splunk> + VictorOps CASE STUDY

Malwarebytes Scaled its SRE Team From 3 People to 19 With VictorOps

Malwarebytes

Executive Summary

As an anti-malware software company protecting the machines of thousands of businesses and families, Malwarebytes takes incident management seriously. When Shawn LoPresto, Malwarebytes' head of SRE, joined the company in 2015, he found that insufficient monitoring and limited process around incident response led to increased time to recovery.

As part of his overhaul of the incident response process, Shawn moved his SRE teams from PagerDuty to VictorOps after finding that many of the features he needed to improve visibility across numerous engineering teams came standard with VictorOps — features that would cost him extra with PagerDuty. VictorOps has fit seamlessly into Malwarebytes' toolchain and helped the company achieve:

- More accountability, reduced incident frequency and greater insight into the business impacts of downtime
- Decreased MTTA/MTTR thanks to less unnecessary communication
- A strong relationship with a service provider that values feedback and delivers on feature requests

Finding Tools (and Pricing Structures) That Scale

Shawn LoPresto has headed up the Malwarebytes SRE group since joining the company in 2015, overseeing 19 people spread across four different teams. His staff is responsible for running all the backend infrastructure for Malwarebytes engineering with the goal of ensuring Malwarebytes is developing scalable, performant, cost-efficient and stable software.

When Shawn first started at Malwarebytes, monitoring was sparse and a formal incident response process was not yet established. As a result, the time to identify and resolve incidents took significantly longer than necessary. Shawn immediately made standardizing, choosing the right vendors and building reusable tools across teams a priority.

According to Shawn, one of the biggest challenges in selecting vendors is deciphering different pricing models because in most cases, each service provider's pricing model is uniquely structured to serve the needs of their business — not the end user. "I just need to know how much I'm going to be spending year over year. I look for products that are going to grow the way we are and have costs that scale along with that growth," says Shawn.

About Malwarebytes

Malwarebytes is a cybersecurity solution that provides comprehensive endpoint protection, detection and remediation. It runs on Microsoft Windows, macOS, Android, iOS and features layers of technology such as anomaly detection, behavior matching and application hardening to stop malware before it impacts performance.

www.malwarebytes.com

Headquarters

Santa Clara, CA

Industry

Software Company

Type

B2B, B2C

The Malwarebytes SRE team sports the famous VictorOps cat t-shirt

Why VictorOps

Prior to signing on with VictorOps, Malwarebytes used PagerDuty to manage alerts and incident response. When the SREs for the Malwarebytes Data Science team — who were using VictorOps at the time — recommended the tool to Shawn, he decided to compare it against PagerDuty.

"There were things I wanted to do inside PagerDuty, like reporting, that were going to cost money, but with VictorOps, it was all included. We would have had to pay for a more advanced plan to get reporting, so that helped us make the decision," says Shawn.

Ultimately, Malwarebytes chose VictorOps because the reporting features they most needed to scale the SRE team came standard with the software. "VictorOps has a very clear pricing structure that has grown with our team. In fact, our customer success manager recently reached out to let us know we aren't utilizing all the user accounts we pay for and helped us adjust down. This is so different from the normal sales rep that would want us to keep adding on even if we don't need to," says Shawn.

How Malwarebytes Uses VictorOps

Now, when an alert is triggered in the Malwarebytes monitoring system, DataDog, it is routed to VictorOps. Each team is able to configure its own escalation policies with multiple routing groups based on the various development teams that support those products. On-call team members are notified via the method of their choosing (SMS, email, push notification or phone call) and can use VictorOps multi-channel Slack integration for collaboration, while simultaneously hooking into StatusPage for research and response.

Once an event has been resolved, Shawn's team utilizes the VictorOps Post Incident Review (PIR) report to assess what happened and take steps to prevent its occurrence in the future.

Increasing Accountability With Reporting

Prior to implementing the PIR process, Shawn says that it was difficult to associate incidents with new or open defects required to resolve the issue strategically. "With VictorOps PIR reports, I'm able to increase accountability by attributing alert frequency and impact directly to the actual issues that need to be resolved," Shawn says.

Team managers consolidate and pull all data from VictorOps PIR and MTTR reports every Friday and present them to the group, which allows them to prioritize defects across development teams. "These reports help reduce the frequency of repeated incidents by illustrating the impact of engineers being taken away from new feature delivery to address problems which were not previously being prioritized," Shawn says.

In addition to helping with post-incident reviews and business reporting, Shawn loves how Incident Frequency Reports allow him to get a quick snapshot of what's going on to see when a group's incident frequency is increasing and needs attention.

An Open Feedback Loop

According to Shawn, what sets VictorOps apart from other incident management tools is the relationship. "The thing I've appreciated most is how receptive VictorOps is to feedback. I feel a lot closer in this relationship than I ever did with PagerDuty," says Shawn.

For example, VictorOps recently asked Shawn to beta test a multi-channel Slack feature he had previously requested. Rather than have his team spend cycles building the new Slack feature on their own, he can leverage something already included in VictorOps.

Since adopting the multi-channel Slack feature, Shawn says his engineers are able to be more fine-tuned in their communication. Developers only get notified from on-call SREs on their team and reducing unnecessary communication has increased the team's velocity significantly.

Shawn says, "Our SRE team has grown from three engineers to 19 and our process as a whole has become more evolved, but VictorOps has always kept up with us."

Malwarebytes scaled its SRE team from 3 people to 19 with Splunk + VictorOps. Sign up for a 14-day free trial and start making on-call suck less for your own team.

splunk> + VictorOps

Learn more: try.victorops.com