SOLARWINDS

Understanding Alert Fatigue

Sascha Giese

Global Tech Evangelist, Observability

Sascha Giese started his career in IT in the early 2000s as a network and system administrator in a public school, where he learned that teaching teachers how to use this thing called *the internet* is more complicated than resolving spanning tree problems.

Giese joined SolarWinds in 2014 as a Solution Engineer and became a subject matter expert on all products in the SolarWinds portfolio. He contributed to the SolarWinds Certified Professional® (SCP) exams and training curriculum. As a Tech Evangelist, his mission is to put humans into focus. Humans working in IT teams around the globe to keep organizations alive are overlooked easily.

Giese states, “IT no longer supports the business; IT runs it instead.”

He studied Media Informatics at the University of Lübeck, Germany, and holds various industry certifications from Cisco, Microsoft, VMware, Amazon, and others.

What is alert fatigue?

What is Alert Fatigue?

- Main problems:
  - The sheer number of alerts
  - The high percentage of false alarms

The Consequences of Alert Fatigue

- Missed or ignored alerts
- Slow response times
- Employee burnout

The Consequences of Alert Fatigue

- A survey[1] conducted by FireEye among C-level security executives at large enterprises worldwide discovered that 37 percent reported that they receive more than 10,000 alerts each month. Of those alerts, more than half (52%) were false positives.
- In fact, IDC estimates that teams at companies with 5,000+ employees wind up ignoring about 23% of their alerts. Those with fewer employees ignore even more[2].

Sources: (1) https://bufferzonesecurity.com/the-cost-of-false-positive-alerts-and-how-to-avoid-alert-fatigue/
(2) https://fieldeffect.com/blog/cyber-security-alert-fatigue

Psychology of Alert Fatigue

- Normalization, desensitization, and habituation
- Exposure leads to tolerance and ignorance
- Repetition of the same alert exacerbates fatigue

Preventing Alert Fatigue: Best Practices

Set Intelligent Thresholds

- Balance between too few and too many alerts
- Differentiate high-risk and low-risk alerts
- Prevent missed incidents without overwhelming responders

Implement Tiered Alert Priorities

- Visual, audible, and sensory cues for importance
- Differentiate alerts based on urgency
- Examples from aviation industry

Ensure Alerts are Actionable

- Specific, actionable alerts improve response
- Reduce the need for extra focus and attention
- Learn from aviation industry's actionable checklists

Consolidate Redundant Alerts

- Redundant alerts contribute to alert fatigue
- Consolidate and reduce reminders
- Improve attention from responders

Create Balanced Schedules

- Distribute alert workload evenly
- Prevent burden on individuals or teams
- Consider coverage needs at different times

Continuous Review and Improvement

- Regularly review processes, alerts, and systems
- Identify missed alerts and reasons
- Adapt thresholds, design, and approaches

Q&A

THANK YOU

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.