

Accelerating Security Response through Automation

Incorporating Threat Intelligence into security tools

Apollo Hernandez & Zach Brabham

splunk > turn data into doing®



Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

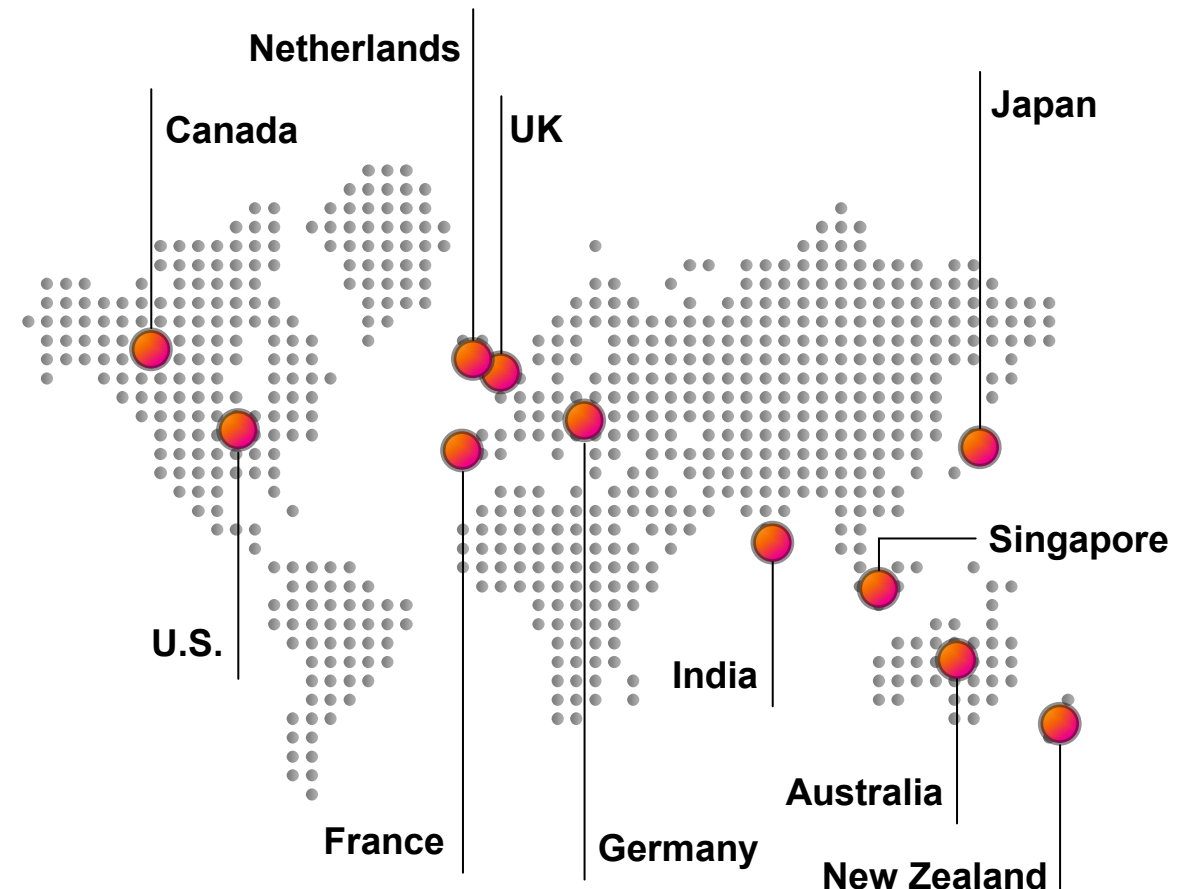
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2022 SPLUNK INC. All rights reserved.

Methodology and Demographics

Between Jan. 19 and Feb. 11, 2022, researchers surveyed 1,227 security and IT leaders who spend more than half their time on security issues.

- **11 countries**
- **15 industries**
 - Aerospace and defense, consumer packaged goods, education, financial services (banking, securities, insurance), government (federal/national, state and local), healthcare, technology, life sciences, manufacturing, media, energy, retail/wholesale, telecom, transportation/logistics, utilities



Why Security Keeps Getting Harder

A year-over-year comparison reveals that security teams face more threats and more complexity, but also have fewer people to get the job done.

Challenges of increasing severity revolve around too many tools, too few analysts, and not enough time.



2022

2021

*Top 7 responses

The events over the past two years have changed the world forever...

Fueling investments in **innovation** and **resilience**

Remote work has surged

46%

work remotely today, compared with 21% working remote pre-pandemic*

Digital transformations are now in high gear

83%

say cloud is important to future growth – critical to accelerating **digital transformation to innovate and compete***

The changing **threat landscape** is outpacing security programs

64%

of organizations find it **harder to keep up** with security requirements*

*Splunk State of Security 2022



But these
investments
often **create**
more data
problems

Magnifying existing challenges in securing your business today...

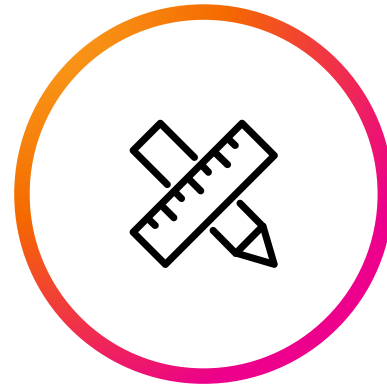
and creating further **SecOps Inefficiencies**



**Lack of
Visibility**



**Expanding
Attack Surface**



**Tooling
Complexity**



**Skilled Resource
Constraints**

Security Teams Are Firefighting

Security teams spend 31% of their time fighting crises (up from 26% last year) rather than preparing for supply chain, ransomware and other attacks.

Why?

- **26%** cite overwhelming tool complexity.
- **29%** cite hiring or retention challenges.
- **28%** cite cloud complexity and lack of visibility.

Talent in Crisis

Security talent is harder to find (and keep) than ever before. The ongoing talent challenges have led to a number of issues

A circular infographic with a purple border and a white center. The number '70%' is written in purple. The circle is partially filled with a purple arc.

70%

Say that the resulting increase in their workload has led them to consider looking for a new role

A circular infographic with a pink border and a white center. The number '76%' is written in pink. The circle is partially filled with a pink arc.

76%

Say team members have been forced to take on responsibilities they aren't ready for

A circular infographic with an orange border and a white center. The number '68%' is written in orange. The circle is partially filled with an orange arc.

68%

Report that talent shortages directly led to the failure of one or more projects/initiatives

A circular infographic with a yellow border and a white center. The number '73%' is written in yellow. The circle is partially filled with a yellow arc.

73%

Say that workers have resigned, citing burnout

The State of Cloud

The still-growing role of cloud computing has become essential to organizations, but it has also hampered security visibility.

- **73%** of organizations use multiple public clouds today.
- **34%** use three or more public cloud service providers.
- **56%** expect they will use three or more public cloud service providers (IaaS and PaaS) 24 months from now.

The two main cloud-native security challenges

- Maintaining consistency across data centers and cloud (**45%**)
- Using multiple security controls, which leads to cost and complexity (**37%**)



Attacked From All Sides

Following the SolarWinds, Kaseya and Log4Shell attacks, supply chain threats are front and center; 40% of survey respondents said that their organization had been affected by a supply chain attack, and 90% of orgs have increased their focus on third-party risk.

But other threats abound:

- **Ransomware:** 79% were attacked; 20% had data/systems held hostage.
- **Phishing:** 51% report business email compromise.
- **Insider attacks:** 39% of organizations report an inside job.

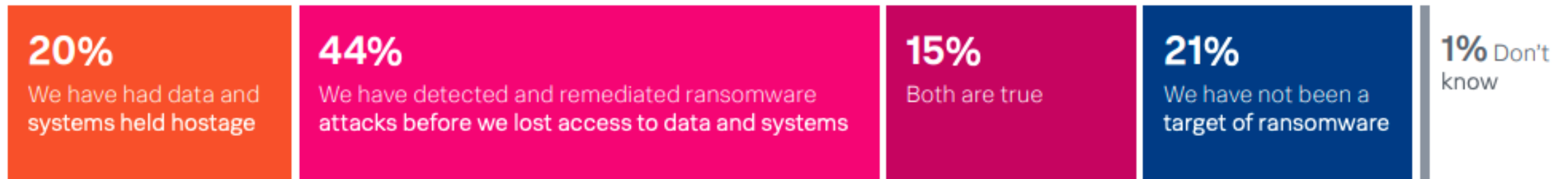
Ransomware: Get Your Playbooks Ready

Among respondents who fell victim to a successful ransomware attack:

- Only **33%** avoided the ransom by restoring from backup.
- About **66%** reported that the criminals were paid.
- Asked how much the largest ransom paid to attackers was, the average response was about US **\$347,000**.

Most Orgs Were Ransomware Targets

79% fended off an attack ... or fell victim.



The Most Promising Security Strategies (Besides Hiring)

Not all doom and gloom

Organizations can turn to other strategies to bolster their security posture and alleviate at least some of the pressures that their security teams face.

47%

Better capture and analysis of security data

52%

Use of increasingly automated solutions (powered by AI/ML) to detect and respond to cybersecurity incidents

41%

Increasing use of MSSPs/outsourcers

45%

Simplifying security tool portfolio via vendor rationalization/using more platform-based controls

41%

Increasing investment in commercial security controls

58%


Increasing the level of investment in security training for IT/cybersecurity staff



Organizations are investing in resilience

By 2025, Gartner predicts big changes in attitudes and resources devoted to resilience


70%



of CEOs will mandate a culture of organizational resilience

To survive coinciding threats from COVID-19, cybercrime, severe weather events, civil unrest and political instabilities¹


50%



of asset-intensive organizations will expand their operational resilience initiative

To include the growing security and safety risks of cyber-physical systems (CPS)

30%



of enterprises will establish new roles focused on IT resilience

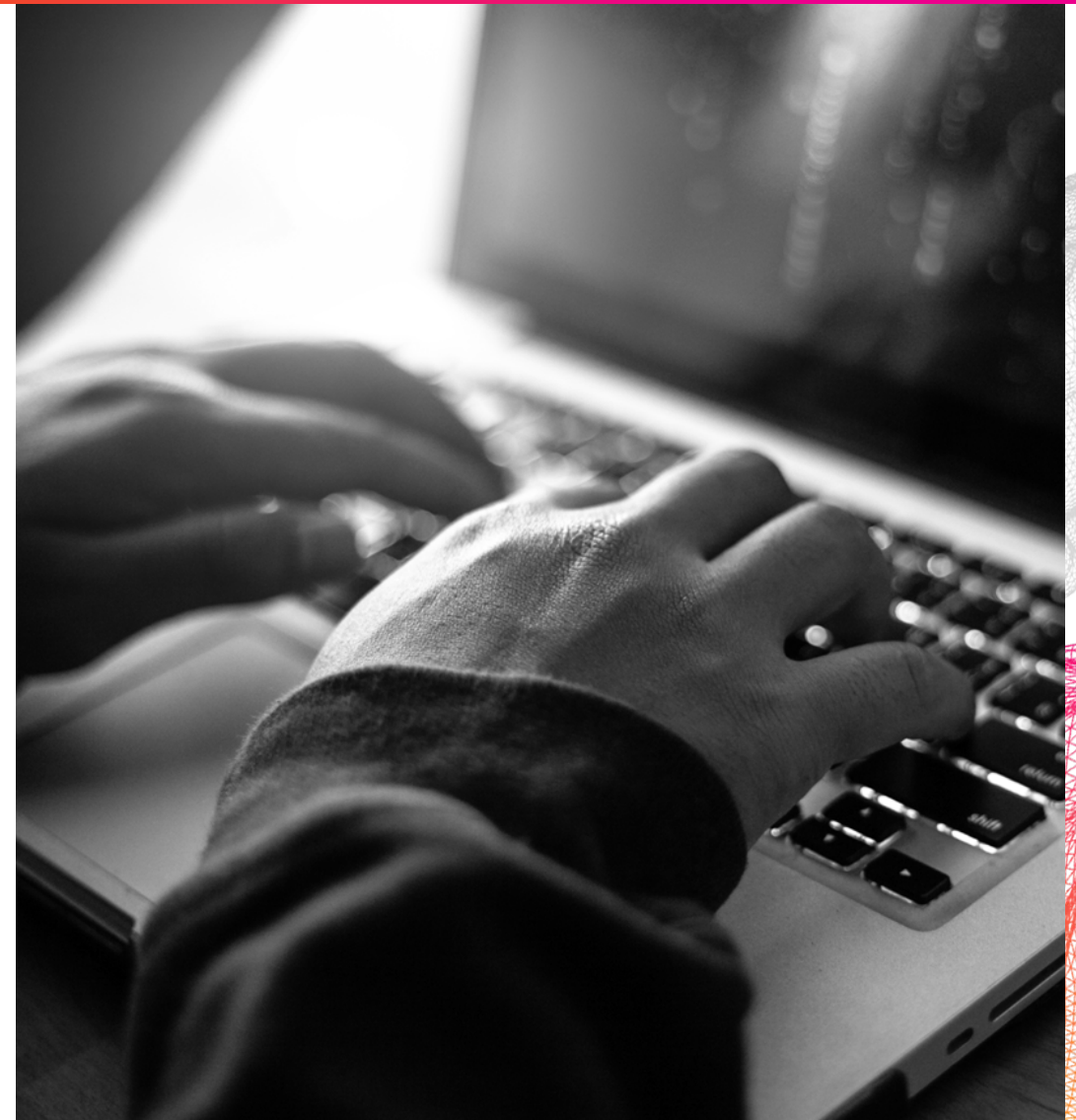
and boost end-to-end reliability, tolerability and recoverability by at least 45%²

Sources:

- (1) Gartner, Outlook for Organizational Resilience, 2021
- (2) Gartner, IT Resilience — 7 Tips for Improving Reliability, Tolerability and Disaster Recovery

Driving an increased need for **cyber resilience**

“The ability to **anticipate, withstand, recover** from, and **adapt** to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”



Our fundamental belief

Security is a data problem

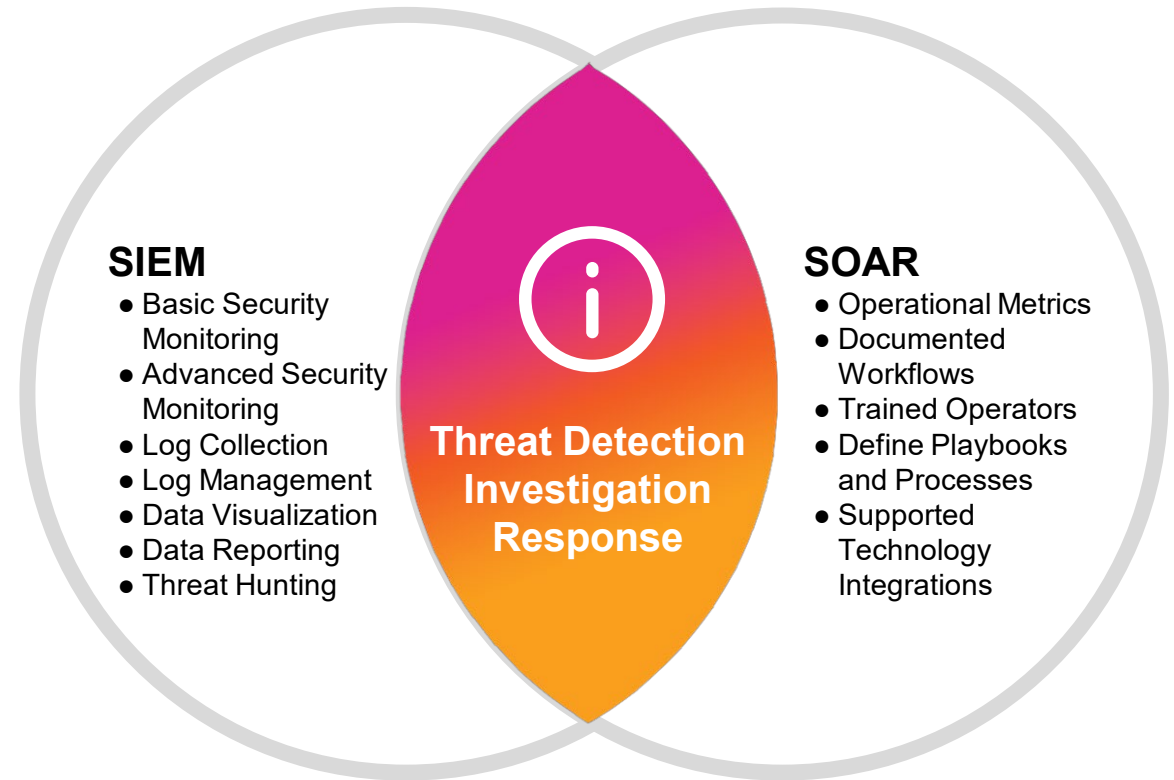


**An incident is
an incident**



**All data
is security
relevant**

SIEM & SOAR Merging

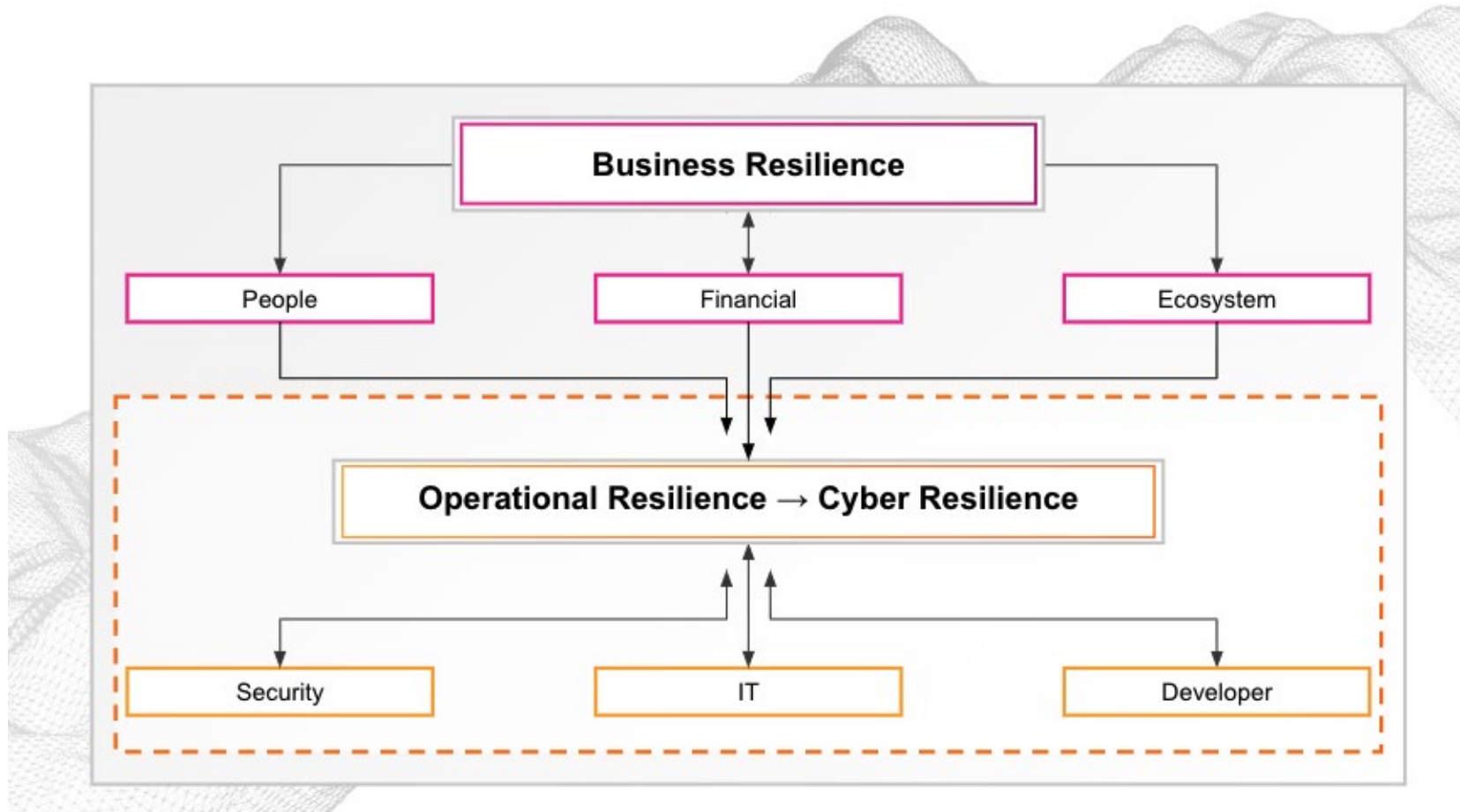


[SOAR Will Not Make You Better at Running SIEM](#)

Published 4 May 2022 - ID G00759000

By Analyst(s): AI Price

Business Resilience demands Operational Cyber Resilience



Analytics and Automation Are Essential for Cyber Resilience

Analytics and automation capabilities let security analysts work smarter and respond to threats at machine speed.

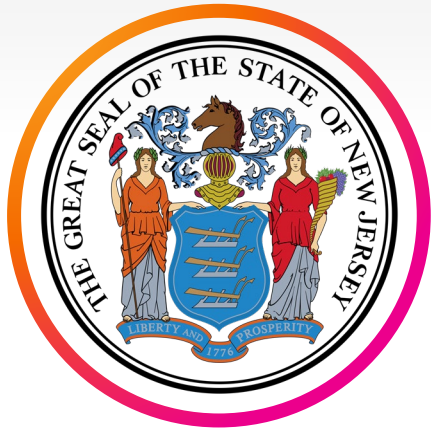
- **82%** of respondents say their CISO is under pressure to increase their data analysis capabilities.
- Fully **85%** (up from **82%** last year) say that security analytics plays a bigger role in their overall cybersecurity strategy and decision-making today than it did two years ago.



Organizations' strong investment in analytics, automation and SOAR technologies continues.

- **67%** of organizations are actively investing in technologies designed for security analytics and operations automation and orchestration.
- Of those, **35%** report their organization uses or will use the automation and orchestration capabilities built into their SIEM.

*77% of organizations have integrated non-security analytics solutions (for **DevOps, IT operations, Risk Management**) with cybersecurity-specific analytics to support decision-making.*



STATE OF NEW JERSEY

Department of Labor

- ▶ **Situation:** Fraudulent unemployment claims have been submitted at an unprecedented rate since the Pandemic Unemployment Assistance program first launched. At that time, there were approximately 1,800 – 2,000 fraud claims, daily. The NJ Department of Labor's Anti-fraud teams were not able to make sense of their data; the starting point was to mine data, consolidate reporting tools, and refine/evolve processes. At the time, NJ DOL were estimating losses in the millions due to this issue. Professional fraudsters were able to easily circumvent existing controls.
- ▶ **Task:** In tandem with a partner, a fraud dashboard was created to detect fraudulent claims before payment was made. The dashboard could be used to search any information on an application, including pre-populated, free-form or formatted data. The dashboard provides the amount of payments made, differentiates in-state and out-of-state zip codes and sends alerts when certain anomalies are detected. Executives can schedule reports detailing weekly, monthly, quarterly, and yearly metrics.
- ▶ **Action:** The dashboard has been able to detect fraudulent claims before payment was even made. It has been used in production over the last two years to help prevent millions of dollars in UIB fraud.
- ▶ **Result:** The Department of Labor been able to save the state \$6.7 Billion dollars in fraudulent claims.



LOCAL SCHOOL DISTRICT

United States

- ▶ **Situation:** Largest county in the State. The IT team for the county oversees 40+ different physical locations. They had a breach of emails that led to people's accounts and credentials being compromised. This breach allowed people to access their network and the capability to make modifications to Peoplesoft including alterations to direct deposit account information. They had no centralized log management tool to do the research within the logs to find the root cause of the breach, which led them into a slow manual process for investigation. They had a specific timeframe to act on the breach and this was made more difficult by the data silos they had to comb through.
- ▶ **Task:** The security team was tasked with implementing a single solution log management tool with centralized visibility into the log data from all the 40+ locations within the county. Also, they were tasked to reduce the meantime to response, since the manually processes were taking them 4-6 hours on average.
- ▶ **Action:** They focused on centralized visibility into their IT infrastructure to ultimately reduce their risk of threats as well as their meantime to response. Their identified data sources to ingest into their SIEM are; VPN logs, Syslog Kiwi Devices, O365, Windows/Linux Servers, Internal Exchange Server, SEP Management Console, and SEP EDR logs.
- ▶ **Result:** After implementing their SIEM and focusing on a data centric solution, they were able to reduce their mean time to response from 4-6 hours to near-real time with advanced dashboarding/automation. They now have the ability to use this valuable threat intel to distribute amongst their different locations to alert faster and mitigate before anything serious happens.

Thank You



Key Recommendations

What more you can do beyond increasing security spending

- 1. Seek talent, teach skills:** Look beyond the traditional security workforce and hire for raw talent, versus trained skills.
- 2. Know your cloud:** Everyone from senior security leadership to tier-one security analysts needs to understand their hybrid, multicloud environment.
- 3. Build Partnerships**
- 4. Use automation:** Enhance your analysts, not replace them.
- 5. Consolidate sprawling toolsets:** Make sure your team has the right tools for the right jobs, while also making sure it can manage the responsibility of care.

