence and data on the latest threat activity, including restricted and invite-only forums. Almost a quarter of the total generated FortiRecon reports are done purely on the human intelligence that we collect, providing the most realistic view of risks.

Summary

FortiRecon ACI provides curated, actionable, timely intelligence to help keep organizations secure, act swiftly, and focus on only the most relevant and significant risks. Visit our website to learn more about FortiRecon.

[1] Scott J. Roberts and Rebekah Brown, "Intelligence-Driven Incident Response: Outwitting the Adversary," O'Reilly Media, Inc., accessed May 27, 2022." British Assessment Bureau, November 29, 2021.

FORTINET

www.fortinet.com

June 3, 2022 5:09 PM
1619982-0-0-EN