Recorded Future®

5 Ways to Automate Security with Intelligence

As threat actors increasingly utilize automation to scale their efforts and increase success rates, staying one step ahead of them requires more time and resources than ever before. The most effective way to combat this is by embracing a similar approach. Some organizations already use SOAR technology to create efficiencies — but **SOAR is just a single component** of a comprehensive automation strategy.

Here are five more ways your organization can leverage intelligence to automate processes and effectively defend against and respond to emerging attacks while empowering your teams to focus on higher-value tasks:

1 **Automate Intelligence Collection and Analysis**

2 **Automate Decision-Making With Confidence**

3 **Automate Intelligence in Existing Workflows**

4 **Automate Proactive and Dynamic Blocking**

5 **Automate Alerts**

Automate *Intelligence Collection and Analysis*

External visibility on threats is required for any security team to be successful, but **manually researching threats and IOCs is incomplete, inconsistent, and drains resources.** With natural language processing and machine learning, it becomes possible to scale collection and automatically analyze data across an incredibly broad range of open, closed, and technical sources. This **drives efficiency across all teams** by providing organizations a comprehensive view of external threats in real-time.

1

Automate *Decision-Making With Confidence*

Quickly identifying and validating malicious activity is imperative to protecting an organization, but **analysts don't have time to manually triage every alert and IOC that shows up in their environment**. Relevant security intelligence can deliver real-time context and empower security teams to quickly triage out false positives based on supporting evidence. The most sophisticated intelligence solutions enable organizations to **automatically identify high-priority alerts** and easily drill into original sources and evidence for deeper analysis.

2

Automate *Intelligence in Existing Workflows*

Security teams spend a great deal of time working in powerful security tools, including SIEM, SOAR, firewalls, and other systems. **Pivoting from one workflow to another system to access intelligence can waste valuable time**. By integrating security intelligence directly into existing tools, security teams can automatically access the rich context required to **make better, faster decisions — without disrupting workflow**.

3

Automate *Proactive and Dynamic Blocking*

Facing constant data overload, **security teams need access to high-confidence indicators** to proactively block threats. Using a solution that delivers high-confidence indicators that are updated in real time enables organizations to integrate the indicators directly into security controls including firewall, email security, and endpoint solutions to **block threats before they enter the environment**.

4

Automate *Alerts*

For many organizations, it's difficult to identify specific threats targeting them. By using a tool that enables automatic alerting based on customized watch lists for groups of people, places, and organizations of interest, security teams can find out immediately when their company, subsidiary, and product names are mentioned, or infrastructure is at risk. With the option to drill down and view original sources of intelligence, teams can **respond faster and more effectively than ever before**.

5

AUTOMATING INCIDENT RESPONSE PROCESSES WITH SOAR

Many security teams embrace SOAR technology to automate incident response and other security processes as a first step towards relieving the pressure of the cybersecurity skills shortage. Quality sources can amplify these platforms by automating evidence-based intelligence to act as an initial decision point — which eliminates most of the required human research. Organizations can create playbooks that use real-time, contextual intelligence to automate processes intelligently.

Ready to Supercharge Your Security Processes?

Recorded Future provides a single solution to automate all of the processes mentioned here, and more!

Request a demo to find out how you can and combat threat actors with automation.

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.