ivanti

From Adversaries to Allies

5 ways to align your security team with IT

Shared mandates – but different approaches

While both security and IT teams' goal is to keep their organization running smoothly, each team approaches this mandate from different directions: security to avoid negative impacts, and IT to improve overall outputs.

Organizational mandates: security versus IT

Security prevents operational disruptions

That is, security specialists continuously minimize the risk of unexpected disruptions due to cyberattacks from either internal or external threats through a variety of continuous tactical implementations and strategic, proactive threat analysis and remediations.

IT facilitates operational outputs

That is, IT specialists increase end user productivity through seamless background technology implementations and maintenance, fixing hardware and software issues that threaten other specialists' output and deliverables.

However, when the two divisions cooperate, both can reach their objectives more effectively.

Processes work well when IT buys into security teams, and there's proactive strategies and processes in place before security makes a request from their IT partners.

But, how can you present your security team's goals and proposed projects in such a way that you'll win active friends in IT, who will want to help security policies succeed – and not accidentally create passive foes, willing to sacrifice your security goals for their own internal priorities?

Top three security-IT alliance advantages

Faster, better results

The IT team is more likely to institute updates and patches that require time and resources if they trust the security team requesting these patches.

Shared resources reducing overall tech expenditures

When teams trust each other, they can use the same tools to achieve different goals. Shared resources reduce organizational overhead of cost centers.

Realistic and sustainable security practices

Security depends on IT to implement security protocols. If the requests are too hard to fulfill or take too much of IT's time, then IT may not be able to maintain those regulations and protocols.

In this eBook, we'll walk you through:

01 **Explaining your "why" behind security plans, changes and requests** prior to implementation – for both IT admins and end user stakeholders.

02 **Reducing security policy impacts** on IT's budgets, schedules and resource allocations.

03 **Compromising** wherever security can afford to be flexible. (Don't let security be the Department of No!)

04 **Developing and enforcing shared goals** with common language, dashboards and metrics wherever possible.

05 **Proactively offering help** – be it administrative lifts, technical expertise, shared resources or otherwise.

After all, a rising tide lifts all ships, and both your security team and IT share the same end goal: a productive, secure workplace.

ivanti

01

Explain why:

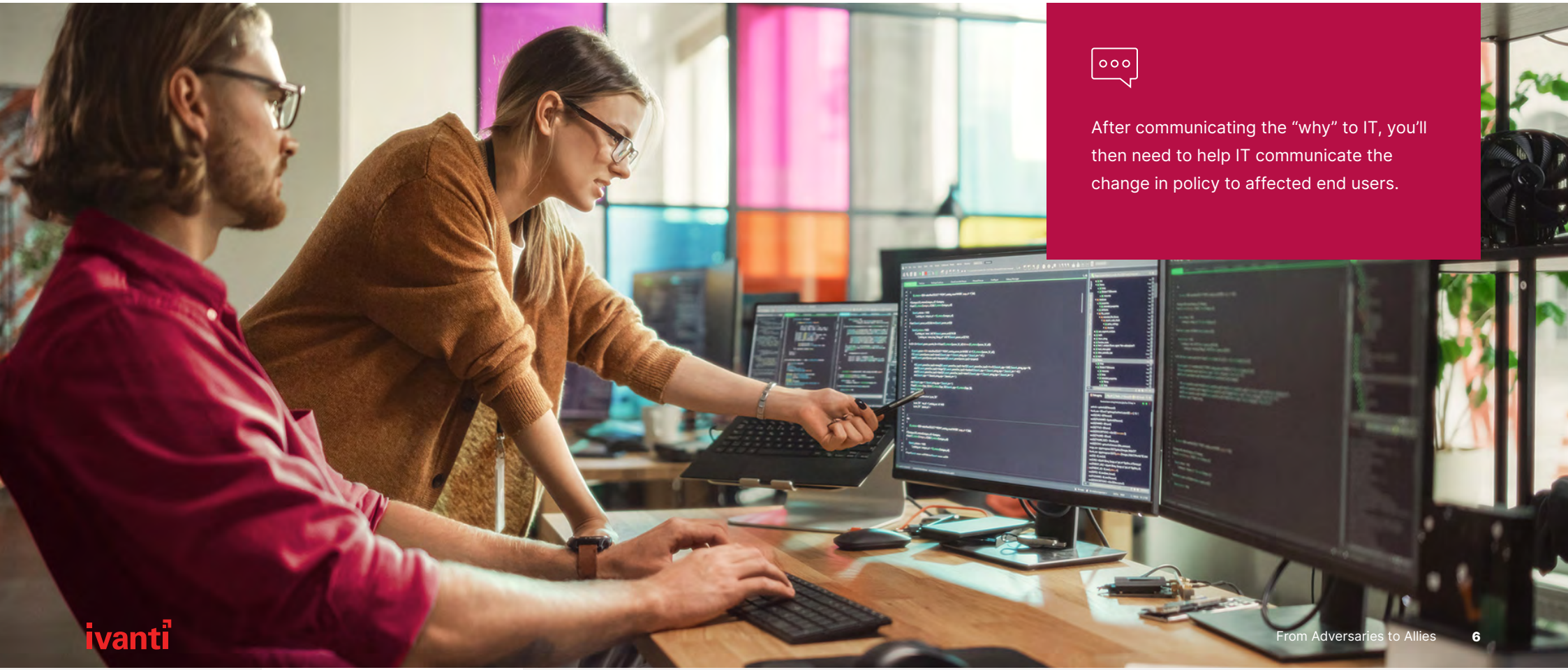
Avoid edicts and offer explanations behind security plans, changes and requests.

ivanti

Don't forget the "why"

Unexplained edicts from security quickly antagonize IT departments. For the sake of time and bandwidth restraints, security requests may be issued without pausing to explain why the change is being requested, or otherwise considering how IT partners can implement them.

For example, if your security team decides to disable removable memory devices, your policy implementation would probably need to start with a head's up to IT to communicate your rationale. You might tell the IT team that by disabling certain types of devices, your organization will have a lower cyberinsurance payment, prevent loss of data through internal and external threats and reduce the organization's risk exposure.



After communicating the "why" to IT, you'll then need to help IT communicate the change in policy to affected end users.

Your joint communication should contain:

A clear explanation of what's impacted without use of industry jargon. For example, the internal write-up for a device ban policy would use terms like "jump drives," "USB drives" or "anything that can have files and connects to computers with a cable" instead of "removable memory devices."

- The policy write-up should also clarify what isn't impacted – in this case, cable-connected computer mice, keyboards, speakers and other peripherals.

Offer a clear timeline with more than a day or two's notice of the change, to give users time to find alternative arrangements and not accidentally lock out USB drives from laptops before a critical sales presentation.

Define exceptions to the mandate – and the hopefully painless process by which to apply for those exceptions – to discourage users from implementing workarounds for their "unique situation."

Identify key representatives or locations to answer the anticipated frequently asked questions, common troubleshooting and handle unexpected edge cases.

Without this communication, the IT team would be flooded with complaints and tickets when the security protocol rolls out – and they might take out that frustration and anger on security.

02

Reduce impacts:

Consider security policy impacts on IT budget, schedule and resources pre-deployment.

ivanti

Anticipate - and mitigate - impacts on IT

Be aware of what other demands the IT team is facing. They may be dealing with a larger project at the time of your request, or they may not have the people they need to complete the task.

Instead, look for tools and systems that make security policies, requests and patches easier to implement for your IT allies – unlike what this security team did to their poor IT department.

Real-World Repercussions

University security forced IT to interview college students for 24-hour temporary passwords

A university's security team once decided to implement device-bound two-step verification for everyone on campus – including the entire student population, who would frequently misplace or lose their devices altogether.

If a student needed to request a temporary new password to access the university network and resources, the security team required:

1. A face-to-face verification of the requestor's identity – either in-person or via Zoom teleconference.
2. In the meeting, the requestor showed official identification while answering multiple security questions.
3. Then, the team could issue temporary credentials… which lasted for only 24 hours.
4. If a student couldn't find their old device – or simply get a new one – in that time, then they would have to re-do the entire process!

If the security team had bothered to consult with their IT department before implementing the burdensome policy, they would have realized the more elegant solution would have been splitting the network by:

- Instituting a more limited student network with lighter authentications.
- Keeping the full interview-and-recovery process for a more-sensitive employee network.

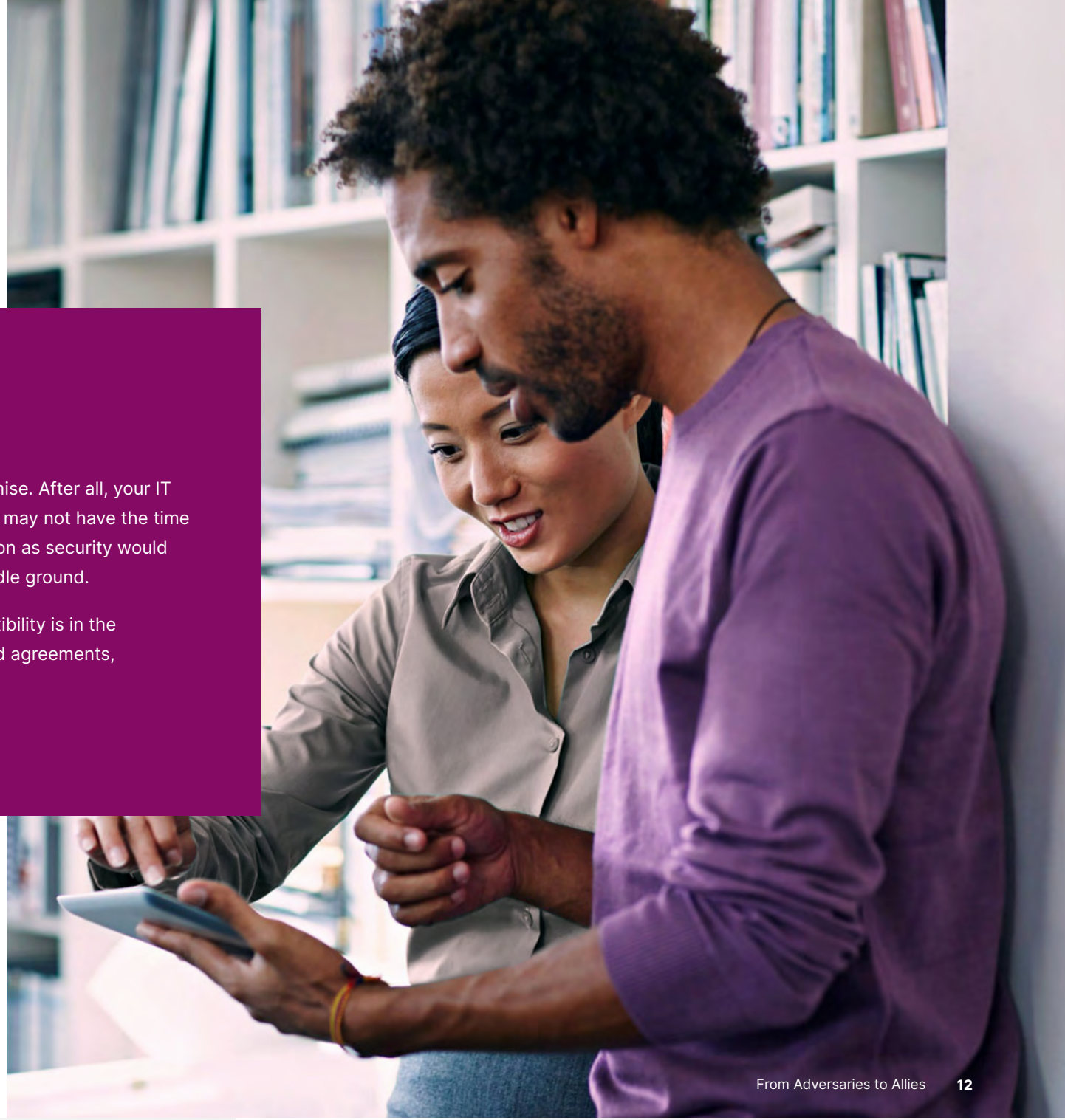
(After all, fully grown adult employees typically have greater incentive and mental capacity to keep track of their devices than younger university students.)

Such a split network system would have been sensitive to IT's needs, while still securing students' personal devices despite frequent college party losses.

Compromise!

Flex where you can, so you're not the "Department of No."

The art of compromise



When working with another department, expect to compromise. After all, your IT team's priority is keeping operations moving smoothly. They may not have the time in their schedule to release a patch or make a change as soon as security would like. By being flexible, security and IT can usually find a middle ground.

One of the ways in which you can proactively solicit this flexibility is in the establishment of mutually agreed upon service windows and agreements, usually codified through service-level agreements (SLAs).

ivanti

This SLA should define collaboration expectations and timeframes for each step, so everyone knows what will happen, when and from whom, including:

All definitions. You'll need to get more basic than you expect – even for something as basic as what your organization considers to be an "exploited vulnerability"!

Necessary specifications and tech stack deployments for each stage of a joint-department process.

- These processes can include anything from patch rollouts to new policy implementations.

Prioritization criteria. Figure out what counts as an emergency to security, versus what's an emergency to IT.

- Custom internal scales, rubrics and other internal evaluation methods can help standardize this part of the process. Develop these alongside your IT team as part of the SLA creation process!

Communication frequency during mutual projects. For example, consider the following process-related questions:

- When can IT expect to hear from security about the specific patch rollouts for a given Patch Tuesday?
- When can security expect to hear back from IT about any issues or confirmation of a successful patch rollout?
- At what point can an open request (from either side) be closed due to lack of response? When should higher-ups be included in the chain?

"Standard" timelines and deliverable expectations for each type of project, from each team – as well as explicitly listed and described exceptions to standard procedure!

Named points of contact or specific positions from each department.

- Their responsibilities will include resolving confusion over SLA policies and procedures, as well as annually reviewing and updating the SLA with their cross-department contact.

04

Develop and enforce shared goals with IT.

ivanti

Establishing shared goals

As we said before, while security and IT have different approaches, they share similar mandates: keeping the organization, its users and all processes running as smoothly as possible.

Therefore, it's worth taking the time to establish those shared goals with IT leadership – as well as creating key performance indicators (KPIs), dashboards and other shared measurements to reinforce the shared goals on a tactical daily basis.

For example, take patch rollouts. (It's a common example in this eBook, but for good reason!)

Both IT and security teams want an organization's technology to run smoothly. So, neither department wants a patch to interrupt workflow, if for different reasons:

- IT would rather not deal with all the help desk tickets generated by a poor patch implementation breaking app utility or connectivity.
- Security doesn't want to annoy end users and encourage them to seek risky workarounds and shadow IT implementations to do their jobs, if a (safer) patched corporate app actively interferes with their previously established workflows.

Enforcing shared goals means avoiding problem avoidance

Occasionally, the IT team's solution is to simply not roll out patches at all – especially if security can't guarantee a patch won't break mission-critical workflows. And, security teams may choose to forget the patch roll-out in the face of IT's pushback.

However, both IT and Security want to avoid dealing with a breach – which often occurs when devices and applications aren't regularly updated against active exploits.

While it's more obviously security's responsibility and burden to fend off cyberattacks, the IT team also suffers during a security breach.

After all, it's IT that must restore tech systems as quickly as possible, even while the security team ensures that backup is safe and all intruders removed from the network.

What will get dropped from IT's priority list if an attack occurs, prompted by an unpatched system?

And so, it's in both security and IT's best interest to figure out a robust patching strategy that works for both teams – all with the shared foundational understanding that all both teams want is to avoid interruption of organization processes at all costs.

Offer help:

Proactively share your own administrative resources, technical expertise and other tools.

Reciprocation makes for better collaboration

If you're asking for something from IT – such as borrowing and adapting their current IT tech stack, policies and processes for your own security use cases – then you need to give something in return.

While that often includes sharing the fiscal responsibility for shared tools and enterprises – with each team contributing a smaller portion of their budget to the shared tool than what it would cost to resource each individually – that help can take many forms.

Ultimately, by sharing tools and resources, security and IT teams can reduce their overall costs and improve collaboration.

Shared tools, dashboards and reports create a context for both teams to understand one another. These windows into each other's worlds build empathy and trust.

Knowing IT's values and priorities will help security teams gain buy-in for different projects in a way that is both practical for and considerate of their IT partners.

And, that buy-in will happen even faster if security offers a helping hand along the way – within reason, of course.

3 creative ways security can help IT beyond budgets

Administrative lifts	Many people – including IT team members – find the paperwork part of their jobs difficult. If it helps the other department think better of you, then offer to take that burden on, insofar as you can. For example, if your IT team predicts that a new security policy will impact ticket queues, then appoint a security specialist to answer all tickets and user queries related to the new policy. You could also "translate" the new policy for a non-technical audience from the original accepted proposal, and then give it to your internal communications team to share with internal stakeholders.
Technical expertise	You may suggest a new process or policy that seems simple to you, but leaves your IT contacts confused. Offer to hold a training session for the responsible IT personnel on the tactical implementations. Or, if you have time, configure the settings on IT's behalf. (Make sure any related troubleshooting materials are easily found for the IT people responsible for maintenance!) In return, ask IT admins to train security, so that your team has a basic understanding of how IT is run at your organization – even if they came to security from IT itself!
Shared resources	We go over how security can request the use of IT's technical capabilities in a different guide. (See "Shifting Security Left" for more details!) However, there's no reason you couldn't make certain security-focused tools available for IT use – especially access to any professional development or training materials you may have for your own team. Doing so will increase IT's understanding of security's mandate and position, which can only help you expedite future requests of their team.

Real-World Repercussions

Cross-department "swarming" out-of-band security risks

Security and IT teams alike often plan their month around the regular “Patch Tuesday” monthly releases through an established testing, piloting and rollout schedule, methodically addressing any implementation issues.

However, some patches drop “out of band,” sending everyone scrambling for two reasons.

1. **Out-of-band patch or remediation releases are usually active exploits,** requiring immediate implementation.
2. **Teams must deprioritize other critical tasks** to prioritize the newly released risk – tasks that continue causing problems while the emergency is resolved.

Rather than scrambling “all hands on deck” for these emergencies, mature organizations have developed a “swarming” method.

- They appoint a **dedicated out-of-band response team** of experts across multiple departments, including security and IT.
- When an out-of-band patch releases, **these teams “swarm”** around the emergency patch or remediation, completely focusing on the fix.
- Meanwhile, their parent departments **continue regularly scheduled** tasks and projects.

By forming these cross-functional teams before out-of-band patches drops, organizations can stay on track while quickly addressing inevitable emergencies.

"It's a culture shift, a swarming mentality.

“[When addressing out-of-band risks], we’re not trying to find who’s at fault. In most of these cases, a vulnerability is not the fault of anybody in the organization.

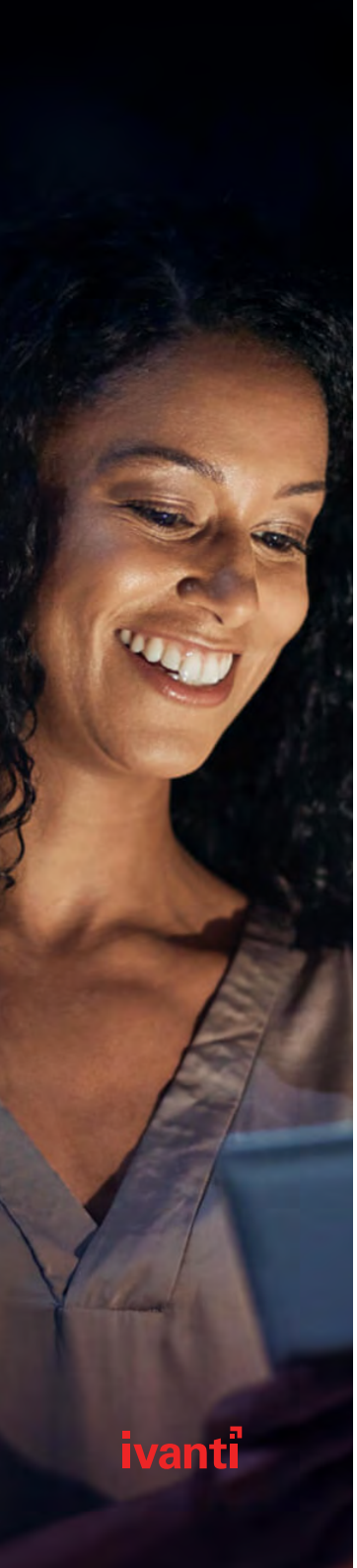
“Instead, in a swarming situation, it’s understood that we simply need to identify who's the best person to go and resolve this.

“Now that we've got that person identified, everybody else in the organization knows that if they're tapped to support that person during that swarm, that [remediation] is their new priority.

“Any other priorities shift down in priority until it's resolved.

“The organizations that I've seen that have adopted more of that swarming mentality respond with a healthier level of response and a typically faster response to the vulnerability being ultimately resolved.”

- Chris Goettl
VP of Endpoint Security Product Management, Ivanti



References

- Australian Cyber Security Centre. (30 June 2017). "Essential 8 Maturity Model": https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Bowermaster, P. (February 2023). "Shift Left to Risk-Based Proactive Security Management." CIO's The Future of Work Summit.
- Center for Internet Security. (2021). "Critical Security Controls Version 8": https://www.cisecurity.org/controls/v8
- Forrester. (2022). "The Total Economic Impact of Ivanti Unified Endpoint Management (UEM) Solutions": https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf
- Forrester. (2022). "The Total Economic Impact of the Ivanti Enterprise Service Management. A Forrester Total Economic Impact Study Commissioned by Ivanti": https://rs.ivanti.com/reports/forrester-tei-ivanti-enterprise-service-management-platform-2021.pdf
- GDPR.EU. (n.d.) "GDPR Checklist for Data Controllers": https://gdpr.eu/checklist
- Goettl, C. (25 March 2021). "Automated Patch Management and Team Swarming are Key Security Practices." Ivanti: https://www.ivanti.com/blog/automated-patch-management-and-team-swarming-are-key-security-practices
- Goettl, C., & Masserini, J. (1 September 2022). "Vulnerability Management in Real Life: 5 Best Practices from Real-World RBVM Programs." Ivanti: https://www.ivanti.com/webinars/2022/vulnerability-management-irl-5-best-practices-from-real-world-rbvm-programs
- Goettle, C. & Stryker, A. (11 May 2023). "Vulnerability Patch Prioritization Problems: Cybersecurity Research Results Part 2." Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12876518-vulnerability-patch-prioritization-problems-cybersecurity-research-results-part-two
- Harvard Business Review. (29 August 2022). "How Much Time and Energy Do We Waste Toggling Between Applications?": https://hbr.org/2022/08/how-much-time-and-energy-do-we-waste-toggling-between-applications
- Ivanti. (18 August 2018). "7 Experts on What Shift Left Means for IT Departments": https://www.ivanti.com/blog/7-experts-on-what-shift-left-means-for-it-departments
- Ivanti. (2022). "The NIST Cybersecurity Framework (CSF): Mapping Ivanti's Solutions to CSF Controls": https://www.ivanti.com/resources/v/doc/ivi/2694/63935da433e2
- Ivanti. (2022). "The Ultimate Guide to Risk-Based Patch Management": https://www.ivanti.com/resources/v/doc/ivi/2705/11190ce11e80
- Ivanti. (2023). "Press Reset: A 2023 Cybersecurity Status Report": https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465
- Ivanti. (2023). "ITSM+ Toolkit": https://www.ivanti.com/resources/v/doc/ivi/2760/e094c24df239

- Ivanti. (2023). “The Ultimate Guide to Unified Endpoint Management (UEM)”: https://www.ivanti.com/resources/v/doc/ivi/2508/b7d55619d0ee
- Ivanti. (28 June 2022). “2022 Digital Employee Experience Report”: https://rs.ivanti.com/ivi/2700/4e528f833de3.pdf
- Ivanti. (n.d.) “IT Jargon Explained: CMDB:” https://www.ivanti.com/glossary/cmdb
- Ivanti. (n.d.) “IESO Shifts Left for Streamlined IT Operations”: https://www.ivanti.com/customers/ieso
- Ivanti. (n.d.) “Southstar Bank “Shifts Left” with Ivanti Neurons”: https://www.ivanti.com/customers/southstar-bank
- Miller, T., & Spicer, D., Stryker, A. (19 January 2023). “IT vs Security: When Hackers Patch for Profit.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12071546-it-vs-security-when-hackers-patch-for-profit
- Morning Consult and IBM. (3 October 2022). “IBM Security Incident Responder Study”: https://www.ibm.com/downloads/cas/XKOY5OLO
- National Institute of Standards and Technology. (2018). “Framework for Improving Critical Infrastructure Cybersecurity” (p14): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Official Journal of the European Union. (14 December 2022). “Directive (EU) 2022/2555 of the European Parliament and of the Council”: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Oltsik, J. (2022). “ESG Research Report: Technology Perspectives from Cybersecurity Professionals.” Enterprise Strategy Group - Information Systems Security Association International: https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Security-Process-and-Technology-Trends-Jul-2022.pdf
- Perri, L. (2023, April 19). “Top Strategic Cybersecurity Trends for 2023.” Gartner: https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023
- Pickering, D. (2022, May 5). “What is DevSecOps? How Great Developers Shift Left for Security.” Ivanti: https://www.ivanti.com/blog/what-is-devsecops-how-great-developers-shift-left-for-security
- Rundle, J. and Nash, K. (2023, May 22). “Security Chiefs Trim the Fat.” The Wall Street Journal: https://www.wsj.com/articles/security-chiefs-trim-the-fat-as-budgets-bite-83c82f99
- SAM. (July 2022). “IoT Security Landscape Report”: https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program
- Shackleford, Dave. (March 2022). “SANS 2022 Cloud Security Survey”: https://8645105.fs1.hubspotusercontent-na1.net/hubfs/8645105/white-paper/sans-2022-cloud-security
- Verma, A., Goettl, C., & Hindman, M. (2022). “How to Win Budget and Influence Non-InfoSec Stakeholders for Your 2023 Cybersecurity Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program

From Adversaries to Allies

5 ways to align your security team with IT

ivanti.com
1 800 982 2130
sales@ivanti.com