Krista™

Technology that understands people.™

Intelligent Automation for Security Orchestration

There are only 24 hours in a day, so making the best use of that time behooves your security posture. Security automation using an intelligent automation platform connects and orchestrates disparate tools and feeds to provide your security analysts more research time. Automating the incident management process using intelligent automation and AI provides enterprises information on which alerts immediate attention. By eliminating time-consuming administration processes and centralizing communication, teams can more effectively neutralize attacks, reduce human error and reduce the meantime to recovery (MTTR).

> 35% of cybersecurity professionals say that the biggest challenges associated with managing an assortment of point tools is that it makes security operations complex and time consuming.

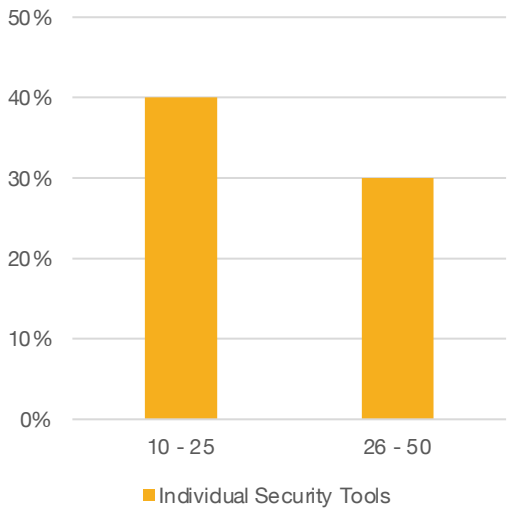
Security organizations have too much to do

ESG recently surveyed security professionals to reveal:

- 40% of security organizations use 10 to 25 different tools, while 30% use around 26 to 50.
- 27% of cybersecurity professionals say they receive too many alerts.
- 35% say that one of the biggest challenges is managing an assortment of point tools.
- 51% of these organizations have a shortage of staff.

There is a shortage of trained staff to respond to millions of alerts. To add to it, SOC teams are primarily involved in doing repeatable, mundane tasks instead of focusing on higher priority tasks, which is to respond and research security threats. Further, security teams grapple with an overload of point tools adding to the confusion and complexity. Together, this can be a recipe for disaster leading to devastating consequences for the organization.

How many security tools do you use?



SOAR Platforms

Security orchestration, automation and response (SOAR) solutions combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. SOAR tools are also used to document and implement processes (aka playbooks, workflows, and processes); support security incident management, and apply machine-based assistance to human security analysts and operators. Workflows can be orchestrated via integrations with other technologies and sometimes automated to deliver:

- Incident triage
- Incident response
- Threat intelligence curation and management
- Compliance monitoring and management

Shortcomings

For all of the efficiency gains SOAR platforms, they do have significant shortcomings that can negatively affect your organization. If you have a SOAR platform or are evaluating implementing one, be aware of these short and long-term circumstances that may arise in the future.

Limited to Security Organizations

SOAR platforms can help automate tasks, but they are limited to your security organization. These platforms integrate with security tools and don't natively integrate with other tools in other parts of your business. If you are looking for automation in other areas of your enterprise, consider looking for a more diverse automation platform.

Process Centric

To achieve high returns with a SOAR platform, you must already have established processes. SOAR platforms are best when you already know precisely what security processes you will automate.

According to Gartner, "The main obstacle to the adoption of a SOAR solution continues to be the lack, or low maturity, of processes and procedures in the security operations team."

Market Consolidation

The SOAR market is consolidating via mergers and acquisitions, so make contingency plans if your SOAR platform is acquired. If the product is deprecated or folded into another platform not already in your SOC, you may be forced to implement another technology.

Not People-Centric

As stated earlier, SOAR platforms are process-centric, not people-centric. Processes that you automate using SOAR platforms need constant maintenance and training to gain full advantage. It would be best if you had a tool to support your people that possess critical-thinking skills who know your organization since the threat landscape continuously evolves.

The main obstacle to the adoption of a SOAR solution continues to be the lack, or low maturity, of processes and procedures in the security operations team.

Gartner*

*Market Guide for Security Orchestration, Automation and Response Solutions
Published 21 September 2020 - ID G00727304

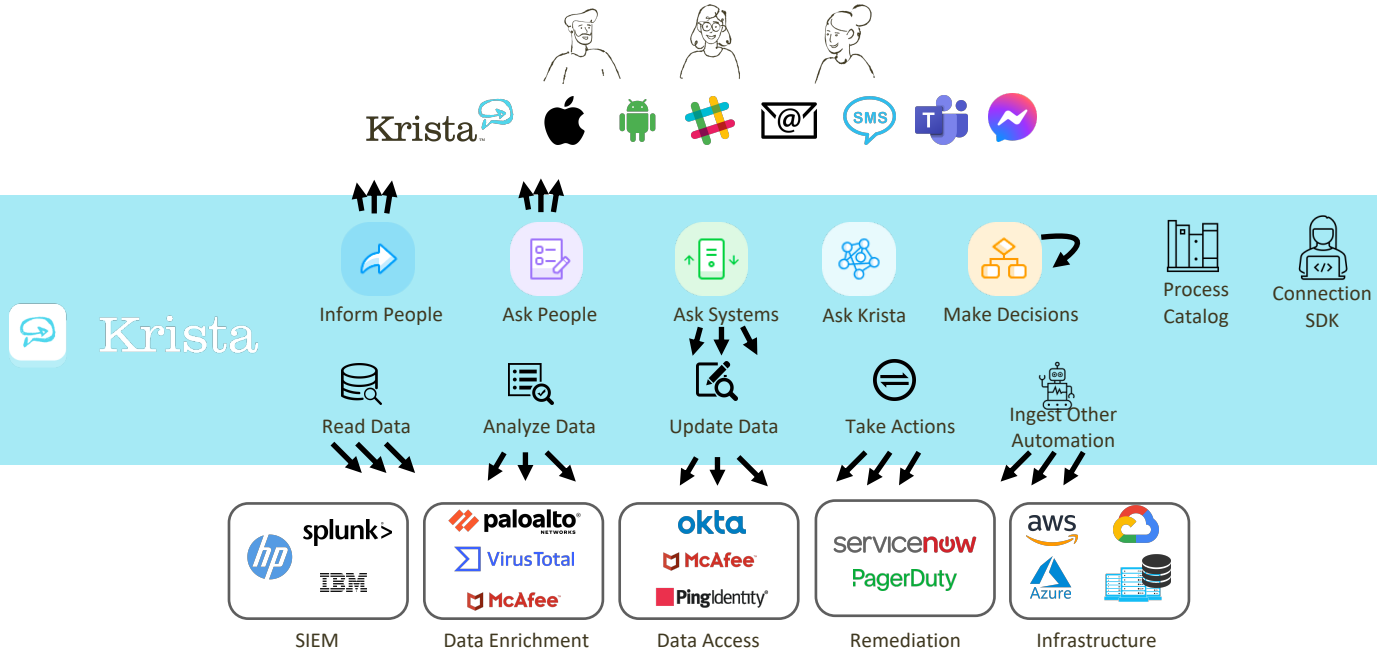
Intelligent automation, or "hyperautomation," as Gartner refers to it, uses technology to automate tasks that once required humans. It's not replacing humans but uses advanced technologies, including artificial intelligence (AI) and machine learning (ML), to increasingly automate processes and augment humans. Instead, it's about transforming business outcomes with digital technologies so your people can perform more critical work.

Krista is a modern Intelligent Automation platform designed to easily leverage existing IT assets in business workflows. It integrates with your existing systems to afford you greater visibility while minimizing dwell time and expediting time to repair. Krista breaks down silos between people and systems by personifying back-end systems to understand a conversation with a person. If you know how to have a conversation with other human beings, you know how to use Krista. It's as simple as that!

Krista is technology that adapts to your people

The conversational approach allows anyone to develop and create workflows around their own business needs. Simple conversation-based workflows empower your security, sales, customer service, field operations, finance, or other IT professionals to ask for information from people and systems. The conversational automation approach democratizes the technology and removes technical skill barriers so anyone can modify processes. This method eliminates maintenance and upkeep required from traditional UI-based record and playback automation platforms or hard-coded bots. Krista's conversations are beautifully simple and easy to modify with enough power, scale, and security to find any answer to any question inside the largest enterprises.

Typically, handling a system alert and fixing it requires significant coordination between teams and associated knowledge handovers. Even after successfully deploying the fix, the investigation of the issue remains in different incident ticketing systems and lacks a central repository. Suppose you need to perform a lesson learned exercise or document the end-to-end process. In that case, one has to scan through the chronology of all these tickets to understand how the separate security teams handled this alert. While this may sound simple, the actual overhead and communicating across teams and across time zones can prove challenging.



Intelligent Incident Management

In the ever-evolving threat landscape, it is not a matter of 'if' but rather 'when' a cybersecurity breach occurs. Acting swiftly and effectively can enhance an organization's cyber resilience and restore it to its secure state. However, this isn't easy with conventional security platforms. SOCs have too many tools. They have too many alerts. They have too few people to comb through millions of threat alerts to locate that one real threat. They need security automation.
Unable to cope with the sheer scale of security alerts, dozens of tools to deal with, and false positives, security teams who already face staff shortages feel overwhelmed. The result—many alerts sneak by, leaving the organization vulnerable to security breaches.

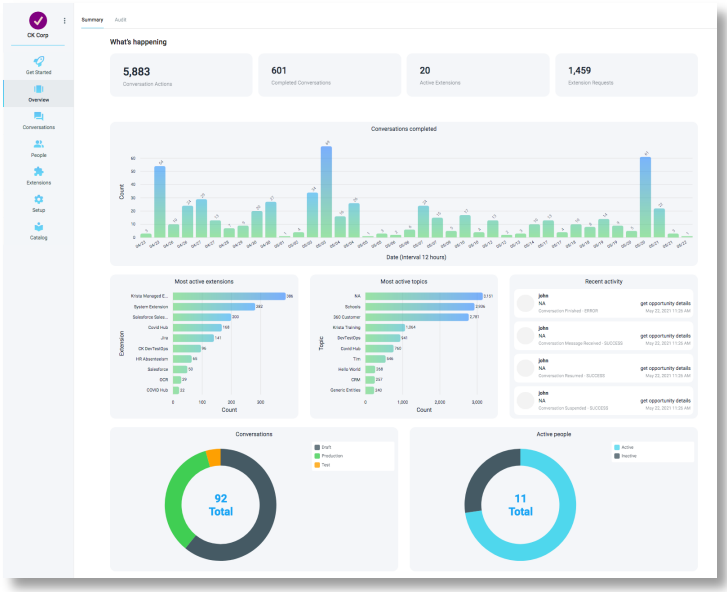
The fact is, it is humanly not possible for analysts to respond to every single alert. So the question then is how do security teams protect the organization despite being severely understaffed?

Krista simplifies incident management processes by having a conversation with people and systems. When a conversation itself is the automation, it's easy to interact and maintain it as you don't need specific knowledge of APIs or programming language to deal with it. Through orchestration and automation, Krista can intuitively perform a series of actions in a matter of seconds to simplify incident and vulnerability management. Once Krista serves as an automation interface, she uses AI to enrich the data from all of your separate tools and helps escalate dangerous and high-priority alerts that need immediate remediation.

Krista automates compliance and documentation.

Compliance, access control, visibility rules, and enterprise-grade security are some rules you need to be aware of in any cybersecurity SOC operation. For example, Krista has built-in enterprise role-based access control at the data level that allows you to see only those pieces of information you're allowed to see based on your role. Role-based data security is essential since not all information is privy to all users in your organization.

By centralizing incident response processes using conversations, Krista logs each step and decision involved in researching alerts. So, if in the future you need information or to document precisely what happened with a specific incident, you don't have to log in to multiple systems to figure out what happened. Instead, Krista can provide you data on the incident and build a report for you, saving you time and administrative headaches.



How Krista Helps You Secure Your Enterprise

To give an example, let us see how an analyst might use Krista. When an alert appears, security teams check multiple systems to find relevant data. Once they have deciphered the incident, they create a ticket to ensure information routes to the right people. If multiple teams work in different time zones/shifts, the primary analyst must provide accurate data and information to the next team. The next shift continues to investigate the alert until it is resolved or escalated to an incident.

Here's a walkthrough of how this works:

1. Krista connects with your disparate tools and systems to provide analysts with a single user interface for all security tools and feeds.

2. Once an alert arrives, analysts can view threat intelligence data in Krista to simplify research and automate documentation.

3. If the primary team did not resolve the issue, it can hand off the conversation to a second team. Krista orchestrates the handoff process to ensure continuity and document the entire process for review and audit purposes, all within the same conversational workflow.

4. If work on a specific alert continues, the second team sends the conversation to a third team. Again, Krista provides all the alert information within the same conversation and informs stakeholders and affected employees.

5. Krista informs everyone of the outcomes, keeping all teams in sync, and updates connected systems automatically.

Typically, this would have been a lengthy process. But with automation, it becomes a simple sequential operation. Automating incident management significantly reduces resolution times while simultaneously reduces the potential for errors. As a result, Krista helps minimize time analyzing alerts, informs affected users and roles, and updates connected systems to assist remediation.

Intelligent automation is sustainable automation

For decades, we have asked our people to learn and adapt to technology instead of having technology adapt to us. Machines and technology get faster and faster–humans do not. It's time we start depending more on technology and powerful artificial intelligence. Krista is an intelligent platform that effectively integrates people, processes, and technology to provide the best solution for your organization. With firms possibly encountering millions of alerts a day, you need AI-led intelligent automation to help you create a more efficient and combative security program.

Deployment is Simple

Krista's Natural Language Processing supports voice, text, and *bots to deliver automation anyone understands. By utilizing existing communication methods in conversations, you take advantage of how your employees already communicate. Krista quickly deploys to existing desktops, mobile phones, Slack, bots, and web browsers that your employees are already using. You won't need to train employees or maintain brittle documentation since the automation follows existing voice and texting conversations similar to WhatsApp or Facebook Messenger. If your employees can text, they can interact with numerous systems to support customers, consume enterprise services, deploy IT changes, or update important KPIs.

Krista Software is in an unrelenting pursuit to help businesses find the right answers. Krista Software produces Krista, an Intelligent Automation platform. Krista empowers businesses to leverage existing IT assets by building low-cost automation applications.

Krista

Web: KristaSoft.com Twitter: @KristaSoft LinkedIn: /Krista-Software