blinkops

CUSTOMER STORY

Beyond Legacy SOAR: How A Global Insurer Achieved 30-Second Incident Response With BlinkOps' Agentic Automation

Overview

A large insurance and reinsurance provider that manages billions of dollars in premiums and serves customers in multiple countries shared their story about improving security processes. For them, robust, scalable security operations are critical to safeguarding client data. For years, the company has relied on legacy SOAR platforms to automate parts of its security processes. Yet these solutions introduced more problems than they solved, such as limited integrations, frequent disruptions, and cumbersome manual tasks. They required an intuitive, well-supported solution to manage their entire range of security alerts and free up team members for higher-value projects.

BlinkOps delivered that solution, helping them drastically reduce alert handling time, expand automation capabilities, and boost morale among security engineers.

The Challenge: Stuck in a Cycle of Legacy SOAR Limitations

Initially, they turned to traditional SOAR platforms to streamline security workflows. While these tools promised extensive automation, the reality fell short:

- **Partial Automation Only:** They could automate some tasks, but large portions of critical processes required manual intervention.
- **Poor Integration Support:** Connecting external tools was complex, slowing progress on new automation use cases.
- **Minimal Vendor Assistance:** Ongoing support was nearly nonexistent, forcing them to troubleshoot frequent breakages alone.
- **High Technical Expertise Required:** Only a few people with specialized skills could build or update the limited set of playbooks.

Deciding on BlinkOps

Evaluating the Market

With their legacy SOAR tools falling short, they assessed several alternatives, including Tines. Their requirements included:

- End-to-End Automation
- Seamless Integration with existing security and IT tools
- Strong Vendor & Engineering Support
- An Intuitive Platform for both experts and newcomers

BlinkOps quickly emerged as the best fit. Its drag-and-drop workflow builder meant no steep coding requirements. A dedicated engineering support model (including monthly or annual hours) removed the barriers that typically come with statement-of-work engagements.

First Impressions

During a POC, the team built and tested new workflows themselves using BlinkOps' intuitive interface. The platform made sense from the start. Fewer steps were required for each automation, and BlinkOps provided quick assistance when needed, enabling the team to transition from prototype to production faster than ever before.

Key Metrics and Business Outcomes

Faster Alerts, Separate Metric Tracking

- **Alert Handling:** BlinkOps' automated workflows reduced resolution time to under one minute. This was so drastic that they now exclude them from the overall MTTR to avoid skewing the company's overall metrics.
- **Scalability:** With such quick response times, the team can now tackle medium and low-priority alerts that once went unaddressed.

Resource Efficiency and Team Morale

- **Time Savings:** Fewer manual tasks allow engineers to focus on large-scale projects, such as firewall upgrades and new security solution rollouts.
- **New Opportunities:** The incident response team has gained extra capacity, taking on more responsibilities and exploring new automation ideas.
- **Better Organizational Planning:** Leaders factor BlinkOps' success into their determination of next year's team structure and resource allocation.

A Closer Look at Technical and Support Benefits of BlinkOps

Easy-to-Use Interface

BlinkOps centers on drag-and-drop workflow creation. Instead of writing code, team members can visually outline each step and see the entire workflow at a glance. This approach lowers the learning curve and fosters a do-it-yourself mentality around automation.

> "BlinkOps is one of those things that I don't dread the calls every week. It gets exciting: what else can we automate?"
> — Senior Security Engineer

Dedicated Engineering Hours

They highlight BlinkOps' support model as a key differentiator. Their contract offers an annual bucket of engineering hours to:

- Build or modify existing workflows
- Get immediate technical assistance for integrations
- Troubleshoot edge cases
- Continually optimize overall automation

This setup reduces reliance on in-house developers and sidesteps the lengthy procurement processes associated with every new project.

Evaluating Alternatives

When they considered Tines, they concluded it would have similar drawbacks to legacy SOAR: heavy development overhead, minimal vendor support, and higher costs for professional services. BlinkOps offered a user-friendly design, strong hands-on support, and rapid time-to-automation, making it the clear choice.

Rapid Improvements with BlinkOps

Dramatic Drop in Resolution Times

One of their biggest wins has been reducing alert resolution time from 10–15 minutes down to 30–60 seconds. Using out-of-the-box integrations, analysts can receive and respond to alerts on any device, including their phones. This shift has let them handle high volumes of alerts far more quickly.

Scaled Agentic SecurityWorkflows

From 5 to 30 workflows

Automated and Cut Alert Response down to 30 seconds

> "Instead of it taking ten to fifteen minutes, it takes, like, thirty seconds to a minute. That enables the team to do more project work."
> — Senior Security Engineer

Real-World Example

During a recent after-hours incident, a senior leader requested that a malicious domain be blocked. Before BlinkOps, the on-call analyst would have needed to:

Legacy SOAR: Power on a laptop → Connect to the corporate VPN → Log into multiple consoles → Manually block the domain

The analyst simply opened Teams on their phone → Selected the relevant workflow → Typed in the domain, blocking it within seconds.

Leadership praised the security team for their speed, and the process became a benchmark for other internal teams seeking to automate their own workflows.

A Surge in Automation Adoption

The security team has expanded from just 5 workflows to 30, with plans for many more. The security team no longer wonders if the platform can handle a new idea. Now, they assume BlinkOps can handle it. This cultural shift has encouraged more experimentation and broader use cases, including a self-service portal that allows other IT functions to submit requests directly to the security team's workflows.

Ongoing Projects and Future Plans

Expanding Use Cases Beyond Cybersecurity

Outside of security, teams now look to BlinkOps whenever a new automation idea comes up, even outside of security. Firewall upgrades, IT service requests, and self-service options for non-security functions are all possible areas of growth.

> "BlinkOps gives us a platform that's fast, easy to use, and incredibly well supported. The drag-and-drop workflows, built-in integrations, and dedicated engineering hours have allowed us to automate across more use cases than we ever could with legacy SOAR tools. It's helped us respond faster, reduce manual work, and expand what our team is capable of handling." — CISO

Positive Internal Adoption

The success of after-hours incident responses, along with leadership praise for rapid blocking of malicious domains, continues to generate interest across the organization. More departments are interested in replicating these results for their own workflows, utilizing BlinkOps to automate repetitive tasks and minimize manual effort.

The Bottom Line:
Agentic Security Automation That Simply Works

By moving to BlinkOps, the security team broke the cycle of underperforming legacy SOAR platforms. Streamlined integrations, end-to-end automations, and hands-on vendor support allowed the security team to scale from five to 30 workflows. They now respond to alerts in under a minute, freeing up staff for strategic security initiatives.

Key Takeaways

- Cut resolution times from 15 minutes to under a minute
- Expanded automation from five to 30 workflows and still growing
- Freed up engineers for major projects like firewall upgrades
- Boosted morale through user-friendly, mobile-ready workflows
- Committed long-term thanks to proven ROI and continued vendor collaboration

BlinkOps' intuitive approach optimizes how the security team invests in people and technology across its broader IT environment, providing the speed and flexibility they need to address security issues as they arise.