

RAPID7

Oktober 2023

Managed SOC - Was Sie Ihren Anbieter unbedingt fragen sollten

Fabian Guter

Threat & XDR Sales Specialist

RAPID7

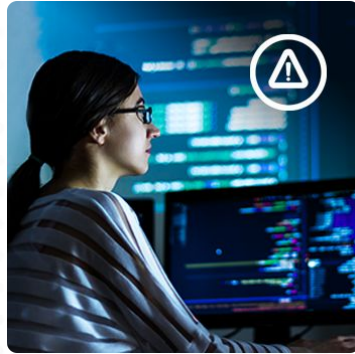
Best-in-Class Technology



**11,000+
Customers**

43% of Fortune 500
NASDAQ: RPD

Security Services



**Global
Footprint**

144 Countries
21 Offices

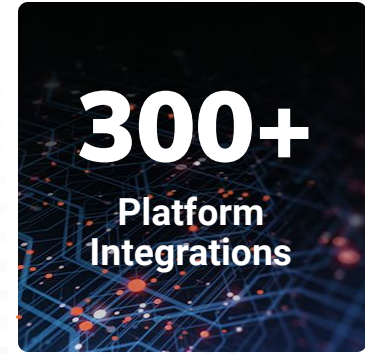
Research and Community



**Leader of
Innovation**

56 Patents
Open Source Communities

Global Ecosystem



Why 1,450+ customers trust Rapid7 MDR



Holistic Security Approach

Combine Detection, Response, and Unlimited Risk Management to have a complete approach to MDR.



Unlimited Data Ingestion

We won't limit our ability to reach your security outcomes due to data costs or pass them on to you.



Strategic Guidance

Advance your program and strengthen your security posture with a team of experts guiding your program.



Transparent Partnership

You see what we see. We've got nothing to hide.



Unlimited Incident Response

We don't stop when there's a major breach. We take detection and response completely end-to-end.



Access to Experts

Consider us an extension of your team. We're here to help you secure your environment, not just respond to alerts.

Sechs Fragen an Ihren SOC/MDR Service



Wie sieht das Onboarding aus, wie schnell bin ich “geschützt” und was muss ich selbst dazu beitragen?

Easy onboarding and rapid time to value

Kickoff Call with the Onboarding Success Mgr

- Handoff from Sales to Onboarding Success Manager
- Refine Onboarding Success Plan
- Schedules Services

CUSTOMER ACTIONS:

- Provide input into Success Plan
- Work with Onboarding Success Mgr on scheduling services

Deployment Services

- Verify anything configured prior is working properly
- Implement configuration of (or review existing) InsightIDR, the InsightConnect Orchestrator, and Active Response
- Implement Hosted Console configuration (or review existing IVM console & determine best migration process to execute)

CUSTOMER ACTIONS:

- Schedule Tech & Tuning Call

IR Planning & Advisory

- IR Planning & Process Foundations Workshop
- D&R Readiness Assessment*

RAPID7'S ACTIONS:

- Provide Advisory Security Expertise

CUSTOMER ACTIONS:

- Have IR Planning Templates prepared for review
- Coordinate internal IR stakeholders for discussions

ONBOARDING WELCOME
1-3 biz days after purchase

SERVICE KICKOFF
Within 1 week of Kickoff

PRODUCT DEPLOYMENT
Within 1-2 weeks of SLC

VERIFICATION
Once deployment is complete

ADVISORY SERVICE
During deployment process

STEADY STATE
After verification

Service Launch Call

- Verify at least (1) agent is deployed
- Enable your team on how to communicate with MDR

RAPID7'S ACTIONS:

- Begin 24x7x365 monitoring on all assets with agents
- Alert investigation and incident validation
- False positive elimination

CUSTOMER ACTIONS:

- Begin self-deploying more agents
- Prepare for the Deployment Consultation call and complete prerequisite steps

Tech & Tuning Call

- Verifies environment in InsightIDR
- Performs Tech and Tuning of InsightIDR & InsightVM

RAPID7'S ACTIONS:

- Customer Advisor (CA) Assignment*
- Moved into 'Steady State'

Onboarding Complete!

- Continue 24x7x365 monitoring
- Security Posture Assessment
- Hypothesis-Driven Threat Hunts
- Ongoing Reporting
- Monthly Meetings with CA*

* Included with MTC Advanced package



Welche eigenen Ressourcen und Expertise muss ich bereitstellen, was wird von meinem Team erwartet?

Customers extend their team with D&R experts

95%+

3-Year Analyst Retention Rate

3

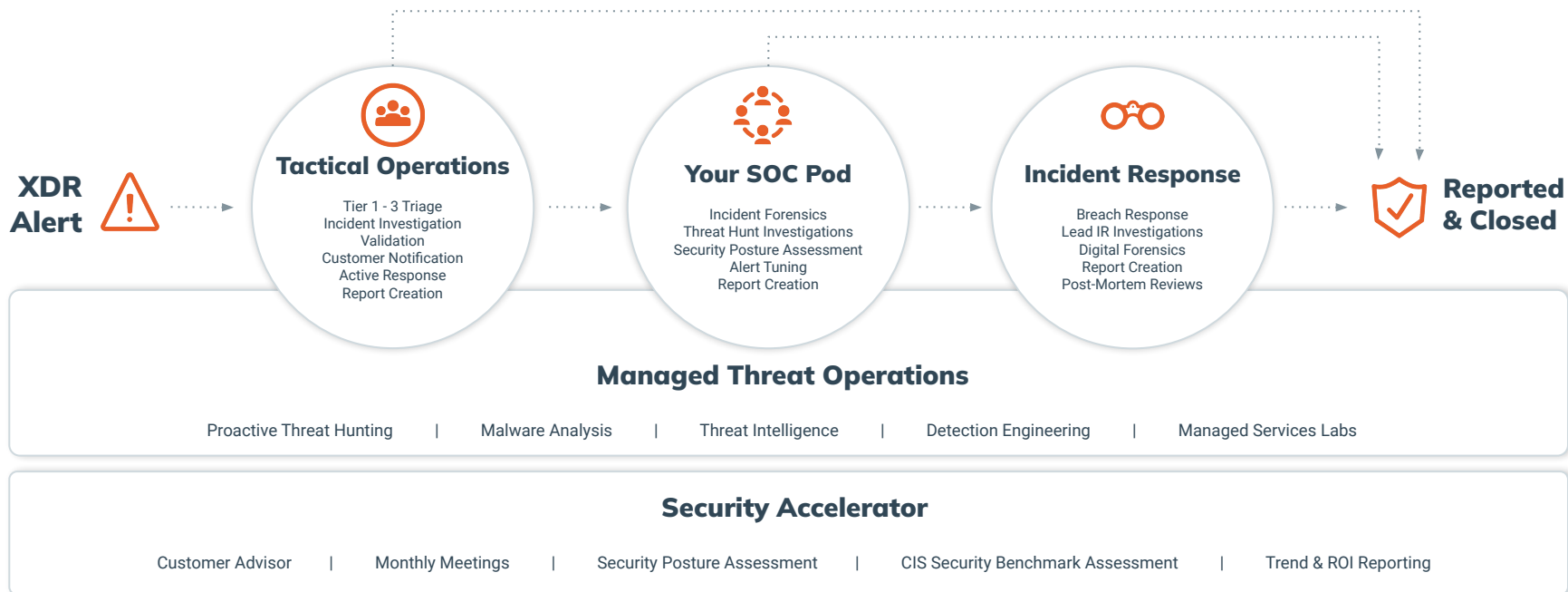
Global SOCs (FTS coverage)

7-10

Analysts per SOC pod

3.7T

Weekly Events Analyzed





**Können Sie mich bei der Prävention von
Angriffen unterstützen?**

Proactive Security

Mitigate Risk and Contain Impact.



Reduce Your Risk Exposure

Unlimited Vulnerability Scanning helps to proactively identify areas of risk.



Know If You're Compromised

Security Posture Assessment shows weaknesses and avenues of improvement.



See Your Entire Environment

Unlimited Data Ingestion = No Data Fees.



Find Unknown Threats

Hypothesis-Driven Threat Hunting finds stealthy attackers in your environment.



Be Prepared For the Worst

IR Planning And Readiness workshops help you define your plan of action.



Meet Compliance Regulations

13 Months Data Retention by default



Wenn Sie einen Angriff feststellen, werden Sie selbständig Maßnahmen einleiten, um Schaden zu begrenzen?

Responsive Security

Stop Attackers In Their Tracks.



Gain Always-On Coverage

24x7 SOC experts with XDR visibility.



Feel Safer With Threat Intel

Curated library of detections from our community, research, and experience.



Stop Attackers In Their Tracks

Active Response contains threats on your behalf. Attack at 3AM or 3PM? We got you.



Be Confident No Matter What

We respond to every incident, minor or major. No IR retainer, time limits, or warranty claims.



Send Us Data, We'll Do The Rest

Unlimited Data Ingestion means we're not limited for how we can detect threats.



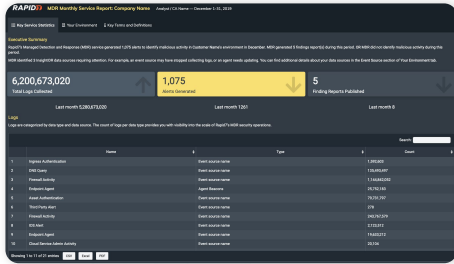
Get Answers, Not Notifications

Exhaustive reports provide everything you need to know (and more) to remediate.

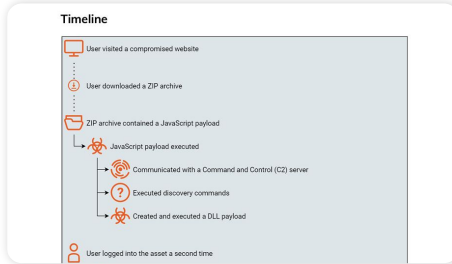


Im Ernstfall, was können wir an Unterstützung erwarten bei der Kommunikation mit internen und externen Interessenvertretern, z.B. Versicherungen, Datenschutzbehörden, Strafverfolgung, ...?

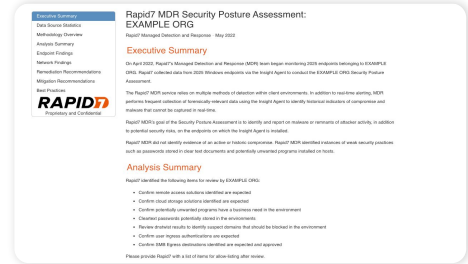
Practitioner-first approach that delivers answers



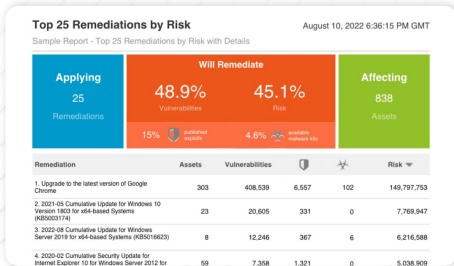
Monthly Service Report



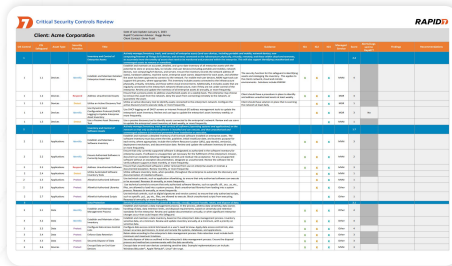
Incident Report



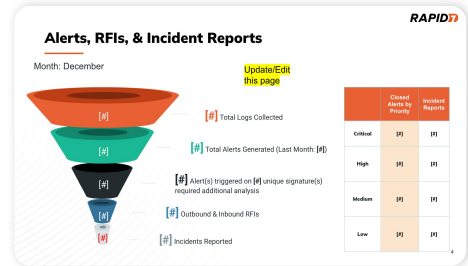
Security Posture Assessment



Top 25 Remediations by Risk



Critical Controls Assessment



Executive & Trend Reports



Was genau bedeutet “Incident Response”, in welchem Umfang und für welche Dauer?

VALUE ADD

Breach Response

MDR experts pivot to DFIR using InsightIDR and Velociraptor:

- Full scope and remediation plan
- Examine any data source
- Continuous updates
- Post-Mortem Report

Examples of Integrated DFIR:

- Multiple endpoints affected
- Lateral movement
- Data exfiltration
- Staging

Table of Contents:

Executive Summary	5
Incident Synopsis	5
Scope	5
Constraints	5
Findings Overview	6
Key Findings	6
Remediation Recommendations	7
Mitigation Recommendations	8
Incident Details	10
Intrusion on Citrix Gateway	10
Pivoting into the Network	15
Lateral Spread	16
Overall Timeline	32
Appendix A: Incident Scope Overview	39
Rules of Investigation and Assumptions	39
Scope of Resources	39
Appendix B: Affected Assets	40
Appendix C: Indicators of Compromise	41
Appendix D: Group Policy Administrative Templates and Related Files	63
Appendix E: C2 Connections	66



Velociraptor

 Confidential and Proprietary

XDR detects threats others miss

We notify you of the investigation

Active Response stops attacks

Incident Report gives the full story

Hunt across all customers

DFIR / Breach Response

If a live attacker is in the environment, MDR pivots to breach response to help you when you need it the most.

Your **complete** approach to MDR

Mitigate Risk and Contain Impact

- ✓ Understand your environment
- ✓ Baselining
- ✓ Unlimited Vulnerability Scanning
- ✓ Threat Hunting
- ✓ Security Posture Assessment
- ✓ IR Planning Workshop
- ✓ D&R Readiness Assessment*
- ✓ 13 Months Data Retention

READINESS

RESULTS



Stop Attackers In Their Tracks

- ✓ 24x7x365 Elite SOC Monitoring
- ✓ XDR Coverage
- ✓ Unlimited Incident Response
- ✓ Threat Intelligence Engine
- ✓ Forensic Investigations & Reports
- ✓ Active Response
- ✓ Unlimited Data Ingestion

RESPONSIVENESS

REMEDIATION

RESULTS

Build A Strong, Resilient Program

- | | |
|--------------------------------------|--|
| ✓ Transparency via Technology Access | ✓ Strategic Security Program Advisory* |
| ✓ Actionable, strategic remediations | ✓ Monthly Security Posture Reviews* |
| ✓ Detailed monthly reporting | ✓ Critical Security Controls Assessment* |
| ✓ Connect with Rapid7's Peer Network | ✓ Executive Trend Report & Readout* |

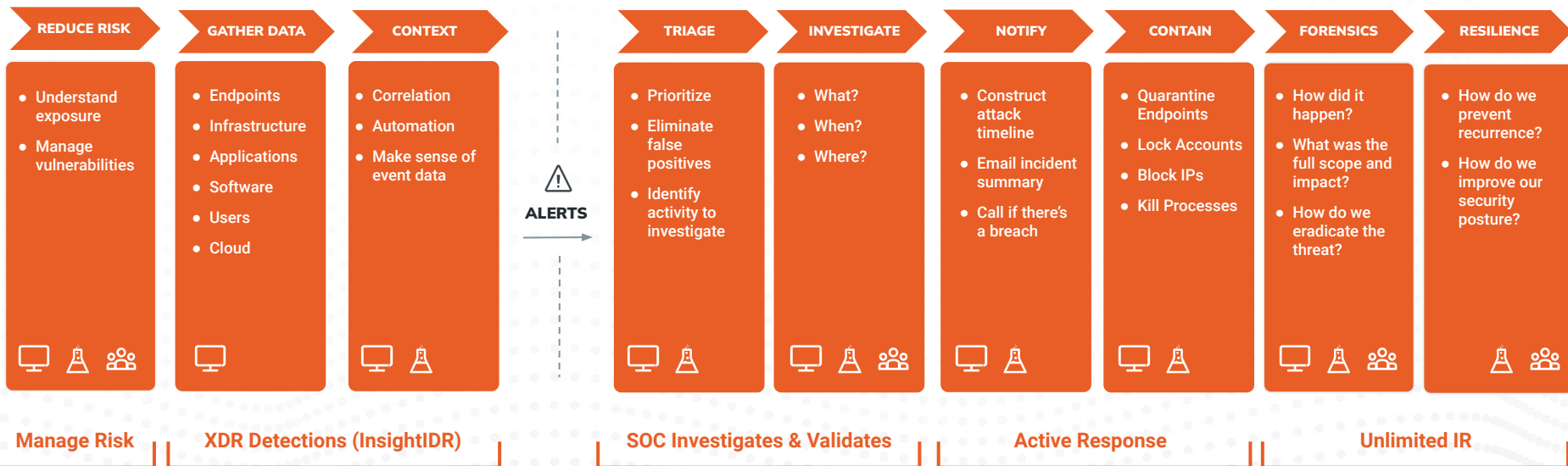
READINESS

REMEDIATION

RESULTS

* Available with MTC Advanced package

Rapid7 takes detection and response from end to end without limits



Rapid7 handles EVERY incident, no matter how large or complex. With us, there is no line. We're there for you when you need it.

Stand: 7-540

Vielen Dank!

Web: <https://www.rapid7.com/solutions/unified-mdr-xdr-vm/>

