Blumira

CASE STUDY

Atlantic Constructors

Atlantic Constructors is Central Virginia's leading service and construction manufacturing provider for commercial and industrial markets. Their highly automated 130,000 square feet fabrication shop and 30,000 square feet office complex support approximately 700 highly-skilled employees, allowing them to efficiently provide complete turn-key solutions.

The Challenge: Limited IT and Security Resources

As IT Director, Jim Paolicelli started as a consultant at ACI, moving into a director role with a small team of help desk employees to support both the company's IT and security functions. One of their goals is to keep the organization safe and secure from security threats like ransomware and account takeover, while keeping an eye on any abnormalities in their environment.

While working with a few outside vendors to conduct security assessments for ACI, SIEM (security information and event management) systems kept coming up as a recommended solution to gain greater visibility into their security posture and help harden their defenses.

After attending a virtual CIO conference, Paolicelli met with several security vendors including Siemplify, Managed Engine and Blumira in search of a SIEM that would fit the needs of their small team – easy to set up, use on a daily basis and could be monitored and managed by an IT administrator without a security background.

The Solution: Blumira's Cloud SIEM Designed for IT

While many SIEMs require security expertise or extensive training to operate, Blumira's cloud SIEM is built to be easy for small IT teams to manage threat detection and response for their organizations. ACI chose Blumira for the simplification of its platform that makes their IT team's day-to-day more automated and effective.

> "I've worked with SIEMs for over 30 years; many collect logs, but analyzing them is time-consuming. I don't have the staff dedicated to sit and read logs all day or with the skillset to analyze our data. We chose Blumira for its simplicity – I needed a solution that would simplify, consolidate and show me what I really need to see," Paolicelli said.

Industry

Manufacturing

Driver

Reduce risk; gain greater visibility into unknown threats

Company Size

1,000

Challenge

The IT Director of Atlantic Constructors, Inc. (ACI) needed a simplified SIEM that his small IT team could use to keep their organization safe from ransomware and account takeovers.

Solution

ACI turned to Blumira's cloud SIEM to help them detect previously unknown threats, following response playbooks written for IT teams to help them remediate threats quickly and easily.

Sign Up Free!
blumira.com/free

Blumira

CASE STUDY

Blumira's platform automates security monitoring by collecting logs and analyzing them using behavior-based detection rules that come fine-tuned to reduce noisy alerts. Prioritized findings come with pre-built playbooks to guide IT teams through next steps for threat response.

> "Our IT help desk employee is in charge of monitoring Blumira. Without requiring a ton of experience, Blumira's platform provides very simplified language and built-in workflows that help him also learn about security as he uses the product – it's not overloading him with alerts and he doesn't need to sift through hundreds of thousands of logs."

By explaining findings in plain language and providing clear question-and-answer workflows, Blumira's goal is to help educate IT teams on security and move their organizations toward greater security maturity over time.

Easy Deployment, Visibility Into Unknown Threats & "Wicked-Fast" SecOps Support

The deployment of Blumira is also designed to be simple enough for IT teams to roll out without requiring additional resources or personnel.

> "I was able to do it myself about 90% within an afternoon – and then Dave (Blumira Technical Account Manager) stepped in to help tweak things as well. It was easy to set up the Duo Security, Crowdstrike, Microsoft 365, Azure and Windows Server integrations using Blumira's excellent documentation," Paolicelli said.

Once deployed, ACI's IT team was able to gain a peace of mind after receiving findings from Blumira's platform on events they would have never seen before, such as insight into Microsoft 365 security group creations and logins from outside of the country.

> "There were a few Microsoft 365 findings where I couldn't quite figure out what was going on, but support has been great – I was getting a wicked-fast response time from the team," Paolicelli said.

Automate Detection & Response With Blumira

- Built-in integrations across hybrid cloud infrastructure, applications and services
- Simplified log collection, threat detection & response playbooks for remediation
- Scheduled, automated & customizable reports of security threats
- Access to Blumira's security experts for additional security advice

*"**We chose Blumira for its simplicity** – I needed a solution that would simplify, consolidate and show me what I really need to see."*

- Jim Paolicelli, IT Director

Sign Up Free!
blumira.com/free

Blumira

CASE STUDY

Acting as an extension of limited IT teams, Blumira's security operations (SecOps) team offers support to help our customers better understand findings, dig in deeper for investigation and provide guided response advice, especially during stressful events. They are available 24/7 for urgent priority issues — learn more about Blumira's support.

Free Security For SMBs

Use Blumira for free, no special Microsoft licensing required.

Blumira's detection and response platform helps SMBs respond faster to attacks to prevent ransomware and data breaches. It only takes minutes to fully deploy, using the existing team and infrastructure you have today.

With Blumira's Free edition, you'll get:

- Coverage for unlimited users and data* for Microsoft 365
- Easy cloud SIEM setup in minutes with Cloud Connectors
- Detections automatically activated, fine-tuned for noise
- Summary dashboard of key findings & basic reports
- Playbooks to guide you through response steps
- 7 days of log data retention (upgrade to paid for 30 days or one year)

**Subject to Blumira's Terms of Service*

Sign Up Free!
blumira.com/free

Actionable Findings, Automated Response & Access to Experts

Threat Analysis

Playbooks For Response

Direct Message a Security Expert