AUTOMATION MYTHS

A security expert's guide to
Incident Response and Automation

RESOLVE SYSTEMS™

MYTH #1

ALL SECURITY PROCEDURES MUST BE DEFINED BEFORE WE CAN AUTOMATE

Organizations are constantly undergoing initiatives to build out manual processes for the Security Operations Center (SOC). Process is imperative for the success of a SOC and without these processes in place, we cannot leverage an automation platform.

MYTH PARTIALLY TRUE:

Security staff who have been educated on clearly-defined, repeatable processes are paramount to creating and maintaining a high-functioning security organization. With typical scripting and end-to-end automation solutions, documenting predefined processes is necessary to reference as automations are developed to avoid automation chaos. Documented standard operating procedures are necessary to train staff and provide auditors with visibility. However, due to competing priorities, and in some cases lack of knowledge, a fully-baked security procedures manual is often an unattainable grail for security groups.

By leveraging a Unified Security Incident Response platform, automation can be added pragmatically and partially along the way, as organizations figure out their procedures. Parts of the process can be automated when they are defined and ready for automation. With the right solution in place, that includes capabilities such as: Process Guidance, Human-Guided Automation, End-to-End Automation, pre-built Playbooks and Security Case Management, security procedures can be developed as part of implementing automation.

SEE SECURITY SOLUTIONS >

“With the right solution, security procedures can be developed as part of implementing automation!”

MYTH #2

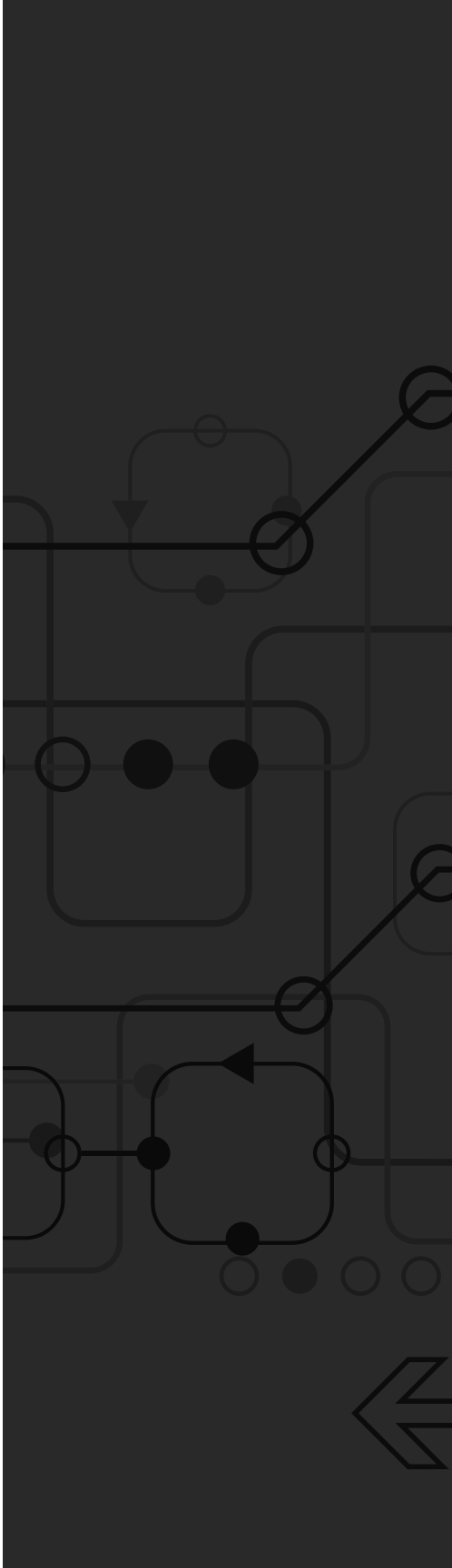
MY FIREWALLS, ENDPOINT PROTECTION, AND SIEM WILL SAVE ME

Our security organization has the best and brightest deploying state-of-the-art layer 7 firewalls, next generation endpoint protection, the most expensive SIEM money can buy, and even a Heisenberg Compensator to help transport away any attack a hax0r 133t can throw at us. There's no chance of us being breached, because our preventative technical security controls are stellar!

MYTH PARTIALLY TRUE:

This myth is 100% busted, but we agree that your organization is staffed with rockstar security minds and that your preventative security tools are top-notch. There's no argument that having good preventative and detective measures in place is best practice. But prevention solutions are only half the battle. When prevention tools notify an analyst of an issue, security teams must have the ability to access a tool that will help them resolve the problem quickly and easily. The truth is, you're going to be breached at some point. Prevention solutions aren't infallible and it's crucial to have an Incident Response playbook and technology in place to enable you to resolve security incidents in an organized and timely manner.

6 TIPS TO MAXIMIZE SECURITY INVESTMENT >



MYTH #3

BUILDING AUTOMATION IS TOO DIFFICULT...WE DON'T HAVE THE SKILLS OR THE TIME TO AUTOMATE!

Our security team is understaffed and overwhelmed! We're too busy fighting fires to even think about esoteric notions like automation. It takes a lot of time and a PhD in Rocket Science to develop and implement.

MYTH BUSTED!

While typical approaches to automation can be extremely time-intensive to develop, limited in functionality and a management nightmare, not all automation solutions are created equal. A tool like Resolve removes the complexity of coding and puts automation in the hands of the people who may not know how to code, but know how to solve problems. These are the people who are going to help build automations. Find a Unified Security Incident Response platform with pre-built Playbooks and easy-to-use process and automation building tools to enable security teams to streamline operations from day one...no coding skills required. Work smarter, not harder.

VIEW AUTOMATION TEMPLATES LIBRARY >

MYTH #4

MY TEAM IS MY FAMILY....I'M NOT INTERESTED IN AUTOMATING JOBS AWAY!

The main purpose of "automation" is to make operations more efficient in order to reduce costs and headcount. I've assembled an elite cybersecurity squad that eliminates any security issues thrown their way. Even if I could automate one or two of their positions away, I wouldn't.

MYTH PARTIALLY TRUE:

Sure, automation can be used to enable workforce reduction. The advent of the assembly line enabled Model T's to be built at unfathomable speeds. Robotics fused with assembly lines allow for almost fully autonomous factories. However in the cybersecurity world, where skilled security professionals are in high demand and extremely low supply, this couldn't be further from the truth. Automation, when utilized as part of a Unified Security Incident Response platform, frees up people from doing the menial, time-consuming tasks and gets them out of reactive mode, allowing for more time to focus on areas that are more meaningful to them. Automation, when done right, allows high-functioning security teams to cut through the noise and focus on resolving their security.

VIEW INCIDENT RESPONSE PLAYBOOKS >

MYTH #5

THE OVERZEALOUS AUTOMATION FAN

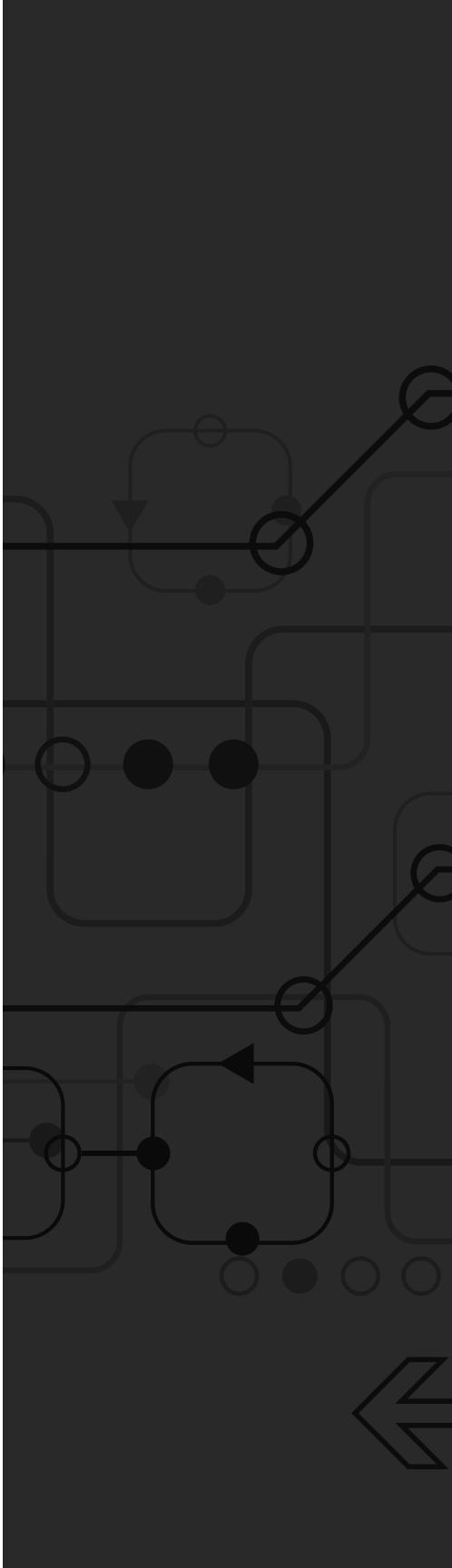
Automation is the answer to all of our security incident response needs. With the right automation solution in place, we'll be able to run our entire security program using nothing more than Ted the new intern. No need for us to employ costly security specialists.

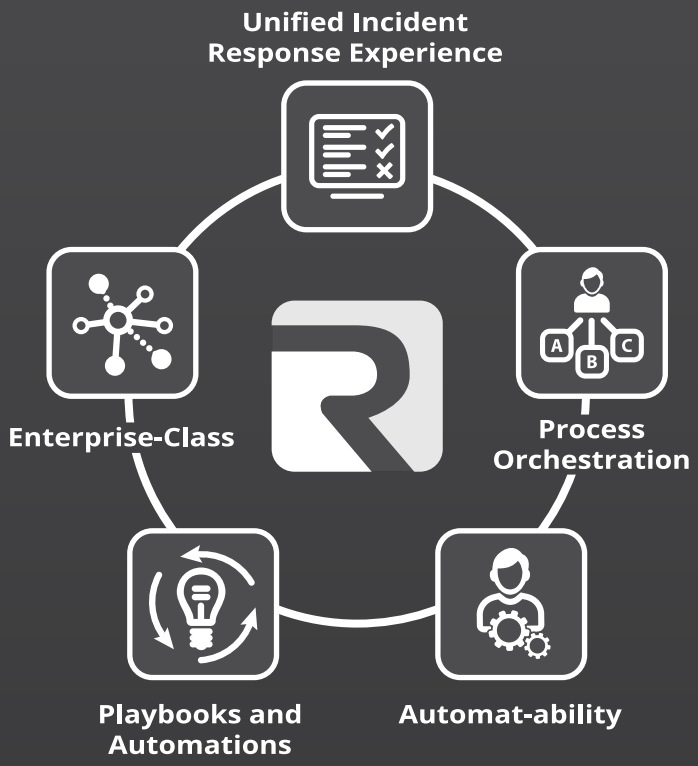
MYTH BUSTED!

Some vendors market and oversell capabilities and unfortunately, the technology doesn't live up to expectations. We wish automation was the solution to every issue. The truth is, especially in security incident response, automation alone will fall short; humans are absolutely required. A Unified Security Incident Response solution like Resolve empowers the team and they are critical to making cognitive decisions and helping with more complex use cases, which improves communication and processes. Automation empowers humans to do their job better and more effectively.

Resolve Systems is the most widely-deployed enterprise Security & IT Incident Response Automation Platform. Resolve takes action on your security events by delivering an organized and automated approach to incident response.

READ WHITE PAPER >





Resolve Systems is the most widely deployed enterprise Security & IT Incident Response Automation Platform. Resolve takes action on your security events by delivering an organized and automated approach to incident response.

CONTACT US

WWW.RESOLVESYSTEMS.COM