RAPID7

November, 2024

The impact of the evolving Threat Landscape on the “Defender’s Dilemma”

Robin Long
Regional CTO, APAC

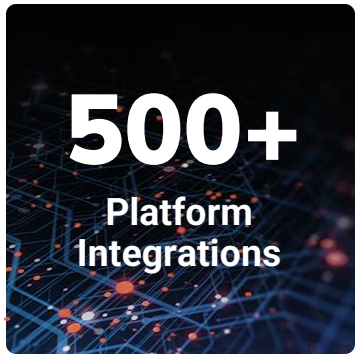
RAPID7

Best-in-Class Technology

Security Services

Research and Community

Global Ecosystem



11,500+ Customers

49% of Fortune 100
NASDAQ: RPD

Global Footprint

144 Countries

4 SOCs worldwide (24/7/365)

Leader of Innovation

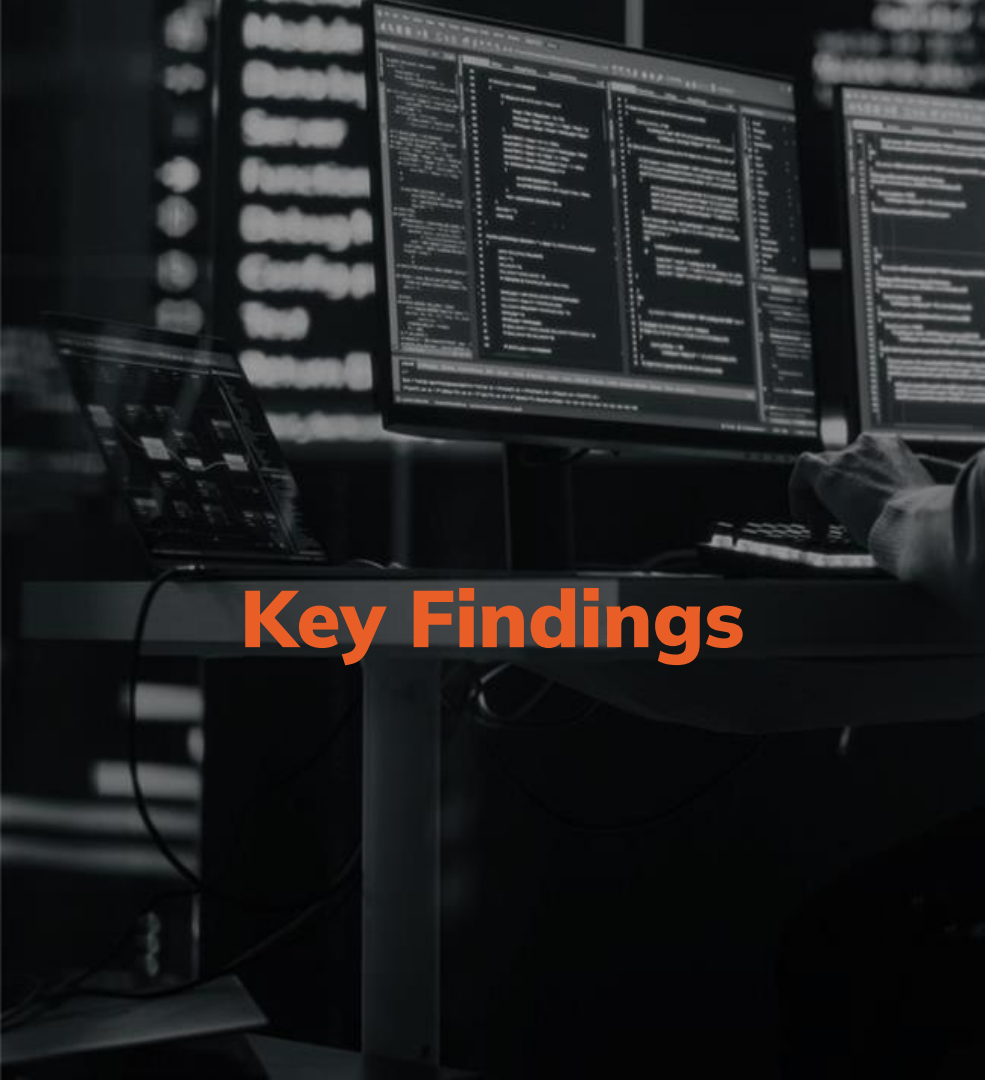
56 Patents
Open Source Communities

Rapid7 2024 Attack Intelligence Report

Rapid7's 2024 Attack Intelligence Report offers analysis and insights to help security practitioners **understand** and **anticipate** modern cyber threats.

This research is based on:

- **1,500+** curated vulnerability and exploit data points
- Analysis of **180+** advanced threat campaigns
- Thousands of tracked **ransomware incidents**, extortion communications, and dark web posts
- Insights from **trillions of security events** across Rapid7 MDR and threat analytics telemetry



Key Findings

5,600+

Ransomware incidents tracked by Rapid7 Labs in 2023 and early 2024

53%

of mass compromise events began with a zero-day attack

$1B+

2023 ransomware payouts

36%

of widespread threat CVEs affected network edge tech

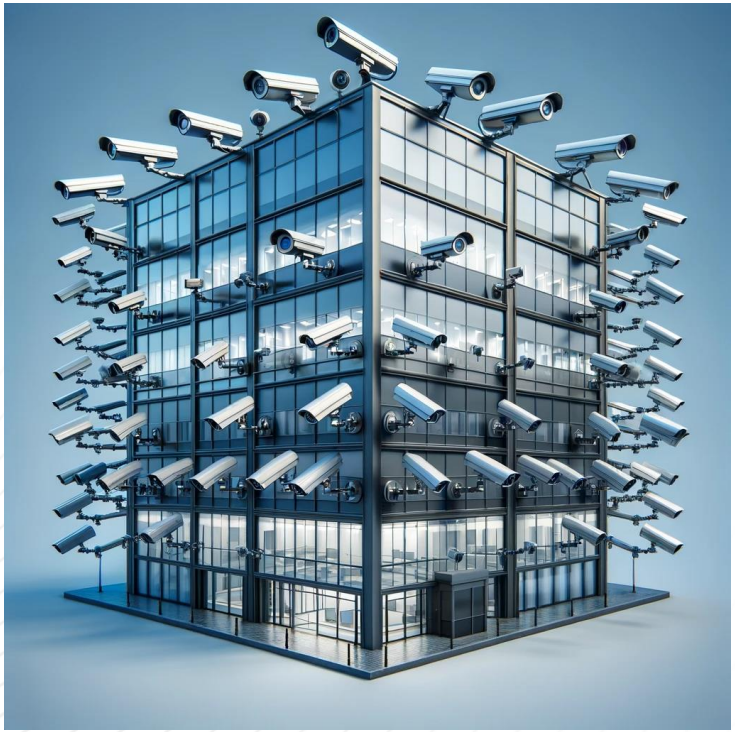
41%

Rapid7-observed incidents where victim had no MFA

1 day

Median time to known vulnerability exploitation

The Defender's Dilemma...



"Defenders have to be right every time. Attackers only need to be right once"

- Continuous Vigilance vs Opportunistic attacks
- Large and evolving attack surface
- Asymmetry of knowledge

Organisations need Visibility and Clarity over...

Internal Environment

Attack Surface

External Threat Landscape

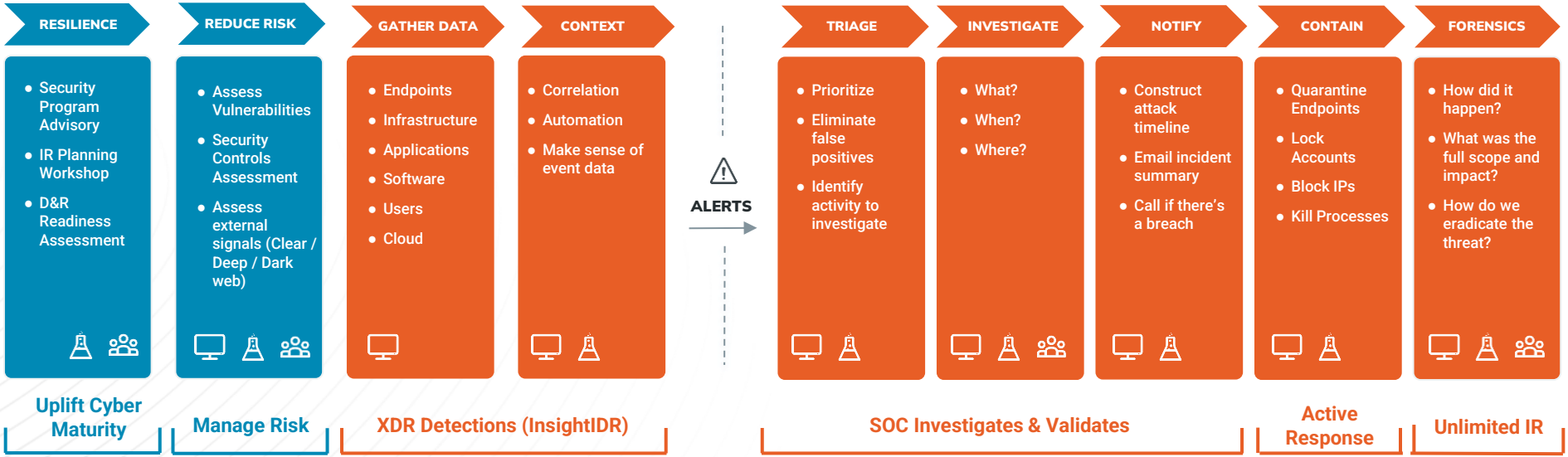

HOW DO WE DETECT AND RESPOND TO THREATS?

Functional Requirements of a Security Operations Centre

	Core SOC Operations				Expanded SOC Operations		
Process	SOC Engineering	Incident Triage & Investigation	Threat Hunting	Incident Response	Exposure Management	Threat Intelligence	Controls Validation and Testing
Technology	Security Incident and Event Monitoring (SIEM), Endpoint/Network/eXtended Detection and Response, Threat Feeds, User Entity Behaviour Analytics, Case Management, Security Orchestration, Automation and Response (SOAR)			Digital Forensics and Incident Response	Cyber Asset Attack Surface Management (CAASM, EASM)	Digital Risk Protection, Threat Intelligence Platform	Penetration testing tools, Continuous Controls Validation
People	SOC Engineers	SOC Analysts	Threat Hunters	Incident Responders	Threat Analysts	Security Engineers	Penetration testers
	Actual number of analysts depend on coverage hours, number of assets, geography, skill, risk profile, funding, automation, etc.						

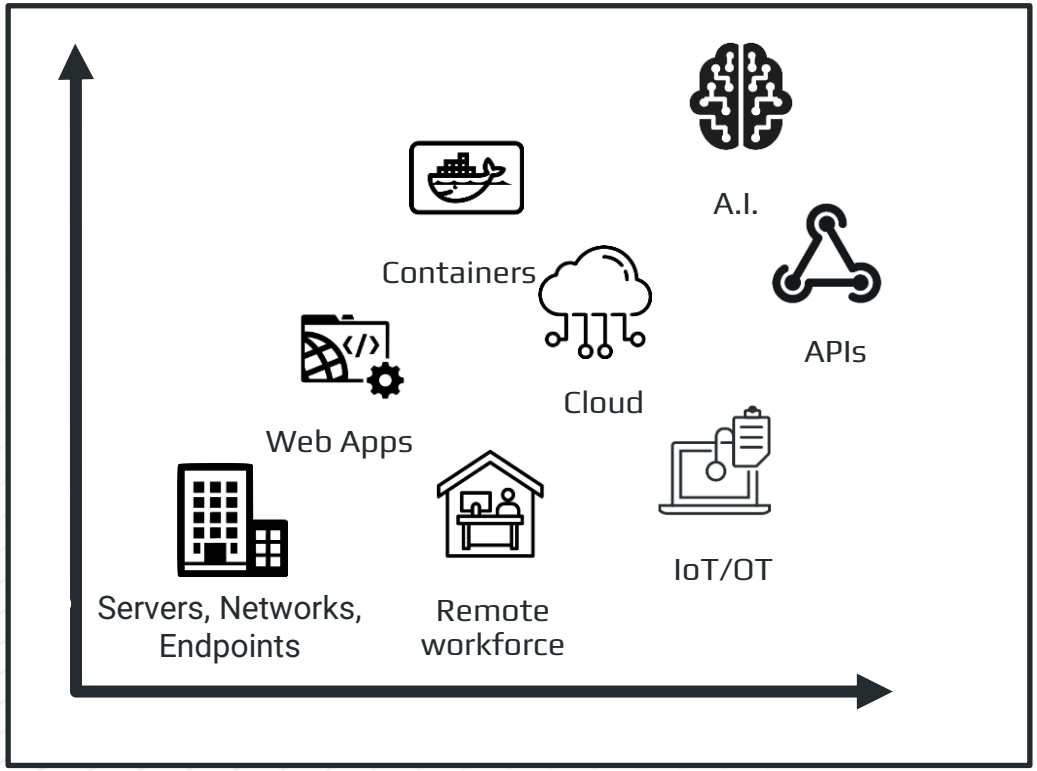
https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Delivering outcomes with Managed Detection and Response




WHAT ARE WE EXPOSING TO ATTACKERS?

The Attack Surface continues to evolve

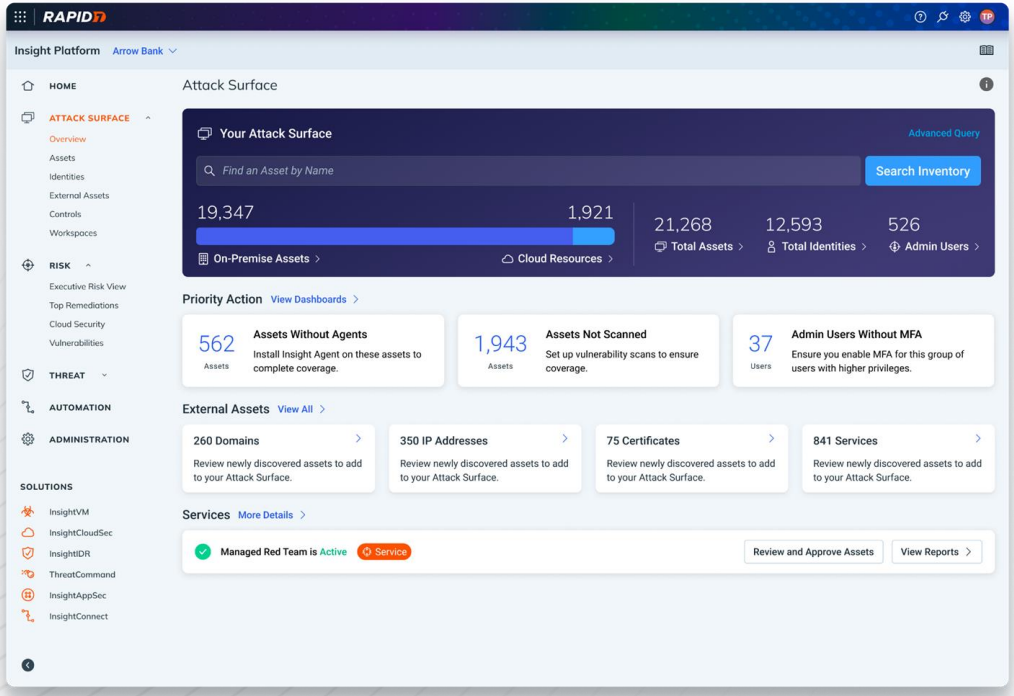


- Expanding rapidly beyond traditional infrastructure
- Security teams often play catch-up and might be bypassed in deployment
- Introduces an expanded attack surface
- Requires broader context & visibility
- Traditional scanning and detection mechanisms may not work

Examples of exposure weaknesses

- Exposed misconfigured APIs
- Exposed High Risk Ports
- Vulnerabilities in Enterprise applications and Infrastructure
- Misconfigured Cloud Applications

Understanding your evolving attack surface



- Considerations for visibility for exposure visibility especially in increasingly complex environment:
  - How quickly will you become aware of new exposures to the Internet?
  - Are there known vulnerabilities or active exploits against these exposures
  - Can these vectors lead to the compromise of internal systems?
  - How effective are your controls to prevent compromise


RAPID7
EXTENDING YOUR VIEW OF EXTERNAL THREATS
(WHO, WHAT, WHEN , WHERE, HOW?)

Categories of Cyber Threat Intelligence

https://www.crest-approved.org/wp-content/uploads/2022/04/CREST-Cyber-Threat-Intelligence.pdf

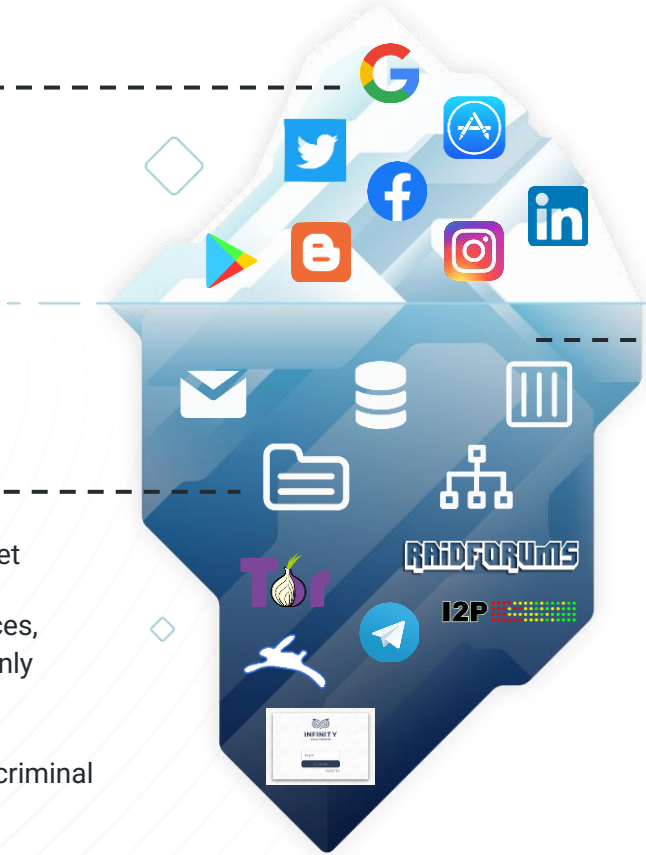
Monitoring the Clear, Deep and Dark Web

Clear Web

- Approx 5%-10% of the Internet
- Search engines
- Media, blogs, etc.

Dark Web

- Approx 0.1% of the Internet
- Anonymous, closed sources, Telegram groups, invite-only (sometimes)
- Tor, P2P, hacker forums, criminal marketplaces, C2s, etc.



Deep Web

- Approx 90-95% of the Internet
- Unindexed by search engines
- Webmail, online banking, corporate intranets, walled gardens, cloud storage, etc.

The value of Digital Risk Protection

Improving your Cyber Peripheral Vision

Pre-Breach

Attack campaign chatter

Fake profiles of Executives

Fake / Impersonation website

Fake Apps

During Breach

Post-Breach

Backdoor access

Compromised credentials

Confidential information

3rd Party Ransomware Breach

Summary

- While we can’t predict every element (Who, What, When, Where, How) of an attack, clarity and visibility can help minimise risk in the following ways:
    - Consider all of the elements required of Extended SOC Operations and how these can be best delivered either through internal or external resources
    - Visibility across our External Attack Surface can reduce the risk of exposures being exploited
    - Visibility across the Clear, Deep and Dark Web can help raise our awareness of potential weaknesses or exposed sensitive data