blink

CASE STUDY

How ControlUp Uses Blink to Automate Security Workflows Reducing MTTR Significantly

About ControlUp

Digital experience management for end-user computing environments

Since ControlUp Technologies launched its first offering in 2014, it raised more than $140 million in funding for a cloud-native platform that empowers enterprise IT teams to better support employees with remote IT services.

With more than 200 employees in global locations (HQ: California) supporting more than 1000 organizations, ControlUp provides digital experience monitoring solutions for various End-user Computing environments, including physical and virtual desktops.

CHALLENGE

Manual processes and change tracking were overloading SecOps team, limiting collaboration with DevOps team

As a SaaS provider for IT operations, security is of utmost importance for ControlUp.

ControlUp Technologies operates a cloud-native platform that empowers enterprise IT teams to better support employees with remote IT services. Eitan Oscar, SecOps Team Leader for ControlUp, manages their security operations, including approvals for new security projects. His team of two SecOps engineers collaborates with DevOps to monitor detections and security alerts, identify security gaps, manage vulnerabilities and fixes, and create security tasks for DevOps and IT teams.

In the past, ControlUp SecOps relied on PowerShell and Python scripts or Microsoft Logic Apps to orchestrate security operations. But with 3+ years of experience building cloud and security workflows this way, Eitan's team needed a more sustainable approach to security workflow automation. Soon, they began exploring no-code platforms like Blink.

Specific challenges ControlUp's SecOps team had around security automations and response in their cloud environments including AWS:

1. **Orchestration and Response for QRadar SIEM Security Alerts**
   Collecting all alerts from QRadar, identifying the root cause, providing enrichment from threat intel sources and performing auto-response when applicable.

2. **Access management, coverage validation automation for CrowdStrike EDR/XDR in AWS**
   There were gaps in EDR/XDR coverage in the AWS EC2 environment and needed tooling to discover and track the resolution of the deployment of protection.

3. **Vulnerability scanning and management with Tenable**
   Grouping and segmenting compute/endpoints and flexible timing of scanning is hard to arrange with the native tooling.

CASE STUDY

About Blink Ops

Founded in 2021 and now present on 3 continents: Blink Ops' mission is to automate security operations everywhere. Blink is secure, decentralized, and cloud-native - all built on AWS. Blink increases the productivity of cloud SecOps teams, reduces costs, and helps you do the things you do best, even better - now through a Co-pilot AI interface.

With a total of 7,000+ automated workflows that cover the entire security ecosystem, Blink provides automation capabilities for dozens of AWS services, and 1,200 + individual pre-built combinations of 130+ action types.

PARTNER SOLUTION

Better SOAR and No-Code Automation for SecOps & DevOps Teams

SecOps automation means more than just integrating services into your SIEM and SOAR platforms and getting alerts. Most companies invest major resources into their security automation tooling and still come up short on their cloud and security operations goals.

Cloud security engineers continuously receive alerts and must take action fast, often across multiple cloud platforms. This means logging in and out of multiple security and infrastructure tools, manual data enrichment tasks, creating Slack channels, notifying affected stakeholders, and then closing and monitoring the alert. Meanwhile, many of the necessary actions across your cloud infrastructure cannot be natively automated by existing SIEM or SOAR.

Blink gives cloud security teams the tools to automate their most critical SecOps workflows. Using Blink, SecOps teams can quickly integrate with cloud services and rapidly compose no-code actions into simple or complex workflows.

1. **Access management, coverage validation automation for CrowdStrike EDR/XDR in AWS**
   Blink is set up to scan for EC2 hosts missing CrowdStrike agent, retrieve asset details then track the resolution of deployment of fixes with the DevOps team

2. **Managing QRadar SIEM Security Alerts**
   Created automation to track issues to work items, then resolutions and fixes in multiple environments then closing the issue in QRadar

3. **Vulnerability scanning and management with Tenable**
   Created automation for scanning and tracking that is customized by workload groups and the optimal time to schedule.

RESULTS & BENEFITS

Reduced SIEM alert MTTR to save hours of work with accessible security automation

- **Significantly reduced MTTR** for SIEM alerts from 1 hour to 5 minutes
- Blink transformed a process that took over an hour into a simple automation that can run in seconds, **saving ControlUp an estimated 30 hours per week.**

Blink has already enabled ControlUp to create 100 workflows across different platforms and handle approximately 15% of their alerts using Blink automations, saving the cost of hiring an additional full-time security analyst. Additionally, ControlUp is planning to automate 40% of its existing alert workflows with Blink over the next two months.

"Today it's faster for us to create new cloud workflows. We don't need to learn all the authentication steps and syntax of each product anymore. We are saving time and money on human resources. Most organizations are administering their cloud applications manually. When cloud maintenance is required, we want to use Blink automations wherever possible."
– Eitan Oscar, SecOps Team Leader, ControlUp

blink

Ready to automate?
Sign up for a demo at blinkops.com/demo