Rapid7 & Payconiq Onboarding Kickoff

Katja Dumon, Account Executitve
Berry Rijnbeek, Sales Engineer
Rik Crommentuijn, Customer Succes Manager

Agenda

- Your Purchase
- Your Rapid7 Account Team
- Onboarding Process & Timeline
- Overview of MTC
  - Managed Service Enablement
  - Agent Deployment
  - Resources
- Your Onboarding Journey
- Next Steps

Thank You for Your Purchase of Managed Threat Complete

MTC Advance

License Count: 260 + 240 assets

Renewal Date: 1/4/2025

Your Rapid7 Account Team

Your Rapid7 Account Team

Katja Dumon
Account Executive
katja_dumon@rapid7.com

Rik Crommentuijn
Customer Success Manager
rik_crommentuijn@rapid7.com

Berry Rijnbeek
Sales Engineer
Berry_rijnbeek@rapid7.com

Account Executive

- Partners to understand your desired outcomes and align to Rapid7 solutions
- Facilitates expansions

Customer Success Manager

- Internal advocate focused on building partnership and maximizing customer investment; facilitates renewal
- Understands your desired outcomes and aligns appropriate resources to drive progress or overcome challenges
- Facilitates value and adoption by reviewing product/service capabilities and communicating updates

Sales Engineer

- Rapid7 technical product expert who validates initial capabilities
- Provides bridge to implementation consultants and can provide guidance and advice post-onboarding

Your Rapid7 Account Team - Technical Resources

Name: TBC
Title
Name@rapir7.com

Name: Petar Gazenov
Customer Advisor
petar_gazenov@rapid7.com

Product Consultant

- Onboarding resources who provide the technical expertise necessary for solution implementation
- Delivers implementation of technical requirements

Customer Advisor

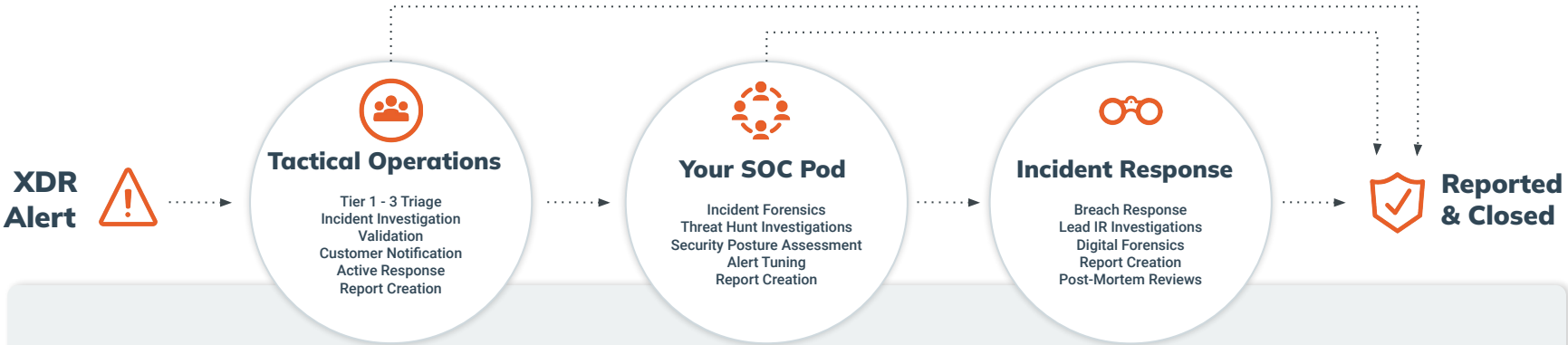
- Serves as extension of security team for your managed service
- Contextualizes SOC findings with transparency
- Provides recommendations based on industry trends and security needs

Customers extend their team with D&R experts

95%+
3-Year Analyst Retention Rate

4
Global SOCs (FTS coverage)

7-10
Analysts per SOC pod



Managed Threat Operations

Proactive Threat Hunting | Malware Analysis | Threat Intelligence | Detection Engineering | Managed Services Labs

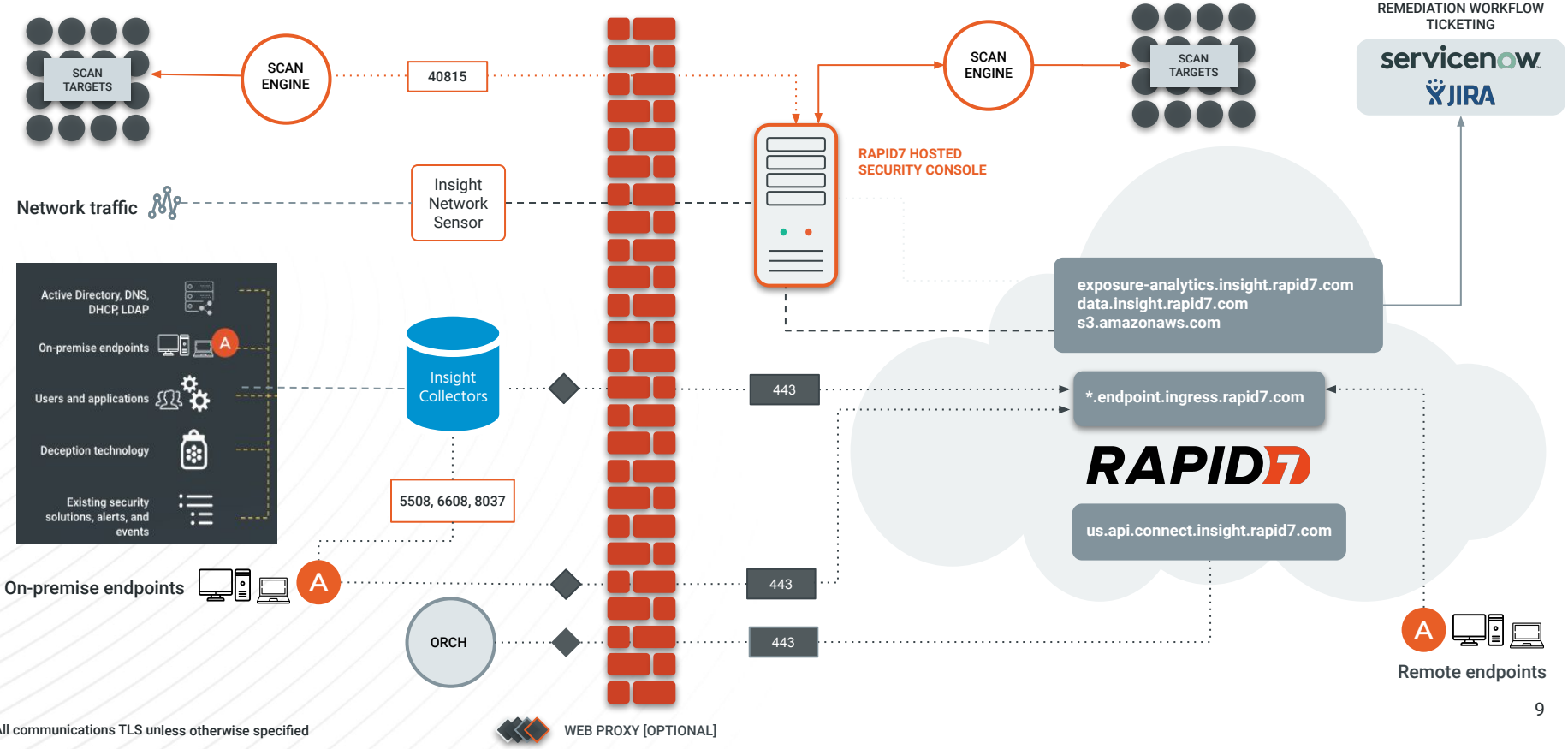
Security Accelerator

Customer Advisor | Monthly Meetings | Security Posture Assessment | CIS Security Benchmark Assessment | Trend & ROI Reporting

MTC Technology Overview

Managed Threat Complete Architecture

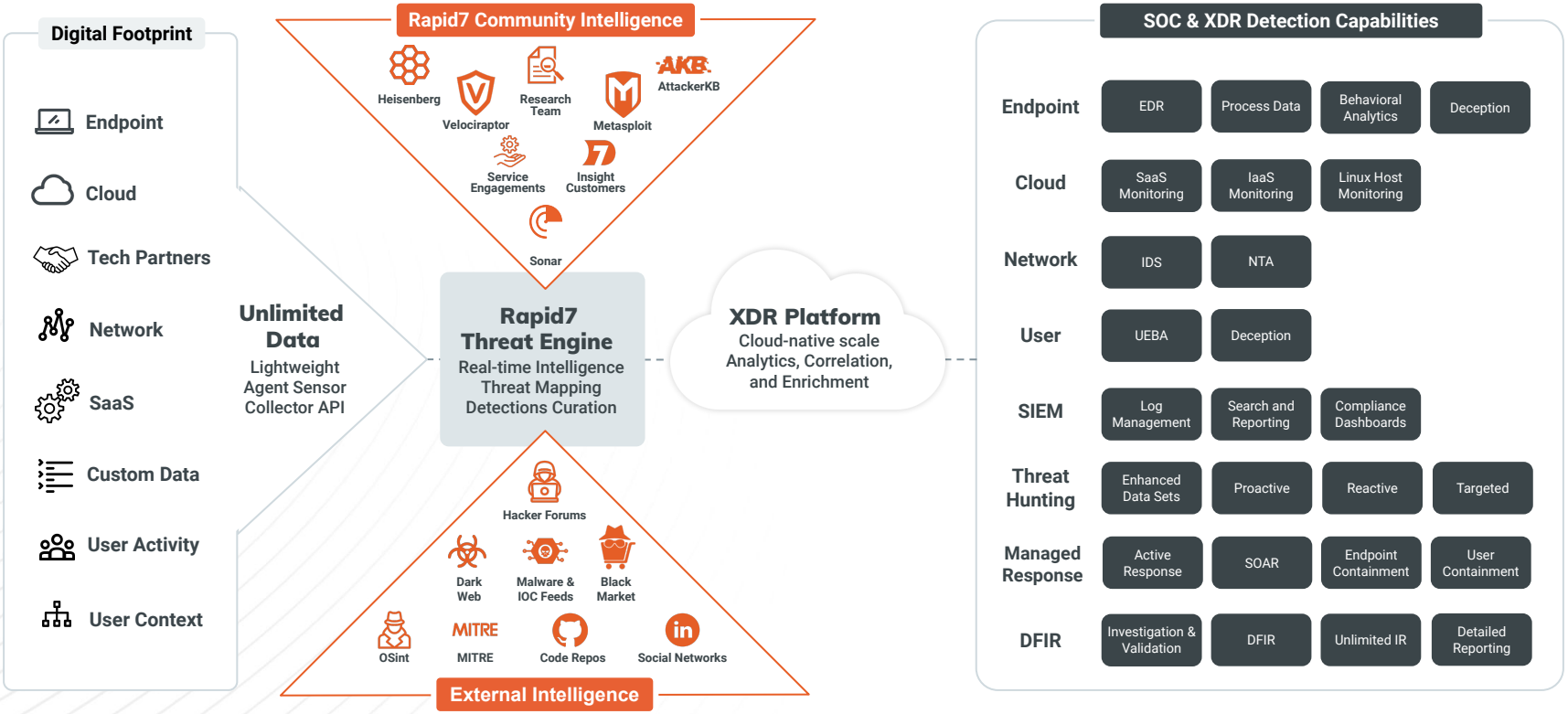
Frankfurt
AWS Region: Europe - Gemany



RESPONSIVE

Stop attackers in their tracks

RAPID7 insightIDR



insightVM

KEY OUTCOMES:

- ✓ Discover and remediate high risk vulnerabilities first
- ✓ Track and collaborate with peers to progress remediation
- ✓ Ensure policy and regulatory compliance
- ✓ Leverage expert research and community insights
- ✓ Increase risk coverage in a fast changing environment

Improve Efficiency and Effectiveness with InsightConnect

Instant Automations

Native Cloud Integrations

Automation Discovery

Quick Actions

Vast Library of Integrations & Workflows

Pre-Built Workflows

Pre-Built Plugins

Visual Workflow Builder

Enhanced Analyst Productivity

Chat Driven Automations

Response Queues

IDR & IVM Automation Triggers

Integrated Community Of Experts

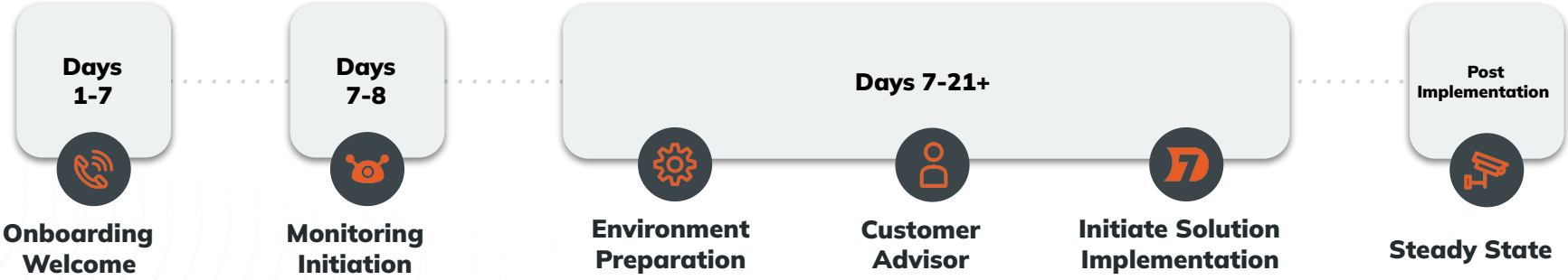
Extension Library

Discuss Forum

Workflow Contributions

Onboarding Process & Timeline

Onboarding for Success.



Rapid7 Actions

- Introduction to Rapid7 Team
- Refine Onboarding Success Plan
- Schedules Services

Customer Actions

- Deploy initial agent
- Provide input into Success Plan

Rapid7 Actions

- Customer Advisor (CA) Assignment
- Begin 24x7x365 monitoring on all assets with agents deployed
- Alert investigation and incident validation
- False positive elimination

Customer Actions

- Begin self-deploying more agents
- Watch Service Launch Video
- IR Planning Workshop

Customer Actions

- Read the MTC Deployment Handbook
- Provision servers for Collector(s), Scan Engine(s), Orchestrator
- Complete firewall rules
- Establish service account credentials
- Change control

Rapid7 Actions

- Customer Advisor Communication Setup
  - **Essentials**: Customer Advisor Pool via Customer Portal
  - **Advanced & Ultimate**: Assigned Customer Advisor
- **Advanced and Ultimate:** Customer Advisor establishes cadence with customer for remaining tasks and steady state communications

Joint Actions*

- Verify everything configured prior is following best practices
- 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)

Rapid7 Actions

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

*Duration of solution implementation is dependent upon purchase and session timing.

Agent Deployment and Monitoring Start:

- All we need is one agent deployed and some info!
- Rapid7 Insight Agent Deployment Instructions
- Allow listing the Rapid7 agent in your Endpoint Protection Platform
- We Need Some Info:
  - Main External Domain
  - 3 points of contacts and their emails and/or cell phones
  - Your Security Email Distro(optional)
  - Expected Asset Count (if different from licensed)

You are moments away from being monitored...

Onboarding Plan: Pre-Implementation Prep

- Next we are doing pre-implementation prep. Proper pre-implementation prep ensure your Product Consultant can be focused on advanced configuration, enablement and troubleshooting.
  - Requirement: Read the MTC Deployment Handbook
  - Please track your progress. Progress Tracker
    This sheet will be critical information for your Product Security Consultant during your scheduled implementation time. Between now and that time, your SE is an excellent resource to ask technical questions.

Important info for you:

- **HOSTED INSIGHTVM CONSOLE IP: 35.156.20.217**
- **HOSTED INSIGHTVM CONSOLE URL: https://helping-ghoul.mtc.rapid7.com**

Service Launch Video:

Service Launch Video

- The Rapid7 SOC will start monitoring any assets that go into implementation after 24 hours of this call.
- We recommend that you watch our Service Launch Video so you can understand what the benefits are.
  - Slide Deck

Key Takeaways

- Rapid7 Agent best practices
- Tiered Alert Response Explanation
- How to effectively communicate with Rapid7
- Review of Detections
- Deception Technology Overview
- Active Response Automated Containment
- How we use Logs in Detections
- Reporting

How to Engage with your Managed Service:

- Customer Advisor communication will be through the portal or scheduled cadence sessions
- For action related requests, use the services portal and create a managed case
- If you are multi-org and do not have the managed portal, email mdr@rapid7.com
- For product related break/fix help, use the services portal and create a support case
- If you believe that you are breached, you can contact our emergency hotline:

  US: +1 844-777-7637
  UK: +44 800-088-5859
  SG: +65 800-852-3321
  AU: +61 2-4734-7032

- SOC Outbound Phone Number(good one to save): 617-906-7121

Additional Resources:

Training:

- Monthly InsightIDR Workshop
- Monthly Insight Agent Kickstart Workshop
- MTC IR Planning Video

Other Resources

- Product Status Notifications - subscribe for notifications about product outages
- Release Notes - reference for all product update information
- Emergent Threat Blog Series - subscribe for updates to the latest threats we're monitoring
- Rapid7 Forum - connect with other customers using Rapid7's products & services
- Rapid7 Extensions Library - find all of our integrations, plugins and workflows
- Rapid7's Blog - cybersecurity resource with latest vulnerability news

Solution Implementation Schedule

Purchased Solution: MTC Advanced

MTC Solution Component	Scheduled Date	Start Time	Duration	Assigned Security Consultant
MDR Session 1			1 hour	
IVM			1 hour	
MDR Session 2			1 hour	
Active Response (ICON)			1 hour	

Next Steps:

Your CSM will schedule a regular cadence with you.

Scheduling your Solution Implementation Sessions

Check for scheduling links from CSM

Continue Agent Deployment & Requirements to be ready for implementation sessions.

Collector, Service accounts, etc

Monitoring within 24 hours

Today's deployed assets will be in monitoring. As your start your implementation engagements, more assets will be put into monitoring covering more of your environment.

provide the names, emails, and phone numbers

primary and secondary contacts or distribution lists who should be reached out to in the case of a security incident.

Thank you.

Questions along the way? Email me at rik_crommentuijn@rapid7.com