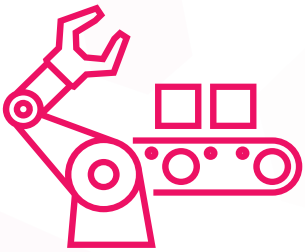
themissinglink
Australia • United Kingdom

UiPath™

Robotic Process Automation for Cyber Security Professionals: An explainer

Cyber security professionals shoulder their fair share of mundane, repetitive tasks that take time and attention away from what's most important – detecting cyber threats and preventing and responding to cyber-attacks. RPA allows your team to focus on what they do best. So, what is it, and how can your organisation take advantage?

What is RPA?

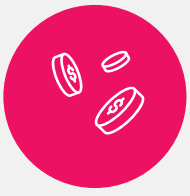


Robotic Process Automation (RPA) is a technology that makes it easy to build, deploy, and manage software robots. These robots emulate the actions usually undertaken at work as they interact with digital systems and software. It's the ultimate scalable digital workforce.

The benefits of RPA

Increase efficiency

Increase productivity



Reduce costs

Remove human error

Free employee time

How can Cyber Security Professionals use RPA?

RPA bots are essential tools to add to your cyber security arsenal, especially as the cyber security landscape continues to become more complex.

They can decrease human error, stamp out unauthorised access, increase the reliability of threat detection and reduce time spent responding to attacks.

Check out some use cases below...

1

Optimise threat detection and prevention

Bridge the gap between identifying indicators of compromise using security monitoring tools and carrying out remediation actions manually.

Trigger RPA bots from other security operation tools such as endpoint detection and response (EDR), extended detection and response (XDR), or security information and event management (SIEM).

2

Improve incident response

Accelerate remediation and help maintain consistent incident response processes.

Automate activities like deleting or quarantining suspicious malware-infected files, performing geolocation lookups on IP addresses and blocking URLs on endpoints – plus much more.

3

Enhance audits and monitor compliance

Ensure compliance to industry standards like ASD-8 and GDPR, optimise internal reporting, and perform smoother audits.

Monitor compliance by proactively stopping any control failures and alerting the appropriate stakeholders. For audits, RPA bots can gather information, generate reports, and distribute those documents to identified contacts.

4

Managing the identity lifecycle

Save time spent on identity management activities (which are equally important and mundane) and redeploy to more complex tasks.

Automate identity management activities like user provisioning, controlling application access, resetting user passwords, and unlocking user accounts.

Automation to ensure compliance

We all make mistakes. It's part of the human condition – but sometimes we can't afford to make errors when it comes to cyber security processes. RPA can help businesses demonstrate their compliance to ISO 27001 requirements more easily. For example, here's how employee onboarding/offboarding works at The Missing Link:

Onboarding

Automated standard IT onboarding tasks saves 40 mins of time per user.

Benefits

- Onboarding tasks executed on time for new starters.
- The consistent and accurate creation of user accounts.
- 100% accurate - broken focus due to conflicting priorities, can cause minor errors from manual processing.
- Frees up skilled L2 resources to spend time on value-adding coaching and problem solving.

Offboarding

Automated standard IT offboarding tasks saves 30 mins of time per user.

Benefits

- Automated 100% of critical-to-security IT offboarding tasks, building and accounts access.
- Removes the risk of incurring pro rata licensing costs.
- The task is always done on time, removing the requirement for The Missing Link support staff to work late to perform critical offboarding tasks.
- ISO compliance requirements met.

SOAR vs. RPA

Working in Cyber Security, you may already be familiar with a Security Orchestration, Automation, and Response platform (SOAR). Though similar, RPA and SOAR have a few key differences and can enhance the workday of a Cyber Security Professional in unique ways.

SOAR	RPA
Purpose-built tools for Cyber Security teams.	Broader set of automation tools useful across many industries.
Interacts with specific security tools and software to perform rigid tasks.	Can automate a wide variety of processes including processes involving systems without APIs.
Only responds to identified threats.	Simple to implement and scale.

SOAR and RPA are a dynamic duo that can work together. In fact, we've already taken advantage of their combined capabilities to be more efficient in The Missing Link's Security Operation Centre (SOC).

Our SOC Bot: A case study

Organisations across all industries are realising a minimum of x5 ROI within the first 12-24 months after implementing a digital workforce using RPA – and our very own SOC is no exception.

Proof of Value: Critical Advisory Email (Microsoft)

How it works

Our RPA bot produces an advisory email twice daily (at 5 am & 5 pm). Each time, our bot:

- Monitors for critical vulnerabilities
- Extracts advisory data; and,
- Generates The Missing Link advisory email.

Benefits

- The email saves ~2 hours of a real team member's time.
- A scalable solution which enables our SOC to meet ASD Level 3 requirements.
- PoV version used to generate collateral for marketing/sales.

Pilot: Critical CVE Notifications

How it works

Our RPA bot produces a list of new critical CVEs twice daily (at 5 am & 5 pm). Each time, our bot:

- Monitors for critical vulnerabilities; and,
- Notifies The Missing Link via Teams.

Benefits

- The notification **saves an average of an hour of a real team member's time each run.**
- Increased visibility into the latest vulnerabilities and improving the quality of SOC services.
- Rapid notification of new critical CVEs, where previously this would take 1-2 days or not at all.
- A searchable audit trail.
- Ability to track the quality and volumes of the NVD feed, to inform the advisory process.

Rapid7 IDR Monthly Report

Benefits

Increased focus on service improvement and proactive analysis

Improved accuracy and reduced review rework

Improved deadline compliance, faster turnaround time of report

~250 hours of time saved each year

Contact us

Ready to transform your Cyber Security Operations and unlock greater efficiency using RPA? Reach out to our team.

GET IN TOUCH

Or call 1300 865 865

themissinglink®