RAPID7

Cybersecurity Series:

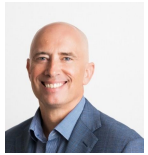
Top Cybersecurity Predictions for 2024

Agenda

- 2023 in Review, Impacts and Lessons Learnt
- Top Predictions for 2024
- Uniting Cybersecurity

Today’s Panelist

Raj Samani
Senior Vice President,
Chief scientist, Rapid7



Rob Dooley
Vice President, APAC,
Rapid7

Jason Hart
Chief Technology Officer - EMEA,
Rapid7

2023 in Review, Impacts and Lessons Learnt

Did Last Year's Prediction Materialise?:

Rapid7 2023 Predictions:

- **We will continue to 'arm the adversary as more vulnerabilities and exploits communicated by the infosec industry are weaponized by threat groups, but information sharing will also become strained as social media giants become less reliable platforms for collaboration.**

- **Security is hard and talent shortage is real. The majority of organizations will continue to do nothing to address hiring practices and nurture top talent.**

- **The disconnect between technical stakeholders and business leaders will increase in 2023.**

2024 Predictions

Prediction: Increasing risks and regulations will intensify pressure on businesses to navigate evolving demands across a complex global landscape.

The growing regulatory focus on cybersecurity and the impending consequences for executives will put into sharp focus the need to meet the regulatory requirements amidst the backdrop of an evolving threat landscape and growing attack surface. SOC teams will face higher workloads to detect/respond to and mitigate risks, which will demand quantifiable metrics to demonstrate compliance.

Key points:

- **Increased Regulatory Scrutiny Across Multiple Jurisdictions:** Executives will be more obliged to manage risk and demonstrate transparency during breaches (or suspected breaches).
- **Compliance Demands:** will pressure SOC teams to promptly demonstrate that requirements are met.
- **Urgent Threat Response:** SOC teams must swiftly detect and respond to threats to prevent data breaches and minimize damage.

Cyber Resolutions:

- **Prioritize Cyber Resilience:** Organizations should prioritize cybersecurity to ensure business continuity and protect valuable assets.
- **Define Performance Metrics:** Establish clear Key Performance Indicators (KPIs) and performance level agreements (PLAs) for SOC effectiveness.
- **Invest in Staff Well-being:** Recognize the importance of staff retention and mental health support to maintain a productive and resilient SOC.

Prediction: Expect a surge in the growth of real-time information sharing within global public-private cyber partnerships.

Anticipate an upswing in real-time information sharing among global public-private cyber partnerships, driven by the need for advanced tools in cyber risk mitigation, fostering stronger collaborations to fortify defenses against evolving threats.

Key points:

- **Advanced Tools Demand:** Real-time information sharing surges due to the demand for sophisticated tools in effective cyber risk mitigation.
- **Dynamic Collaborations:** Governments and businesses unite in focused, real-time collaborations, moving beyond historical quarterly meetings to share threat intelligence and resources.
- **Targeted Threat Response:** Real-time sharing addresses shrinking timelines, concentrating efforts to swiftly respond to emerging threats from initial vectors to final payloads.

Cyber Resolutions:

- **Proactive Partnerships:** Actively engage in dynamic partnerships, emphasizing real-time information sharing and collaborative actions beyond traditional meetings.
- **Government Collaboration:** Seek collaborations with government agencies, fostering a proactive 'information-sharing' mentality and open communication channels for collective cyber defense.
- **Real-Time Response:** Embrace a real-time sharing approach for a swift and targeted response to the evolving threat landscape through enhanced partnerships and collaboration.

Prediction: The continued use of zero-day vulnerabilities exploited by ransomware groups will compel SOCs to focus on exposure management and validation strategies.

In the evolving cybersecurity landscape, proactive SOC practices, guided by the vision of an extended SOC, center around exposure management and validation, prompting security leaders and practitioners to fortify security foundations for heightened organizational resilience.

Key points:

- **Strategic Exposure Management:** SOCs will proactively shift focus from reactive measures, prioritizing exposure management to identify and mitigate vulnerabilities before exploitation occurs.
- **Validation for Assurance:** Continuous validation practices will align security measures with evolving threats, providing assurance amidst the dynamic cyber landscape.
- **Operational Resilience:** Through proactive exposure management and continuous validation, SOCs will fortify operational resilience against emerging, sophisticated threats.

Cyber Resolutions:

- **Integrate Continuous Validation:** Embed continuous validation into security protocols, ensuring the ongoing effectiveness of defensive measures.
- **Empower SOC Teams:** Provide SOC teams with training and tools for proactive exposure management, cultivating a culture of vigilance and adaptability.
- **Collaborate on Threat Intelligence:** Establish collaborative partnerships for sharing threat intelligence, augmenting the collective capacity to anticipate and address emerging cyber threats.

Uniting Cybersecurity

Research and Resources

Research and Resources

- Presentation - Slides
- Tips to Addressing Misconfigurations and Cutting Costs - Webinar
- 2023 Mid-Year Threat Review - Report
- Rapid7 Cloud Misconfiguration Report 2022 - Report
- Executive Risk View - Dashboard
- Managed Threat Complete - Threat Package
- Cloud Risk Complete - Cloud Package
- Speaker Profiles - Social

Thank you!

Visit: rapid7.com

Contact: info@rapid7.com