
3 KEYS TO HAVING AN
INFOSEC TEAM
THAT LOVES THEIR JOB
Balbix

THEY KNOW WHAT TO FOCUS ON

There are a hundreds, if not thousands, of cybersecurity tasks that your team can be working on at any given time. If your team is spending large swaths of time trying to identify which vulnerabilities are critical, frustration will eventually build up. Sifting through the noise of security issues is overwhelming and will quickly burn even the most experienced cybersecurity professional out.

Effective InfoSec leaders empower their teams to be productive by providing them with prioritized lists of vulnerabilities that need to be remediated. Exemplary InfoSec leaders go above and beyond in helping their team understand the context of vulnerabilities as well. Not only does this boost efficiency, but it also frees up time for team members to undertake their own initiatives and avoid mindless patching.


2

THEY ARE GIVEN OWNERSHIP AND CAN TRACK THEIR PROGRESS

Humans generally perform best when provided with some degree of autonomy in how the task may be achieved and are more engaged when they know they have room to learn. Assigning ownership of risk areas to team members will give them a sense of autonomy, allowing them to take initiative and harness their own creative methods. Furthermore, providing employees with an intuitive tool or structure by which to track their progress will give them a sense of accomplishment.

As an InfoSec leader, you have the ability to turn cybersecurity posture improvement into a gamified experience for the members of your team. The right context, tools, and incentives empower everyone to do their part in reducing cyber-risk.


3

THEY SEE HOW THEIR WORK CONTRIBUTES TO KEY BUSINESS OUTCOMES

Even the most junior members of your InfoSec team should have an understanding of the company's overall cybersecurity posture and how their role contributes to improving it. Spend time communicating your vision to your team and engaging in conversation about how key objectives will be achieved will be achieved with staff members at all levels.

A great way to stay aligned with your team on high-level goals is using risk heatmaps and dashboards. Ideally, these dashboards will provide risk metrics and have the ability to drill down on specific areas of risk. If employees can see that patching a specific group of assets will decrease overall risk levels by 25%, they are likely to feel a greater sense of purpose and passion for your cybersecurity vision.

TURN THE PAGE TO SEE HOW BALBIX CAN HELP

HOW BALBIX CAN HELP

KNOWING WHERE TO FOCUS

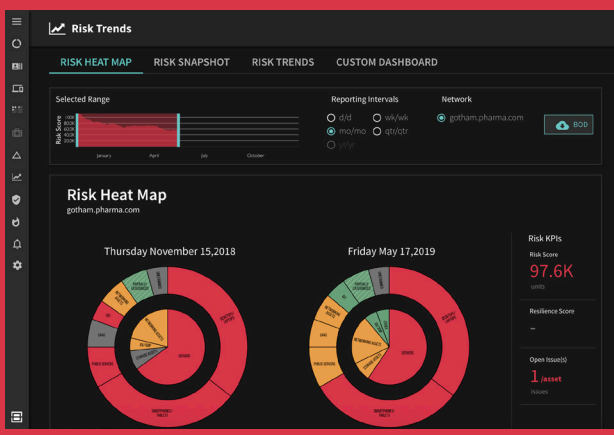
Balbix provides prioritized lists of vulnerabilities with insights into the issues affecting assets and the impact a breach on that asset would have for your enterprise. Furthermore, Balbix gives prescriptive fixes for each vulnerability and offers automated ticketing to seamlessly assign patches. Continuous analysis ensures that your team has a live view into top risk insights.

ASSIGNING RISK OWNERS AND TRACKING PROGRESS

Balbix allows you to create dynamic groups for risk areas and assign owners. Team members can track their progress over time and see how their remediations impact overall risk levels. They can also compete with one another via leaderboards and managers can reward employees who are going above and beyond.

ALIGN WITH BUSINESS-LEVEL RISK METRICS

Balbix's real-time and continuous risk heat maps quantify breach risk for you. In the dashboard, you can create a clear plan for transforming your heat map from red to green and decreasing overall risk levels. Measuring progress over time is easy with exportable risk snapshots and trend maps.



Balbix®

www.balbix.com/contact
866.936.3180