SOLUTION BRIEF

ATAR Labs Security Solution

Automated Investigation and Response With ATAR and Fortinet

Executive Summary

The integration of ATAR with the Fortinet Security Fabric creates a fast-acting environment that is highly responsive against threats, with top-of-the-line capabilities distributed across the enterprise at your fingertips. ATAR evaluates threats detected across your enterprise and during the investigation phase, and utilizes seamless FortiAnalyzer and FortiSandbox integrations to query information for improving the decision-making process. To stop adversaries, ATAR's full-blown orchestration and automation engine enables blocking malicious actors via FortiGate, FortiManager, FortiMail, and FortiDDoS solutions at machine speed.

Joint customers can enjoy the benefits of this integration out of the box, with no additional investment needed.

Business Challenge

Cyberattacks are increasingly becoming the number 1 source of risk for all enterprises; every organization tries to ensure that all attacks are defeated and their assets are protected. Insider and external attackers are successfully stealing data, tampering with databases, and forcing and stopping the execution of critical services. These attackers might be individuals, organized crime syndicates, competing corporations, and even nation-states.

Enterprises in all sectors are spending a great deal to secure their data, computing environment, and services from such attacks. However, this is becoming extremely challenging for several reasons:

- **Attacks are superfast now.** Attackers use malicious software to attack, which explains why we see attacks getting in, doing some harm, and getting out in 15–20 minutes today.
- **Organizations receive hundreds of cyber alerts a day.** Several hundreds of attack alerts a day, if not more, have become typical, and investigating and responding to all of these in real time is almost impossible.
- **Existing security tools do not work collaboratively.** This lack of cooperation of security tools results in poor overall protection.
- **Teams never have enough cyber experts.** In order to operate, organizations feel they always need more people. Due to these reasons, cybersecurity is a major challenge for many organizations.

ATAR Labs and Fortinet recently established a technology partnership to address the above challenges to help organizations automate and orchestrate incident response playbooks by leveraging the Fortinet Security Fabric.

Joint Solution Components

- Fortinet FortiGate, FortiManager, FortAnalyzer, FortiSendbox, FortiMail, FortiDDos
- ATAR Labs SOAR Platform

Joint Solution Benefits

- Gain fully automated and unified security operations through automation and orchestration capabilities and machine-speed decision-making
- Automatically block/unblock malicious IP addresses and URLs with FortiGate integration
- Block malicious email senders with FortiMail integration
- Leverage FortiManager's orchestration capabilities to take action on multiple devices
- Integrate FortiSandbox's malware analysis and FortiAnalyzer query results into ATAR incidents automatically

FORTINET FABRIC-READY

Joint Solution Description

The integration of ATAR with the Fortinet Security Fabric creates a fast-acting environment that is highly responsive against threats, with top-of-the-line capabilities distributed across the enterprise at your fingertips. ATAR evaluates threats detected across your enterprise, and during the investigation phase, utilizes seamless FortiAnalyzer and FortiSandbox integrations to query information for improving the

decision-making process. To stop adversaries, ATAR's full-blown orchestration and automation engine enables blocking malicious actors on FortiGate, FortiManager, FortiMail, and FortiDDoS solutions at machine speed. Joint customers can enjoy the benefits of this integration out of the box, with no additional investment needed.

Key features of the solution include the following:

- **Automated Alert Triage and Consolidation:** Prioritize which alerts are more important than others, sorting all alerts in order of priority. Analyze the alerts based on the organization's rules. Consolidate multiple independent alerts into a smaller number of consolidated cyber incidents for investigation to significantly decrease the total volume of work for the security operators.
- **Eliminate False Alerts:** Automatically collect additional data from systems and/or reach out to employees and ask questions to apply context to alert and reveal whether the alert was genuine or false.
- **Offload Security Teams via Automation:** Utilize the Fortinet Security Fabric and automate repetitive incident response steps, and allow security operations center (SOC) analysts to focus on things that require human intellect.
- **Increase Productivity:** Unify different tools and platforms by providing a unified command-and-control interface to greatly increase the productivity of SOC personnel and accelerate responses.

The functionality of the joint solution is summarized in the illustration below:

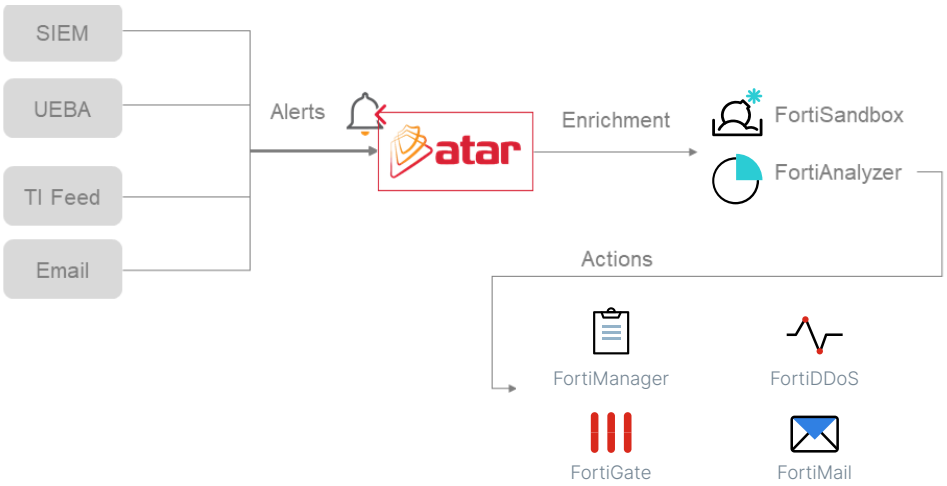

Figure 1: Automated incident investigation and response.

ATAR SOAR Platform

ATAR puts itself in the middle of the attack battleground, solving problems by creating a platform that can help the biggest, most technically capable SOC as well as the smallest of operations. An easy-to-use interface facilitates incident handling, and granular automation capabilities help reduce SOC personnel workload.

ATAR integrations serve as an organic extension of your analysts, helping them easily take a diverse range of actions without knowing the technology itself. ATAR chooses the best options and populates the most complex and required parts, allowing analysts to think about the incidents instead of the technical details of the technology.

A detailed audit trail and flexible design help SOCs shape ATAR to their own needs and work seamlessly.

The Fortinet products that ATAR integrates with are FortiAnalyzer, FortiDDoS, FortiGate, FortiMail, FortiManager, and FortiSandbox. These Fortinet products are part of the Fortinet Security Fabric, which provides broad, integrated, and automated solutions that enable:

- Security-Driven Networking that secures and accelerates the network and user experience
- Zero Trust Network Access that identifies and secures users and devices both on and off network
- Dynamic Cloud Security that secures and controls cloud infrastructure and applications
- Artificial intelligence (AI)-driven Security Operations that automatically prevents, detects, and responds to cyber threats

Use Case

Investigating and Blocking Phishing Campaigns

Challenge: Assessing the impact of phishing campaigns and blocking the adversaries can be time-intensive.

Answer: ATAR and Fortinet technologies collect additional data to fully understand the situation in an investigation and containment playbook:

1. ATAR follows email inboxes for users' phishing reports, extracts indicators of compromise (IOCs) (sender, IP, URL, file, etc.) from the reported suspicious email, and automatically creates an incident record on its service desk
2. ATAR sends file and URL to FortiSandbox and retrieves the analysis report
3. ATAR asks FortiAnalyzer for URL access logs for the last 12 hours
4. SOC analyst analyzes the reports and logs gathered and assesses the attack and its impact on the organization
5. ATAR blocks sender email domain on FortiMail to stop spread
6. Also blocks sender IP and URL via FortiManager/FortiGate
7. ATAR blocks user accounts and quarantines user PCs who have visited the malicious URL, to stop the malware spread
8. Analyst informs affected users and triggers eradication steps

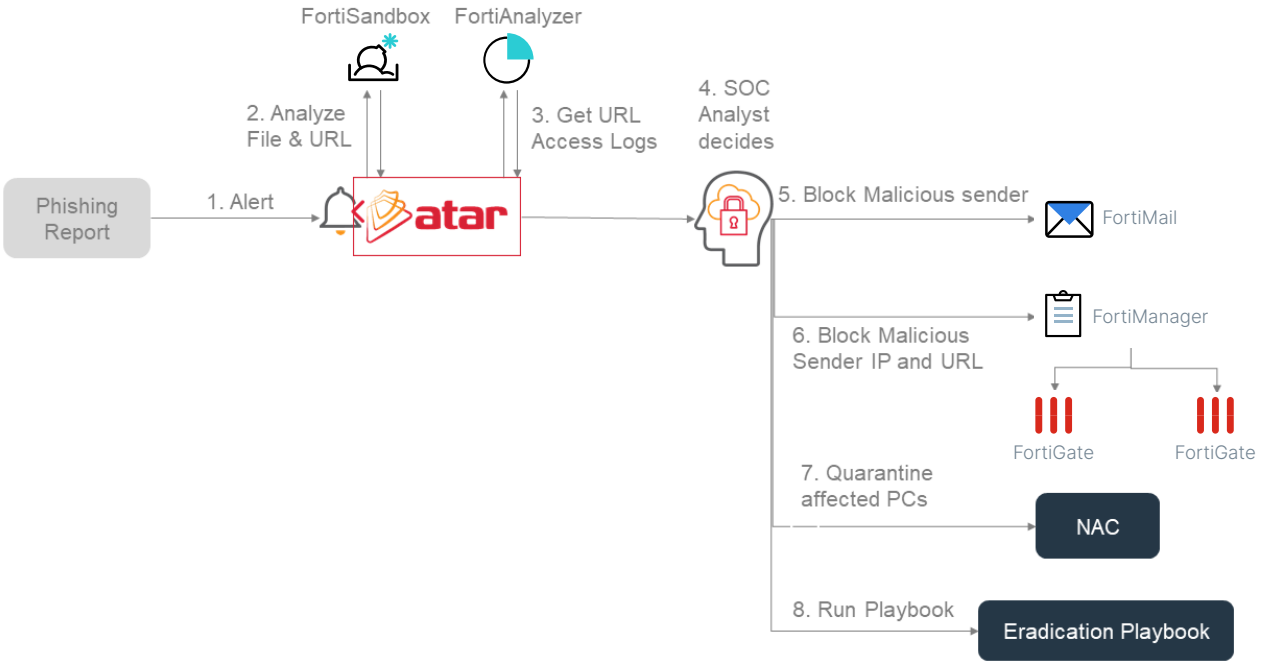

Figure 2: Workflow for example use case.

About ATAR Labs

ATAR Labs launches SOAR platform ATAR that supports organizations that cannot catch up with the speed and volume of cyber-attacks. ATAR defense robot automatically runs the pre-taught touch of a human expert. This means, while 30-40% of the total alarm handling the load is covered by the platform, incident investigation and response capabilities provided by ATAR allow the operation center experts to analyze and resolve incidents 15 to 20 times faster. To get more information about ATAR Labs visit www.atarlabs.io.

August 20, 2021 2:27 PM

sb-FA-atar-labs-security-solution-07212021

707454-A-0-EN