08/05/2020

Continuous Third-Party Risk Assessment for the Ever-Changing Security Reality

Allan Liska
Threat Intelligence Analyst, Recorded Future

Recorded Future®

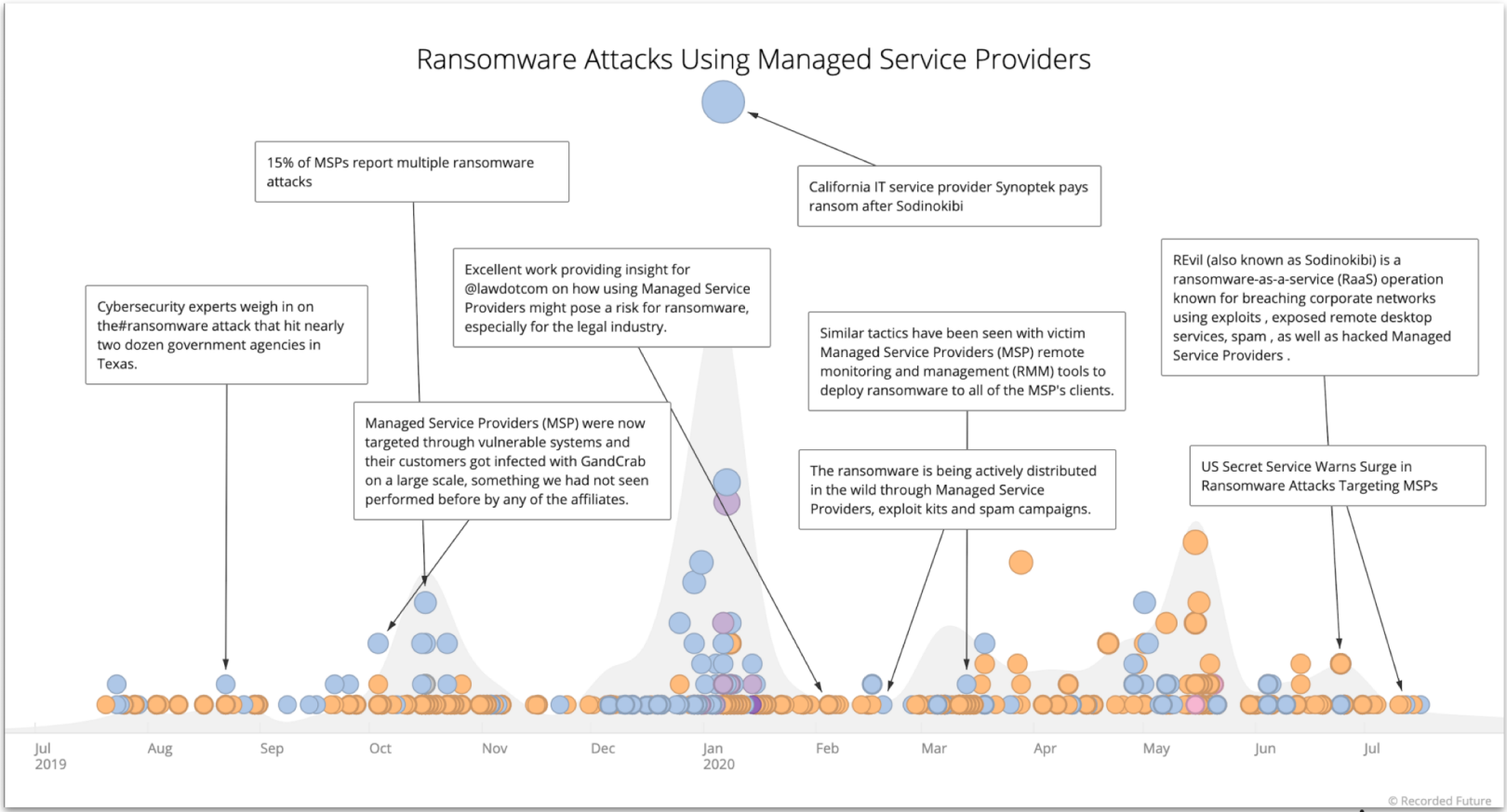
About Allan Liska

Allan Liska is an intelligence analyst at Recorded Future. Allan has more than 15 years of experience in information security and has worked as both a blue teamer and a red teamer for the intelligence community and the private sector. Allan has helped countless organizations improve their security posture by using more effective and integrated intelligence.

Introduction

- Risk Management budgets are being cut.
- But, risks continue to grow and your team is still expected to deliver the same level of assessment, if not more.
- Outsourcing is a fact of life with tightening budgets, which means the number of third parties connecting to your organization is going to increase.
- Understanding the risks posed by all of these vendors is a challenge.
- Continuous third party risk assessment (TPRA) helps improve your understanding of the risks and can save your organization money.

The Risks from Third Parties is Growing…



https://app.recordedfuture.com/live/sc/5AdB5CTQiIJW

Recorded Future®

However …

- Before an organization can understand the risk from their vendors, they need to know who their vendors are.
- Good vendor population and inventory is a foundational and critical part of any third-party vendor program.
- Shadow IT and other methods of procurement can make tracking third-party inventory difficult.

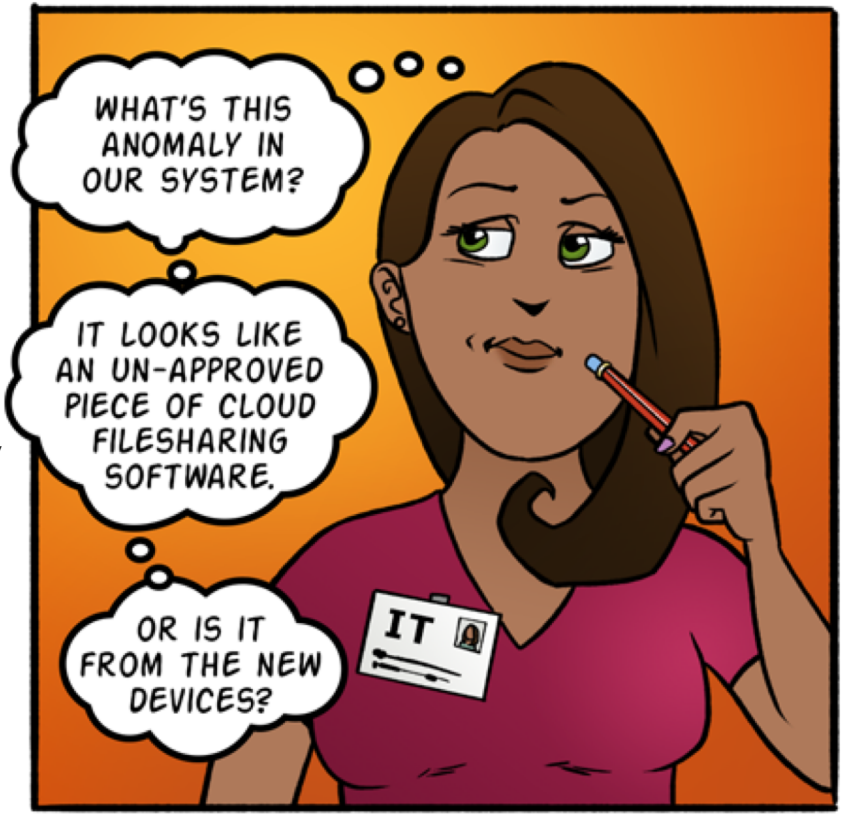


Image source: Symantec

Continuous Monitoring Can Augment Surveys

- Surveys are still an important part of Third Party Risk Assessment.
- But surveys are expensive. They take a long time to fill out, provide only a snapshot in time, and take a long time to enter the data.
- As the the number of partners and vendors who connect into your organization increase, the cost of surveys become more expensive.

Creating Tiered Vendors

- Many organizations help mitigate the cost by creating tiered vendor systems.
- Critical (Tier 1) vendors are assessed more often, while lower tiered vendors (Tiers 2 - 4) are assessed less often.
- Tier 1 vendors might be assessed biannually. Lower tiered vendors could be assessed annually or even less often.

Continuous Monitoring and Tiered Vendors

- With continuous monitoring in place, your organization can help determine how often you need to assess your tiered vendors.
- If you are assessing Tier 1 vendors annually, but find that that Risk Score of one of your Tier 1 vendors has changed significantly, you might move to assessing that vendor more often.
- Conversely a lower tier vendor with no change in Risk Score might be assessed less often, saving your team money and time.

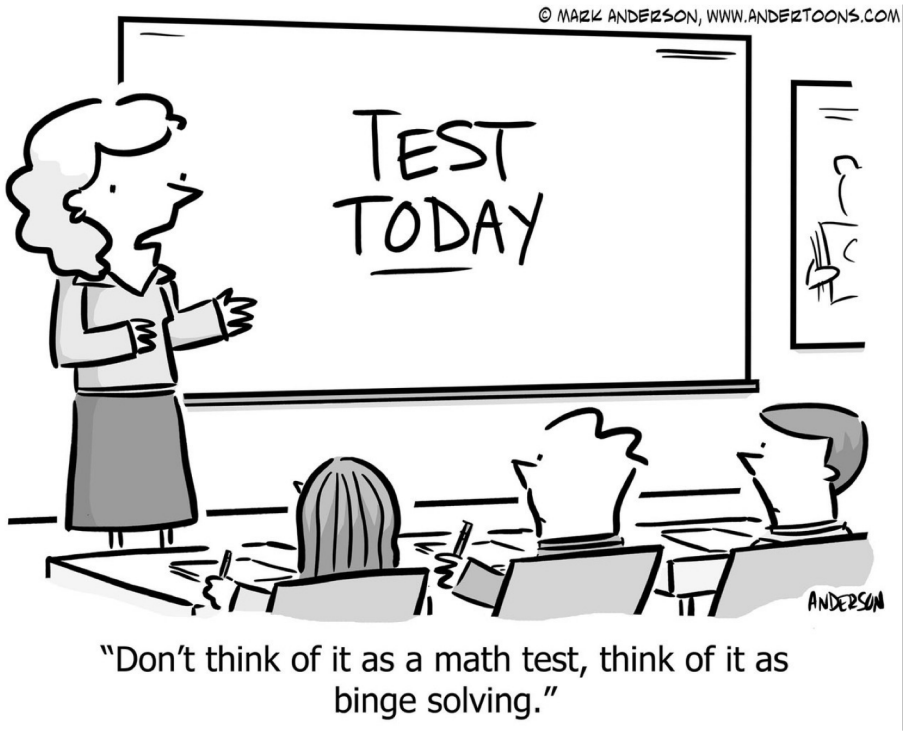


Image: https://andertoons.com/testing/cartoon/7503/dont-think-of-it-as-math-test-think-of-it-as-binge-solving

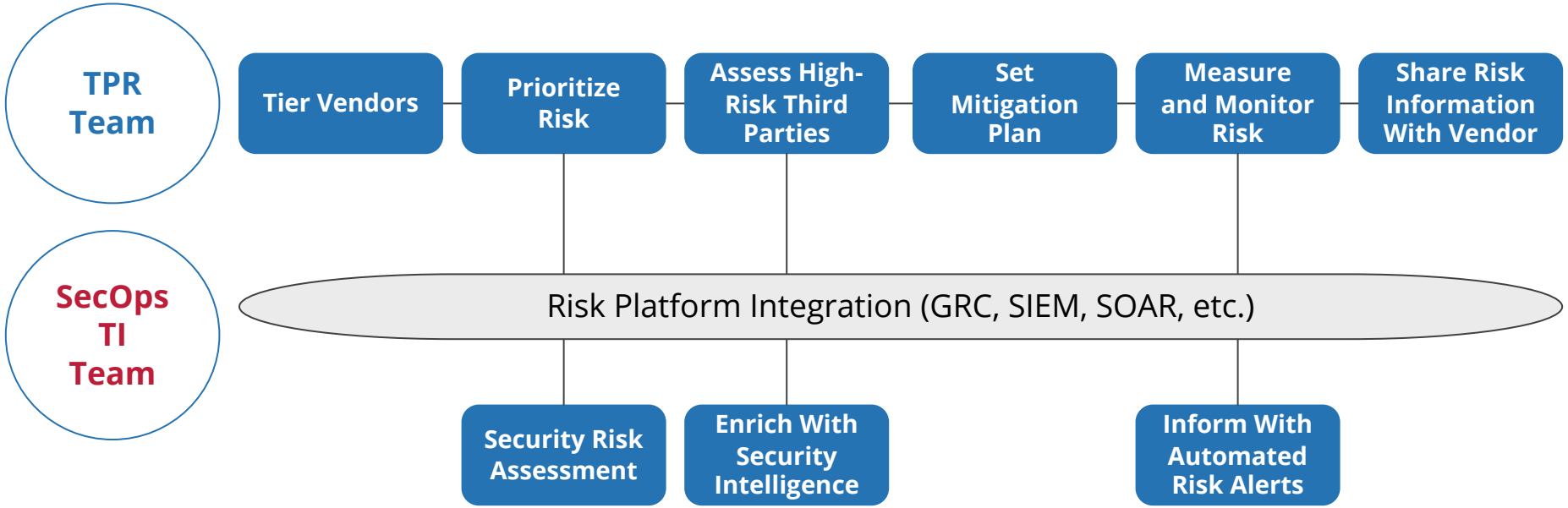
Continuous Monitoring and Custom Assessments

- Assessments take a long time to fill out, and it takes a long time to enter the data into your database.

- With continuous monitoring from objective third parties your organization can pre-populate some, if not most, of the assessment answers. Or only send parts of the assessment you need answers to over to vendors.

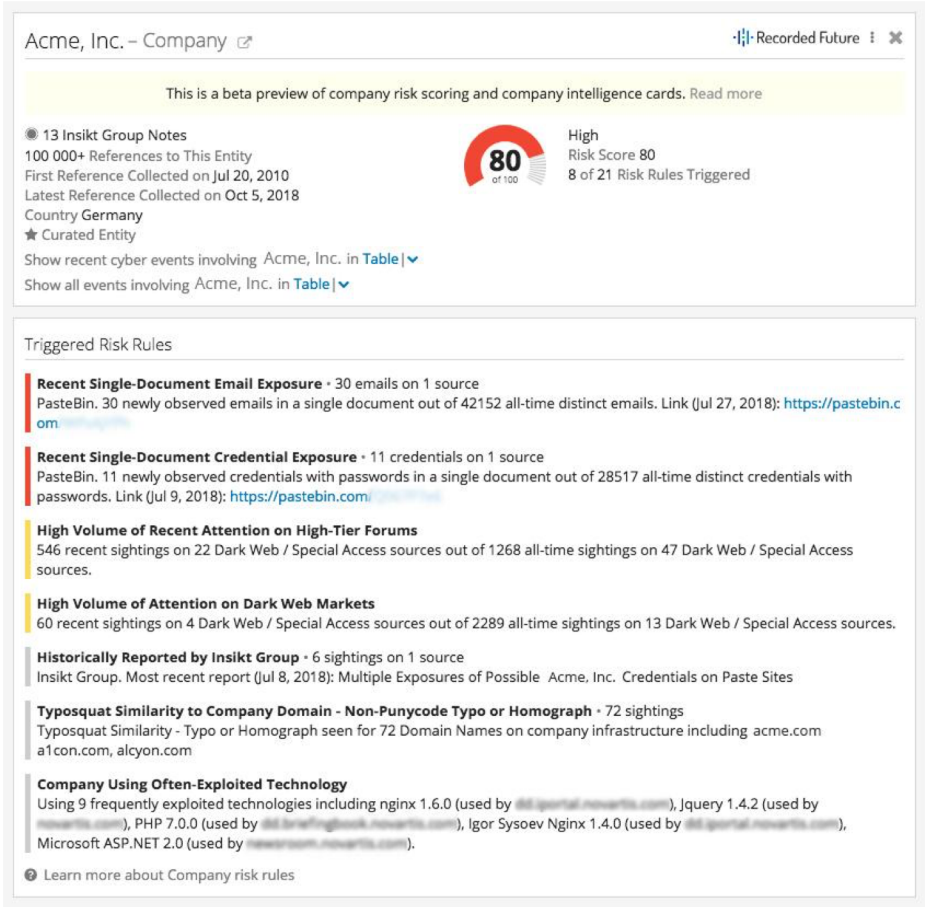
- Again, this helps your partners and vendors save time and money, can speed up the procurement process, and save your organization a lot of money as well.

What Does This Automation Look Like?



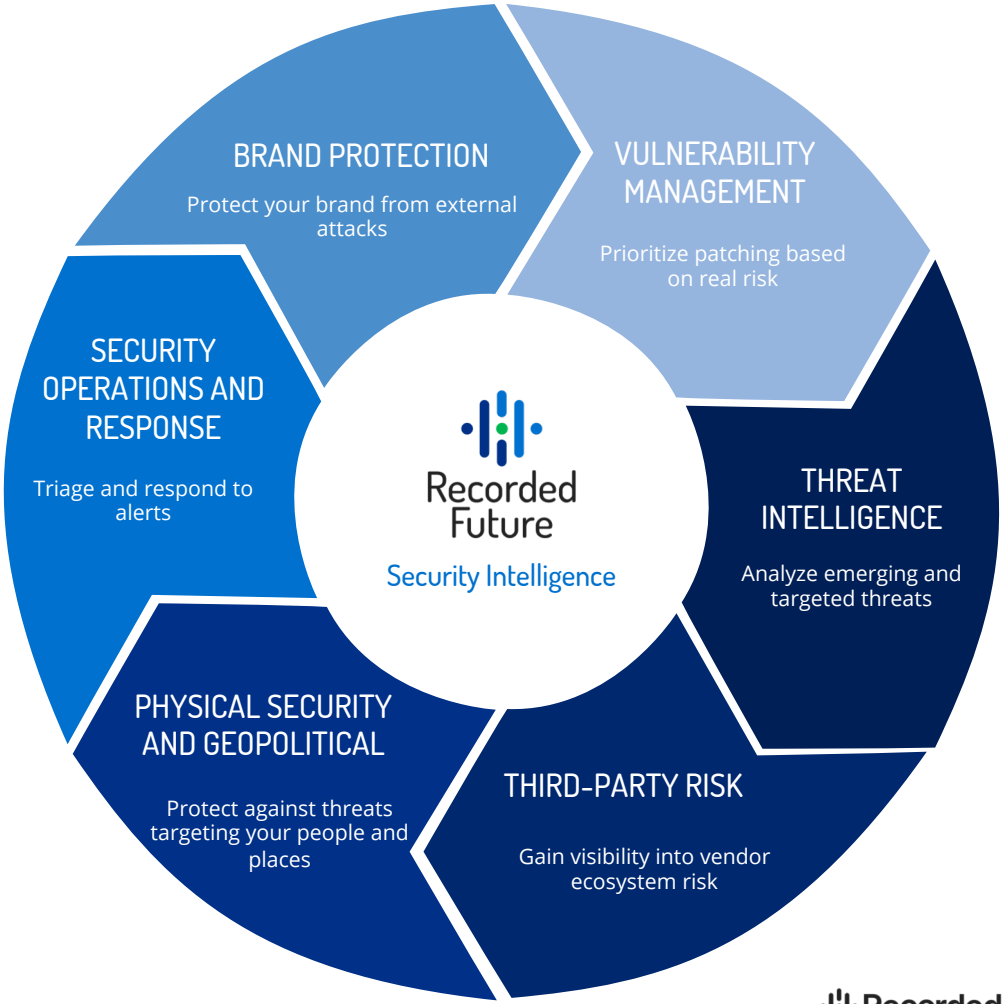
Key Takeaways

- Continuous Monitoring in conjunction with traditional assessment methods can provide the most accurate, up to date view the risks presented by partners and vendors.
- Using intelligence gathered from continuous monitoring sources, your organization can decide how often to assess tiered vendors, and what questions you need to ask those vendors.
- Combining continuous monitoring, with traditional assessment and automating as much of the process as possible can save your organization and your partners and vendors time, resources and money.



Recorded Future®

Intelligence Supercharges Security and Risk



Learn more about third-party risk:

go.recordedfuture.com/third-party-risk

Recorded Future®