PROCESSUNITY THIRD-PARTY RISK MANAGEMENT

Threat & Vulnerability Response

Identify, Assess, Respond, and Report on Emerging Threats and Vulnerabilities in Your Extended Third-Party Ecosystem

Threat & Vulnerability Response

Third-Party Risk Management (TPRM) teams face a sea of vulnerability data that holds warning signs of the next security incident. When a new vulnerability emerges, you need to sift through this data to rapidly understand the size of the problem, identify affected third parties, and respond with remediation actions. Only then can you assure your leadership team that your organization will minimize its potential for loss.

With ProcessUnity Threat & Vulnerability Response, you adopt a turnkey solution that empowers your team to efficiently identify, assess, respond, and report on threats and vulnerabilities in your organization's extended ecosystem. Designed to shorten your team's response time from weeks or months to days, ProcessUnity combines our powerful TPRM Platform with unmatched third-party risk data from our Global Risk Exchange to promote a fast and informed response.

Threat & Vulnerability Response Solution Components

- Active Monitoring Service for Emerging Threats
- Continuous Threat-Monitoring and Alerts
- Portfolio-Specific Threat Prioritization
- Comprehensive Threat Intelligence Alerts
- Advanced Threat Intelligence
- Assessment Scoping & Scoring
- One-Click Executive Reporting

Why ProcessUnity Threat & Vulnerability Response

Advanced Protection

Identify and mitigate threats before they cause catastrophic harm.

Provide expanded third-party coverage without the need for additional headcount.

Streamline the steps to thwart breaches that may originate from a third-party vendor.

Efficient Response

Streamline your response to mitigate the impact of an attack.

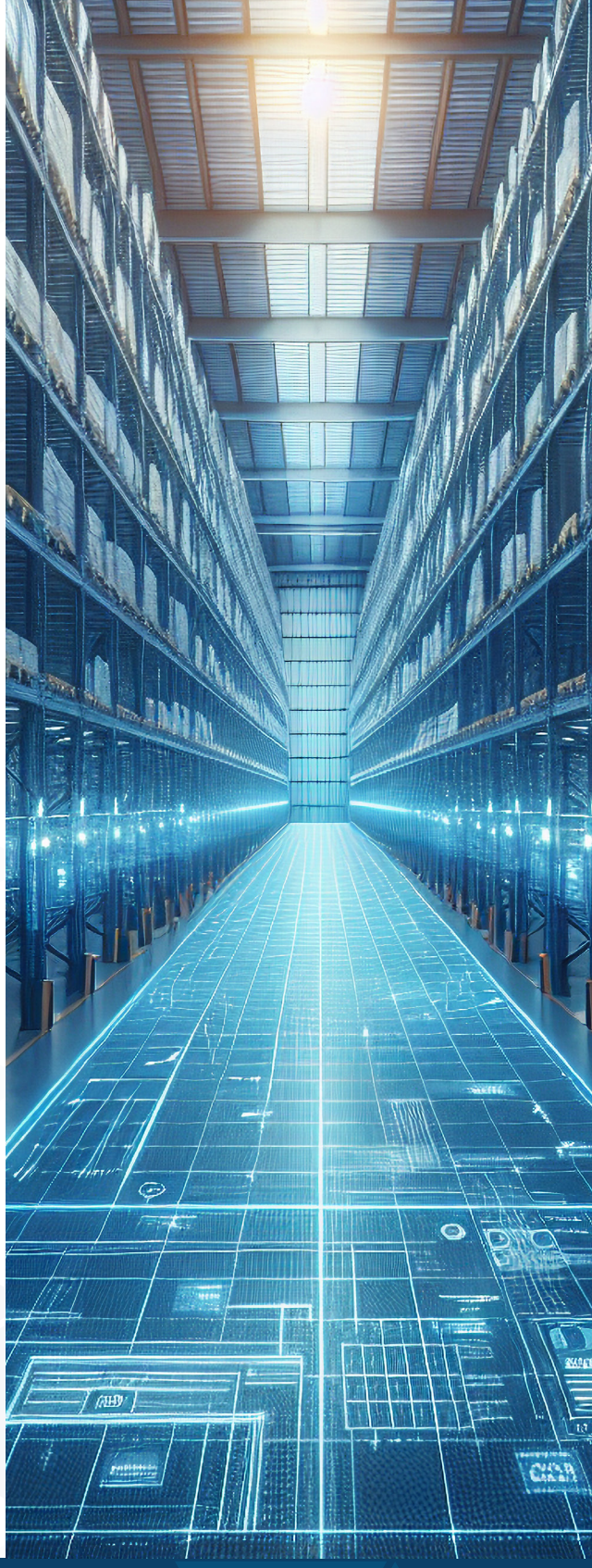
Respond in hours and days instead of weeks and months, or even worse, not at all.

Coordinate your response based on the third parties most likely to be impacted.

Demonstrated Effectiveness

Show management that you have an effective and efficient process for managing exposure to known vulnerabilities.

Generate summary reports with the push of a button, proving your team's efficiency and effectiveness in crisis situations.



ProcessUnity combines our powerful TPRM Platform with unmatched third-party risk data from our Global Risk Exchange to promote a fast and informed response.

How We Help

Continuous Indicator of Compromise Alerts

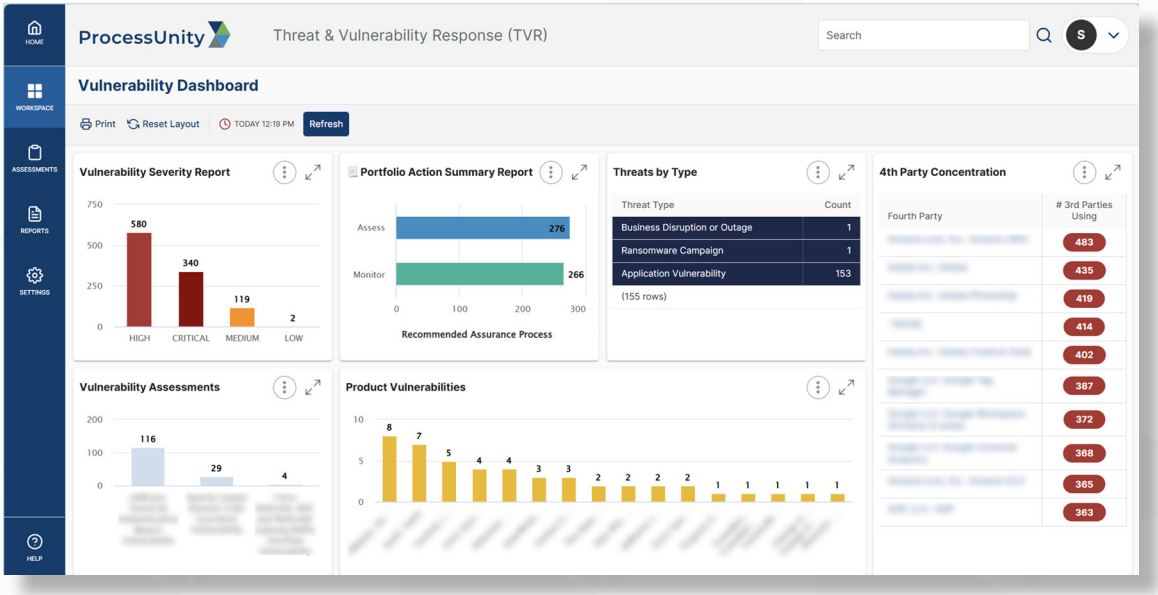
With a growing workload and ever-increasing exposure, your team may struggle to monitor active cyber threats continuously, risking a delayed response to a known vulnerability in your third-party ecosystem or an inability to get ahead of critical threats.

You need a way to identify critical threats quickly and efficiently to assess your exposure correctly. But with limited resources and an ever-increasing number of third parties in your portfolio, how can you get out in front of an active threat?

Complete Visibility into Active Cyber Threats

With ProcessUnity Threat and Vulnerability Response, your team gains portfolio-relevant, real-time intelligence for active threats and vulnerabilities referenced in the NIST NVD and CISA KEV. Critical alerts, aligned to your third-party portfolio, inform you of the severity of an active vulnerability and provide remediation guidance. The ProcessUnity Threat Research Team continuously monitors for active threats relevant to you, delivering complete visibility so you can make efficient and informed decisions.

The ProcessUnity Threat Research Team consists of cybersecurity and infosec professionals who continuously monitor CISA KEVs and actively map controls to emerging threats in the ProcessUnity platform. When CISA classifies a KEV and identifies the MITRE Tactics, Techniques, and Procedures (TTPs) used to exploit the vulnerability in question, ProcessUnity publishes a Threat Profile so you can analyze your portfolio to determine which third parties are susceptible to this specific exploit.



Get an at-a-glance view of the state of threat and vulnerability response across your organization, including severity reports and assessment status updates.

Prioritized Threat Alerts

How do you know where to focus with so many vulnerabilities being tracked? Even if your organization maintains effective oversight, your extended supply chain could face disruption from your vendor's suppliers or your subcontractors.

With expansive fourth-party technographic insights, ProcessUnitymaps each vendor and impacted product to the vulnerability, reducing the noise by alerting you to vendors who use the vulnerable technology or service.

The Industry's Most Comprehensive Threat Intelligence

ProcessUnity leverages Recorded Future data to actively monitor social media and the dark web for threat indicators, delivering the industry's most advanced integrated threat intelligence for third-party risk management. This comprehensive view of active and potential threats helps identify gaps or control deficiencies within your third parties that may increase your organization's risk. When ProcessUnity detects an indicator of compromise via Recorded Future, a near-instantaneous alert keeps your team in the know. It's the most comprehensive threat intelligence out there.

Vulnerability Name / Third Party	4. Other Vulnerabilities	1. Vulnerable Software Version	2. Vulnerability Impact	3. Unable to Remediate
	--	--	--	--
Apache Log4j2 Remote Code Execution Vulnerability				
[redacted]	No	Yes	Yes	No
[redacted]	Yes	No	Yes	No
[redacted]	Yes	Yes	Yes	Yes
[redacted]	No	No	Yes	No
[redacted]	Yes	Yes	No	Yes
[redacted]	No	Yes	Yes	No
[redacted]	Yes	Yes	No	Yes
[redacted]	Yes	No	Yes	No
[redacted]	Yes	No	No	Yes
[redacted]	No	No	No	No
[redacted]	Yes	No	No	No
[redacted]	No	No	No	No
[redacted]	No	No	No	Yes
[redacted]	No	No	Yes	Yes
[redacted]	No	Yes	No	No
[redacted]	No	No	No	No

Streamline your review of third-party responses to the emergency vulnerability questionnaire with configurable non-preferred responses and questionairre scoring.

Prioritized Portfolio-Relevant Assessments

Maintaining ongoing exposure assessments becomes more complex as your organization grows and incorporates more third parties. This is especially true when dealing with a critical threat. How can you prioritize which third parties need evaluation?

Narrow your Focus Based on Inherent Risk

ProcessUnity prioritizes third parties for you and your team to assess in response to each active threat, accelerating your response to a serious threat by targeting affected vendors for assessment. The inherent risk scores, as defined in your internal inherent risk questionnaires or via ProcessUnity's AI-driven Auto Inherent Risk Score, identify your most critical third parties to assess..

Technographic and Demographic Refinement

Each critical vulnerability is evaluated to identify demographic and technographic signals mapped to the MITRE ATT&CK Framework. ProcessUnity Threat and Vulnerability Response cross-references these signals with your portfolio to identify any organization:

- Using the vulnerable application or technology, or
- That fits the active threat's exclusive victimology profile or industry.

The result is a highly targeted list of third parties for you to assess, resulting in a manageable, timely, and focused Threat and Vulnerability Response campaign that yields better results faster.

Vulnerability Impact Assessments & Reporting

Doing an assessment and reporting the results takes time. And because this is an active threat, time is not on your side. You need to issue the assessment quickly, get prompt results from your most critical third parties, and inform the stakeholders in your organization of your progress.

Launch Impact Assessments Based on Threat Metadata

Once your list of prioritized third parties is complete, ProcessUnity initiates its threat response workflow. The collected metadata related to the active threat automatically populates the threat response template, and a customized questionnaire for the active threat is sent to each organization on the prioritized list. Because the questionnaire only includes details necessary to assess the current vulnerability, response from your third parties is much faster than expected for a typical due diligence assessment. For those third parties that don't respond promptly, ProcessUnity workflow sends out reminders and alerts to trigger a response.

Validate Submissions Against Preferred Responses

As your third parties respond, ProcessUnity tabulates the results in a dashboard so you can quickly assess and compare their answers against your preferred criteria. The workflow engine initiates the mitigation process by creating an open issue if a response does not align. The result is a highly efficient and rapid response to any critical threat.

Push a Button, Generate a Report

Often, the anxiety and frustration of senior executives and the board during a critical crisis can be mollified with transparency. This is especially true during an active cyber threat. ProcessUnity Threat and Vulnerability Response provides summary reports to educate leadership on assessment status. With the push of a button, you can generate a report demonstrating the effectiveness of your process, showcasing your leadership and your team's efficiency during an active cyber threat crisis.

Stay Ahead of Emerging Threats & Vulnerabilities

Ready to gain a better way to manage emerging threats and vulnerabilities? Contact us on our website to learn more.

ProcessUnity Third-Party Risk Management significantly reduces third-party onboarding and due diligence cycle times. Fueled by best-in-class workflow software, a universal data core for all TPRM information, the world's largest third-party risk exchange database and powerful artificial intelligence capabilities, ProcessUnity enables organizations to proactively mitigate first- and third-party risks.

ProcessUnity

www.processunity.com/TVR

240823