Blumira

Blumira Case Study:

Crescent City

Blumira
CASE STUDY

The City of Crescent City

The City of Crescent City, CA is known for its beautiful beaches and surrounding old growth Redwood forests. Incorporated in 1854, it is one of the oldest cities in California, and serves as the county seat for Del Norte County.

The Challenge: Limited IT and Security Resources

With 60 full-time employees, the City of Crescent City needed a security solution that their 1-person IT team could easily manage, in addition to daily management of their servers, workstations, cloud applications and mobile device management.

According to their Information Systems Administrator Fritz Ludemann, the traditional syslog applications weren't providing enough security coverage, and he was seeking a solution that would also do some threat hunting on their behalf.

He decided a SIEM (systems information and event management) platform would provide the overall visibility they needed. Initial research turned up vendors and providers better suited for large enterprise deployments.

> "I researched a number of SIEM providers online and found most were way out-of-the-ballpark expensive, required a lot of infrastructure and didn't provide a great return on our investment," Ludemann said.

The Solution: Easy to Use, Automated Threat Mitigation

Ludemann first spotted Blumira on Capterra, a software review and comparison site. According to their procurement process, they required at least three competing quotes from different security vendors.

> "I was looking for a tool that would help automate security and fit the profile of our organization; a small municipality," Ludemann said. "I looked at a number of products, but they didn't have the threat mitigation and reporting tools that Blumira had at an acceptable price point, which was a big negative for me."

Industry

State & Local Gov

Driver

Greater security coverage; automated threat hunting

Company Size

60

Challenge

With limited IT and security resources, the City of Crescent City's 1-person IT team needed an easy-to-deploy solution to provide network visibility and threat mitigation for ransomware.

Solution

Blumira's out-of-the-box integrations allowed their IT admin to set up a trial within an afternoon, providing easy management, threat hunting, and guided remediation for their small municipality.

Blumira

CASE STUDY

As the primary IT personnel also juggling security, Ludemann needed an easy-to-deploy solution that he could also easily manage. He needed more visibility into what was happening at the network level, and also needed threat mitigation to deal with critical threats like ransomware.

> "The one thing that really stood out right away was the ease of deployment – I had a working trial operational inside of an afternoon," Ludemann said. "The fact that I could get that level of insight in a cloud-based solution, with little infrastructure that I had to maintain was a great fit for our use cases and limited resources."

The fast time to security was driven by Blumira's out-of-the-box integrations that easily connect and centralize data from Crescent City's existing tech stack to analyze it for indicators of threats.

> "The steps are pretty much outlined on the Blumira website on how to deploy the solution," Ludemann said. "After a couple of conversations with an account executive and a tech, we were able to get a config file set up, followed those instructions and had my servers covered that afternoon."

Three-Step Rapid Response For Faster Resolution

As the key responder, Ludemann interacts with Blumira findings on a day-to-day basis and uses playbooks to help guide him on how to respond.

> "When a threat is detected, there's a workflow attached to the finding that guides us as to what we should do and how we should respond to it. The built-in response is another great feature – we can reach out to your team directly," Ludemann said.

Blumira's platform can automatically block known threats and provides step-by-step remediation instructions for every finding that is detected, making it easy for resource-strapped IT teams to quickly contain threats. Blumira's security operations team can be contacted directly within the platform to help with any additional questions or support.

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

*"The one thing that really stood out right away was the **ease of deployment** – I had a working trial operational inside of an afternoon"*

- Fritz Ludeman
Information Systems Administrator

Sign Up Free!
blumira.com/free

Blumira
CASE STUDY

Automating Security and Operational Visibility

In addition to the threat mitigation and remediation capabilities, Ludemann can leverage Blumira's dashboards and reporting to gain visibility into security changes in Crescent City's environment.

> "The dashboard is great – it gives me a broad overview and visibility into any user account changes and much more. I have scheduled reports sent to me every day," Ludemann said. "Small organizations like ours without a good SIEM are much less likely to know if there's an attacker in their environment. Blumira helps me know if there's a problem."

Crescent City's endpoint protection sends logs to Blumira's platform for centralization and security monitoring, analysis, notification and guided response.

> "So far, everything we've had that's triggered an alert has been through our endpoint detection – such as someone tried to connect to a website that was compromised, or an attachment was infected," Ludemann said. "Blumira has actually alerted me before our endpoint detection does."

Sign Up Free!
blumira.com/free