C/Ɔ CYBELLUM

Building a PSIRT From the Ground Up

The people, processes, and tools for a successful PSIRT organization

The Colonial Pipeline cyber security breach in 2021 marked a watershed moment in IT security. Though this attack shut down the largest oil pipeline in the U.S. and resulted in a $4.4 million ransom payment, it most likely made headlines simply because it represents in shocking clarity the most disturbing cyber security trend of recent years: Attacks on operational technology (OT) have now gone mainstream.

Other recent attacks underscore this conclusion, including the Oldsmar water purification plant breach and an attack against JBS SA, the world's largest meat processor, that led to an $11M ransom payment. Every industry, from hospitals and medical devices to automotive and industrial machinery, has seen a rise in attacks targeting non-traditional endpoints. No longer content to hack email or web servers, attackers are going after "real-world" devices that control production lines, vehicles, cameras, and more. And these attacks could have particularly devastating and immediate real-world consequences.

The primary challenge facing business leaders in manufacturing today is that the expansion in operational technology, intelligent devices, and IoT has been absolutely essential from a business standpoint. For any company looking to stay relevant, there's no question of not adapting to the times and integrating today's wide range of connected devices and processes. But as business leaders have started to realize, all this connectivity has also broadened their attack surface, creating the need for an integrated, cohesive security approach.

Any vulnerability in a connected product or device can potentially be exploited to make it perform unpredictably, opening up a nearly infinite range of potential repercussions when it comes to safety — along with massive monetary losses and damage to your reputation. Many companies — particularly small- and medium-sized businesses — never recover from a cyber attack. It's up to you to ensure that your company can grow and adapt, harnessing the best of today's technology and connectivity while creating a hardened, resilient security posture that ensures you won't be the next company to show up in the headlines.

In this whitepaper, we'll look at the product security incident response team (PSIRT), which brings stakeholders together to establish a unified, hardened posture that intelligently anticipates risks and ensures resilience if the worst does happen.

Today, if you're manufacturing software-driven devices, regardless of your industry, you need a PSIRT. To help you get up and running efficiently, we'll explore popular models for setting up a PSIRT, then look at three crucial elements you need in place to drive its success.

The need for *a PSIRT*

In most cases, following a cyber attack, businesses fail because they lack a coordinated, unified response to threats and breaches. Instead, there are ad hoc processes that fail to come together at critical times, leaving major aspects of security to fall through the cracks.

But a growing number of companies — across industries including communications, automotive, medical, energy, and many more — are being proactive and facing the growing risk by creating an integrated PSIRT.

Establishing a PSIRT recognizes a key reality for most larger companies today: Many components are shared across products. Coupled with the growing demand for standards and regulatory compliance, this fact means that security can no longer be a siloed activity, separated by department.

The most recent PSIRT Services Framework, created by the FIRST community, provides several models for creating a PSIRT within your business, with the goal of ensuring seamless product security that's tightly integrated with the rest of the company's operations. This framework suggests three primary models: distributed, centralized, and hybrid. The main difference between the three models has to do with where the PSIRT is drawn from and the hierarchy of who they report to.

01 | Distributed PSIRT

Representatives of teams across your organization (engineering, support, management) serve together within the PSIRT and report to team leaders.

✓ PROS

Best for organizations with a wide range of products, can easily scale the PSIRT as needed, costs distributed across the organization

✕ CONS

Less control over individual departments, so staff lack accountability to the PSIRT

02 | Centralized PSIRT

A larger team of PSIRT staff are distributed among multiple departments across the organization (engineering, support, management) and report to security executives.

✓ PROS

Best for organizations with a few, homogeneous products; collects experts and creates tighter accountability

✕ CONS

Does not scale as well as distributed model, cannot adapt easily to expanding product range, makes the PSIRT a new cost center

03 | Hybrid PSIRT

Considered the “best of both worlds,” this PSIRT has the flexibility to fit multiple organization types and sizes, along with varied product ranges. This will generally make use of a smaller team, as in the distributed model, but likely retains accountability to senior executives to create a focused, “the buck stops here” approach. The hybrid approach will look different for every organization.

✓ PROS

Adapts readily to the size and scale of your organization

✕ CONS

May lack clear coordination and hierarchy unless care is taken during planning phases

Key components of your PSIRT

Regardless of the model you choose, there are a few essential common elements that drive the success of your PSIRT. Every single PSIRT relies on the right combination of people, processes, and technology, which we will explore in the following sections.

01 | People

One of the first steps in setting up a PSIRT is creating a staffing plan, which identifies the skill sets needed and competencies expected when selecting individuals for the team. If existing staff don't possess the necessary skills and competencies, the staffing plan should also determine whether these will be met through outsourcing, vendor support services, or upskilling existing team members with appropriate, role- based training. According to FIRST, all team members should have at least "a solid understanding of basic security concepts and knowledge of the products that are being supported."

At the very least, you'll want to create the following roles within your PSIRT:

PSIRT Manager

A central head or managing executive to whom the rest of the team reports, the manager's primary responsibility is to oversee the operations of the PSIRT initiative. This includes the creation of policies, processes, procedures, and guidelines for the team's operations. The PSIRT manager also represents the PSIRT within the organization and ensures ongoing buy-in from management—critical for making the PSIRT a priority in the budget—and internal stakeholders.

PSIRT Analysts

These are the people who handle the analysis and remediation of security vulnerabilities. Analysts have to continually monitor a variety of sources for vulnerabilities, attack techniques, and potential threats that may pose a risk to the company's products; they also work with product teams to pinpoint and remediate vulnerabilities. See the Process section below for details.

Security Points of Contact

There should be points of contact designated in each of the organization's product or business lines who take responsibility for addressing all security issues in their domain, including risk quantification, analysis, and remediation across all affected product versions.

Legal Points of Contact

The role of the legal POC is to ensure that there is no violation of IP or liability issues due to incidents, SLAs with customers, etc., along with any other regulatory concerns arising from PSIRT operations.

Communications Contact

This team member must be skilled in crisis communications for on- message and ongoing incident response. This can be a high-pressure role—for instance, handling media inquiries during the investigation of a breach for which answers are not yet readily available, along with rebuilding the brand and reputation following the incident.

02 | Processes

To ensure that operations run smoothly when a security event arises, the team must define key policies and procedures ahead of time. Many of these activities must be established during the "peacetime" prior to an incident, so that positive practices will already be in place if and when a threat occurs.

Maintaining a A Central Repository

As part of the peacetime routine, the PSIRT should create and maintain a central repository of all products and software. A given product or asset may comprise dozens of components from a number of different suppliers, with each supplier developing the underlying software on various platforms and hardware architectures. Hence, listing all software components, versions, and configurations is no small task.

The PSIRT needs to upload the resulting software inventory or SBOM (software bill of materials) to the central repository and keep it up-to-date with every new product version or update. You can then manage this data using a dedicated asset management tool (see the Technology section below), ensuring the team has continuous real-time access to security data for all your latest product versions, as well as their distribution to customers.

Identifying and Involving Stakeholders

The PSIRT must also identify the various stakeholders with whom the team may need to interact when a security event arises. These can include parties inside a company, such as leadership and development teams, as well as outside entities, including component providers, developers, and customers.

The team needs to establish processes and mechanisms to facilitate the sharing of information with each of these stakeholders (e.g., a vulnerability disclosure framework). This will include creating incident response (IR) playbooks defining procedures both for attack conditions and peacetime training.

Actively Monitoring Threats

The third type of PSIRT process revolves around the collection of threat intelligence, including data on product vulnerabilities, vulnerable third-party components (e.g., TCP/IP stacks), and architectural weaknesses. Your PSIRT should spread a wide net, actively checking channels such as exploit databases, news outlets, technical blogs, and social media for relevant news, as well as subscribing to relevant vendor advisories and security mailing lists for open-source projects.

The team should also maintain a vulnerability disclosure program and advertise contact points to facilitate submissions by interested parties. Your threat monitoring process needs to include deliberately establishing and engaging with an active ecosystem of partners, peers, and researchers (or "finders") with relevant security expertise to share threat intelligence.

A PSIRT should also invest in actively hunting for new attack techniques and potential threats. During peacetime, this can mean creating guidelines, including recommendations or best practices that are passed along to product security and development teams, or even holding workshops on relevant topics. This will help establish and facilitate routine product security assessments within the framework of the entire secure software development lifecycle (SDLC).

Organizations that foster secure development lifecycle practices—and invest in building them—will spend less overall on remediating security flaws by catching them earlier in the development process.

Screening, Analyzing, and Remediating Incidents

Last but by no means least, the PSIRT must define a process for responding to cybersecurity incidents. While the aim of establishing a PSIRT is that these incidents will ideally be less threatening and have fewer repercussions for the organization as a whole, it is obviously still essential to have these processes in place.

The process of incident analysis will vary depending on the organization: Companies that receive a high volume of vulnerability reports may need to screen and validate each report before creating a ticket or case. The identified risk(s) can then be prioritized and communicated to the relevant team. Defining the exact policies and mechanisms for this process ahead of time ensures maximum efficiency when it's crunch time.

The PSIRT needs to have predefined processes and mechanisms in place for risk analysis and remediation, including root cause analysis across all affected products and versions, as well as delivery of a patch or other remedy to all relevant stakeholders. The incident post-mortem process should also address the need for ongoing education and awareness among the product development, engineering, and management teams.

03 | Technology

Once the right people and processes are in place for your PSIRT, you can begin to identify and evaluate technologies that can support them.

This stage demands caution. While a rise in awareness across multiple industries is a great starting point, this has resulted in a number of vendors providing individual tools that promise to solve one piece of the technology puzzle. Yet you need to be very careful about adopting a piecemeal approach to security—not all the components you select may integrate with one another, and you may find that you're paying too much for overlapping security tools.

Instead, look for a single platform that incorporates the comprehensive, security-first needs of your PSIRT, throughout the entire product lifecycle. This is really the best way to protect your customers — and your business.

Technologies you need to support your PSIRT team include:

Asset Management

Creating, analyzing, and maintaining an up-to-date inventory of all products released to market and their detailed bill of materials (SBOM), along with versioning, licenses, OS configurations, and more, is not as simple as you might think. Supply chain complexity means you also need to be aware of third-party and open-source components. You can't track and fix risks you can't see.

Threat Intelligence

Software threat management is a constantly shifting tide pool of new and evolving weaknesses, CVEs, zero-days, exploits, and attack techniques. Don't get sucked in. A modern PSIRT platform will provide continuous monitoring and aggregation of vulnerability and threat feeds such as the NVD, VulnDB, Exploit Database, and Metasploit.

Impact-Based Incident Response

As so many companies have discovered, threat intelligence is worse than useless without a deep understanding of which threats are most relevant to your business, resulting in a flood of alerts that can distract your team from its core mission — or, worse, go ignored and unresolved. An automated PSIRT platform can provide relevancy checks across all your assets. This gives you the context you need to focus on threats that truly impact your products and improve your team's focus, reducing the time and effort needed for forensic analysis and incident resolution.

Digital Twinning

With digital twinning, you can scan and pinpoint potential vulnerabilities and other issues using an exact blueprint copy of your system and all its components, including the OS, encryption, control flows, and API calls. This lets you reproduce attacks and test overall resilience with zero risk to your
organization and your customers.

Workflow Tools

Any PSIRT platform must integrate into the way your company works. By creating and routing tickets for new security incidents, as well as tracking each issue to its resolution, you ensure that nothing falls through the cracks. Tickets should be meaningful — including a full impact assessment on components and devices — with clear guidance to resolve threats and policy violations.

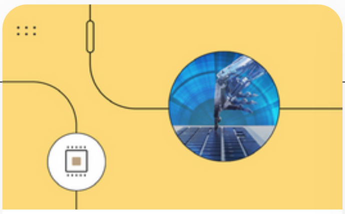
Reporting

By providing data and metrics around PSIRT performance, such as time to resolution (TTR), your team can demonstrate ROI from day one, proving its value in reducing the number and impact of security incidents. This business outcome data in turn helps stakeholders understand the essential role of the PSIRT and provide for an ongoing allocation of budget and other resources.

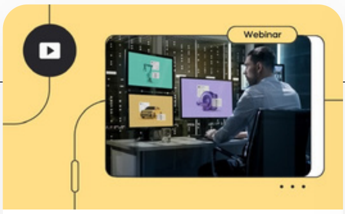
Shifting gears: toward the PSIRT future

Establishing a PSIRT can help your organization shift gears from being in reactive mode to leveraging a well-oiled, proactive security posture. Once you have the right people, processes, and resources in place, your PSIRT will ideally function not as an isolated module within your organization, but instead operate in lockstep with the product, engineering, and support teams, driving best practices across all departments.

Dive deeper



Implementing Proactive Product Security With PSIRT Automation



Securing Connected Devices in the Field: from Monitoring to Incident Response

Peacetime PSIRT Activities – Getting the Most of Your PSIRT Investment

Easily manage post production risk

Naturally, all three elements — people, processes, and resources — are essential to success. However, when it comes to resources, there are many possible pitfalls. With an integrated PSIRT platform, you can ensure that you avoid any problems you could encounter trying to adopt a variety of products from multiple vendors.

How it works

Go from detection to investigation under one roof. See your most relevant risks to their post-production products, then facilitate detailed investigations - all in one central location.

Automate PSIRT grunt work so you can focus on thorough investigations -Quickly clear through noise and identify your products' most urgent vulnerabilities. Integrate seamlessly with your SIEM, SOAR, and other operational systems, so you can quickly mitigate incidents.

Keep your finger on the pulse of all security-related events - Take decisive steps against the most relevant cyber risks, all in the context of your specific products and systems. Slash time to remediation and take critical steps towards keeping post-production products continuously secure.

Automate threat intelligence - Automated aggregation and monitoring of threat intelligence sources identify what's relevant to your specific products.

Facilitate entire investigations - Get a workbench for creating and managing investigations, from comprising relevant info, to formulating the analysis, and opening relevant tickets. Then, generate customized reports for each individual stakeholder.

Reduce remediation times - Leveraging pre-existing data about your product's software saves you time on threat monitoring, investigations, and mitigation activities.

Comply faster with post production standards - Ongoing data collection of all product security activities allow you to meet standards from CISA, FDA, IMDRF, ISO, and others.

Across a range of industries, including automotive, medical, and industrial, Cybellum's platform empowers device manufacturers and their suppliers to identify and remediate security risks at scale, throughout the entire product life cycle.

Get your PSIRT program up to speed. Book a demo.

Learn More about Product Security

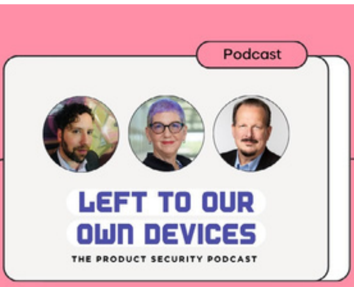
Blogs

The US National Cybersecurity Strategy Through A Product Security Lens

EV Charging Stations: An Emerging Threat for Automotive OEMs

Keeping the Software Supply Chain Accountable with SBOMs

Podcasts



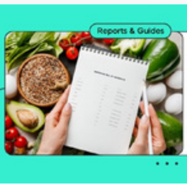
Knowledge Base

Webinar

Making Your Medical Devices Cyber Compliant for the Omnibus: from Theory to Practice

Learn More →

Reports & Guides



SBOM for Connected Devices: Getting it Right

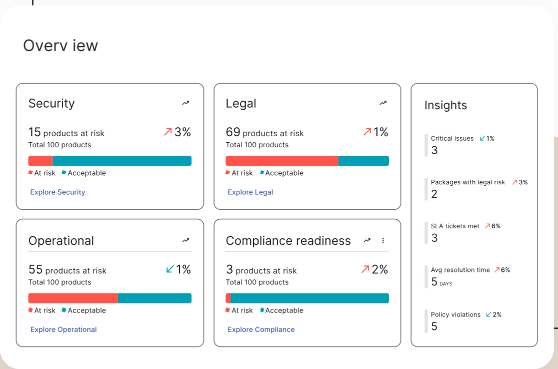
Learn More →

Case Study

LG Vehicle Component Solutions Case Study

Learn More →

More about the Product Security Platform



Overv iew

Security
15 products at risk ↗3%
Total 100 products
At risk Acceptable
Explore Security

Legal
69 products at risk ↗1%
Total 100 products
At risk Acceptable
Explore Legal

Operational
55 products at risk ↙1%
Total 100 products
At risk Acceptable
Explore Operational

Compliance readiness
3 products at risk ↗2%
Total 100 products
At risk Acceptable
Explore Compliance

Insights
Critical issues ↙1%
3
Packages with legal risk ↗3%
2
SLA tickets met ↗6%
3
Avg resolution time ↗6%
5 DAYS
Policy violations ↙2%
5

Follow us for news and updates

cybellum.com