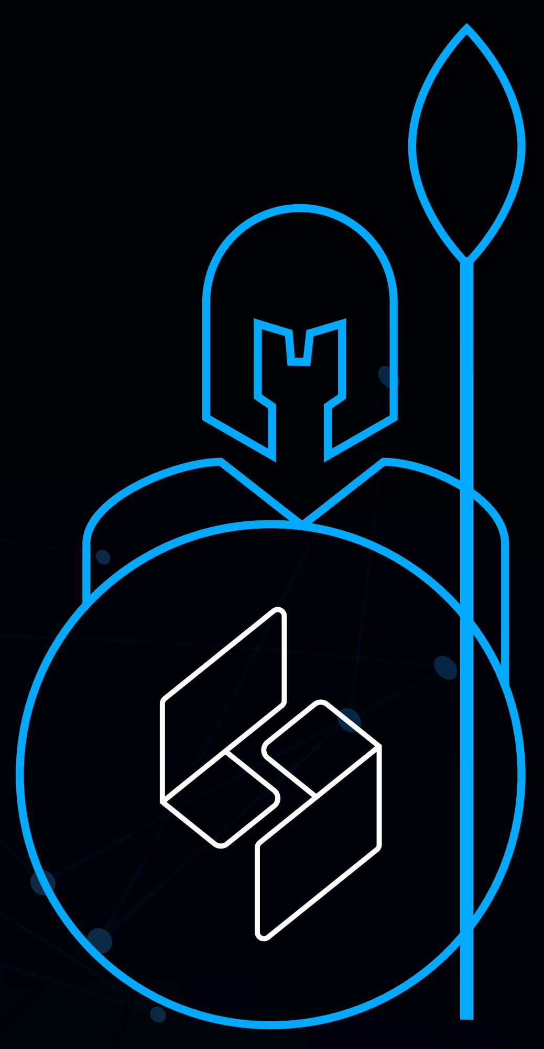
SWIMLANE

# ARMING **YOUR SOC**

With Security Orchestration, Automation and Response (SOAR)



## Increased **Vulnerabilities**

### Attackers Capitalizing on Human Vulnerability

Google reported a

**350% increase**

in **active phishing websites** since January 2020

*Source: www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine*

**Social Engineering**

Phishing emails

Domain registrations

Trusted brand impersonation *(WHO, CDC)*

Financial themes *(stimulus, loans)*

**Working From Home**

Inadequate protections *(Using personal devices for work projects/access)*

Maintaining connectivity *(VPN status monitoring)*

## Current State **COVID-19/Coronavirus**

### Shrinking Budgets

Estimate Worldwide IT spending

**5.1%**
January 2020

**-2.1%**
March 2020

*Source: https://www.idc.com/getdoc.jsp?containerId=prUS46186120*

### Existing Exposure

of cyber incidents are caused directly by employees

*Source: https://www.willistowerswatson.com/en-US/Insights/2020/06/after-covid-19-cyber-and-the-coming-remote-work-revolution*

### Expanded Landscape

Gartner found that **74%**

of organizations plan to shift some employees to remote work permanently

*Source: https://www.vox.com/recode/2020/5/21/21234242/coronavirus-covid-19-remote-work-from-home-office-reopening*

## Benefits of **SOAR**

### More Effective Use of Existing Resources

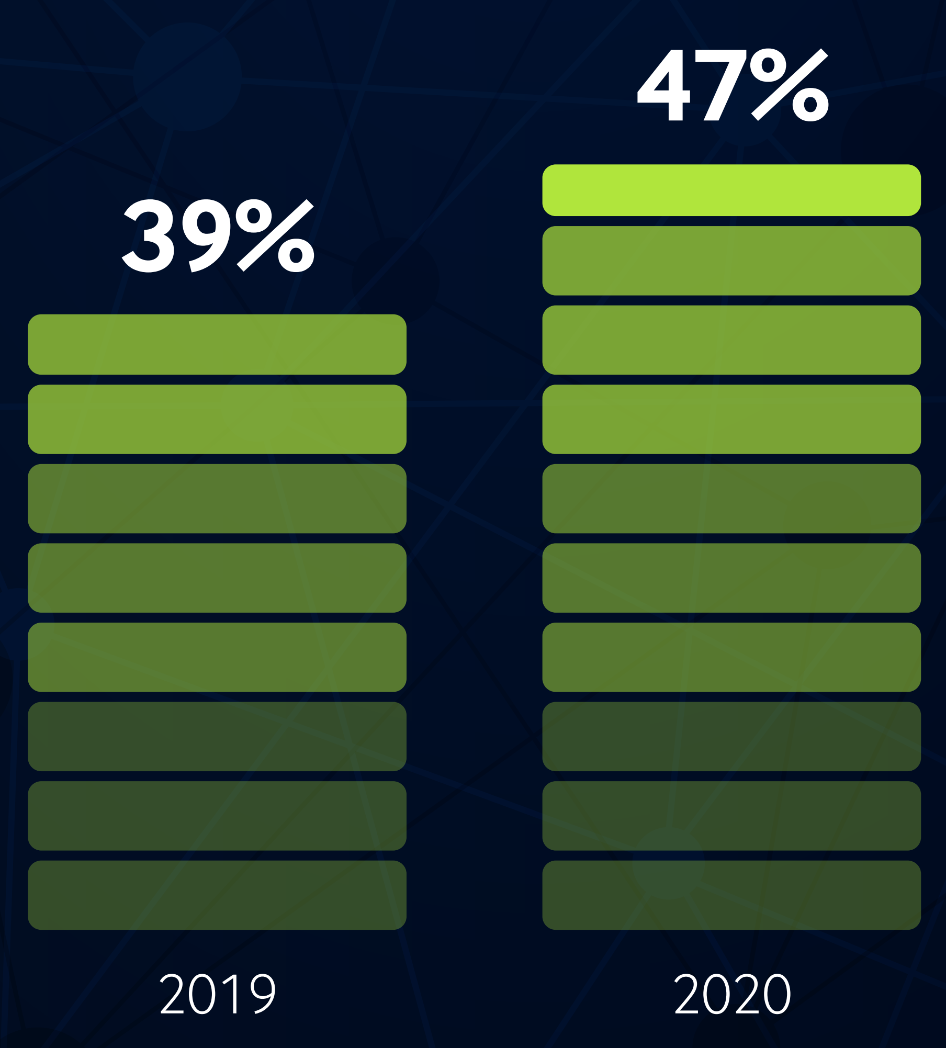
Personnel not tied to manual, repetitive, time-consuming tasks

Orchestration, automation and response occur at machine speed

Integrate existing tools to form a cohesive armament

Single tool to learn

**Automation adoption continues to rise**



*Source: 2020 SANS Automation and Integration Survey*

swimlane.com

© 2020 Swimlane