



# RSM Defense Overview

Managed Threat Detection and Response



# Elevating managed security

RSM

**DEFENSE**

## ALWAYS ON

24x7 security analysts monitoring our clients' environments for suspicious and confirmed threats

## FOREVER VIGILANT

Leveraging automation workflows, reducing MTTD and dwell time for our clients to speed in faster response and recovery

## INFORMED RESPONSE

Threat intelligence is integrated into everything we do, aids in prioritizing risks, and determining the correct course of action

## CAPABILITIES



### Security event monitoring

Real-time security monitoring of client environments, correlating events, and analyzing potential threats leveraging our SaaS XDR Service



### Attack surface reduction

Fully managed vulnerability capabilities include continuous scanning, file, and configuration monitoring, false positive analysis, and detailed remediation actions.



### Threat intelligence

Fully integrated intelligence sources help influence the decision-making process for our analysts.



### Network Traffic Analyses

Collecting NetFlow to provide additional intelligence in threat investigations



### Automated response

Leveraging automated playbooks, we can perform predefined scripted remediation activities



### Endpoint security

Identifying risks, behaviors, and anomalies affecting your endpoints. Continuous hunting, tuning, and informed response.



### IoT/device monitoring

Providing threat monitoring of clients ICS environments utilizing a lightweight collector meant for plant and healthcare environments

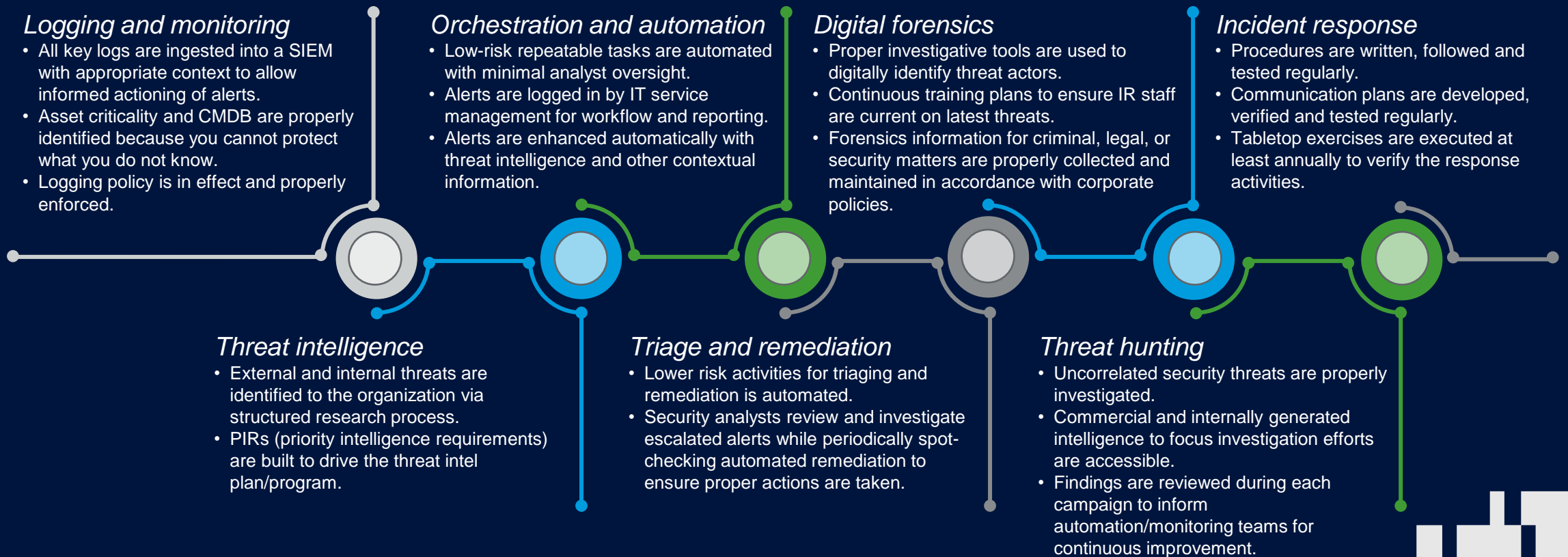


### Brand safeguarding

Monitoring cybersquatting activity and protecting your domain name from typo-squatting to safeguard your reputation

# Security monitoring and response

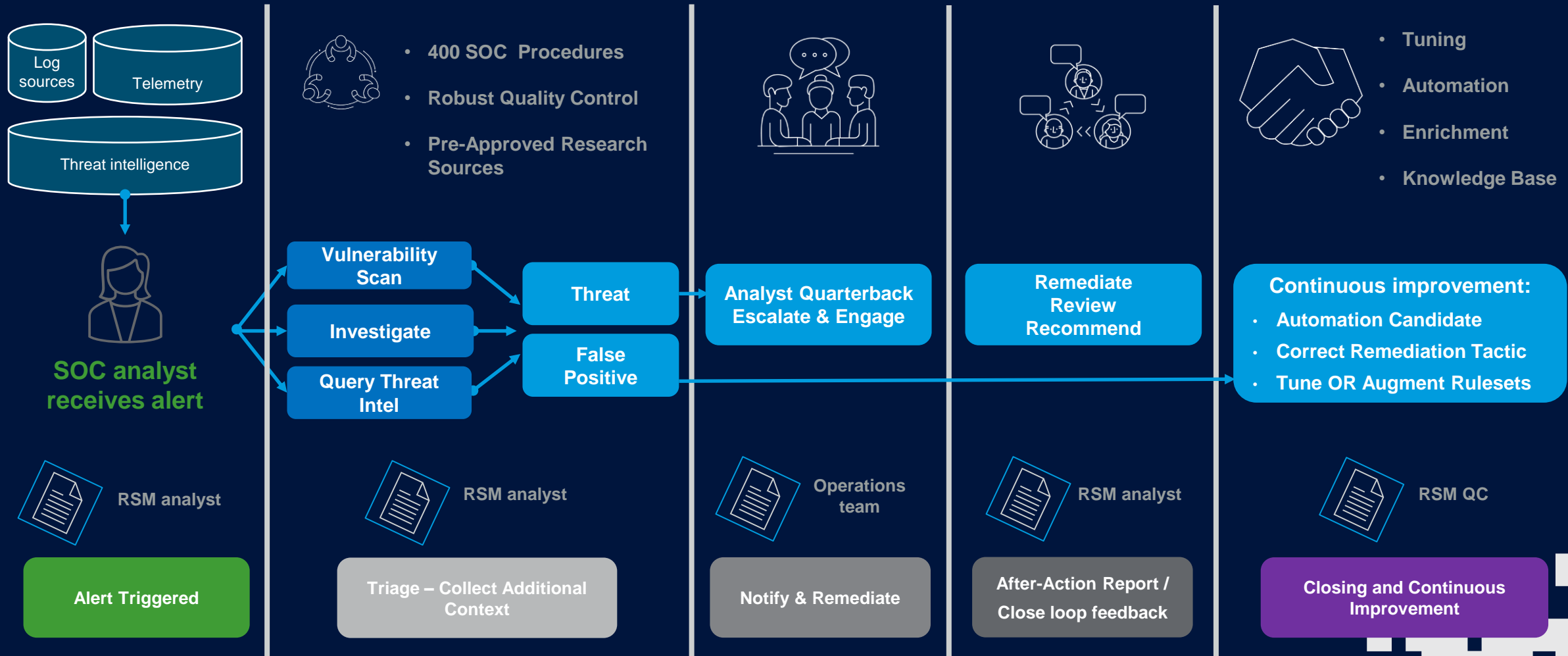
Innovative **security monitoring and response** enables organizations to effectively and efficiently respond to incidents through orchestration and automation. It also allows the organization to transform reactive processes into proactive ones by integrating threat hunting and intelligence.





# Day In The Life | Threat detection

## RSM SOC – Incident Alert & Response Procedure



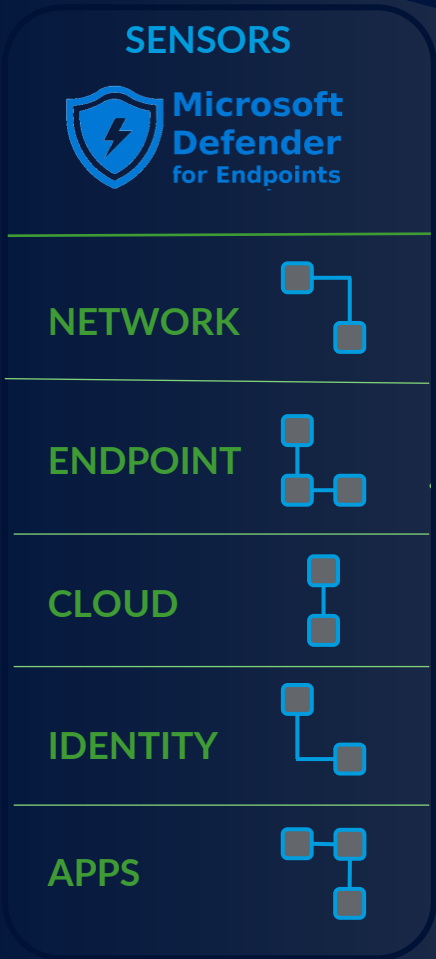
# RSM Defense Tech Stack



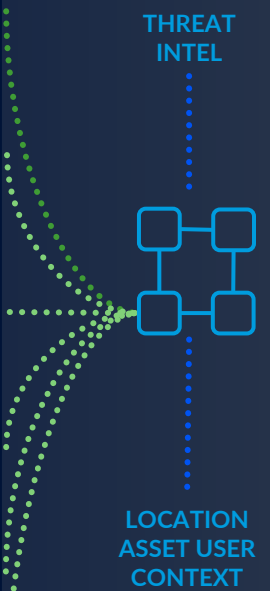
RSM  
DEFENSE

YOUR  
TOOLS

Entire Enterprise Attack  
Surface Collection



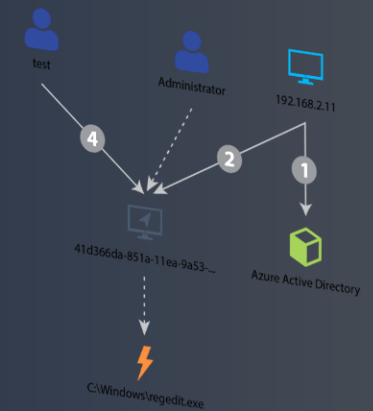
Normalized,  
Enriched Data



Multi Method  
Detections



ML-Based Incident  
Correlation



Investigation & Intelligent  
Response



Sentinel

servicenow  
IT / Security Service  
Management



# Fully managed NG-XDR service offering



## Extended Detection & Response

- 24x7 Security Operations
- Threat Hunting & Tuning
- Incident / Case Handling
- Mature Documented Procedures
- Custom Threat Intelligence Subscriptions

## Network Detection & Response

- Network Traffic Analyses
- Deep Packet Inspection / Blocking
- Behavior Analysis / Certificate Inspection
- SOAR Automation – Drop, Disable, Contain

## Configuration Monitoring

- Privacy Framework
- Security Framework



## Vulnerability Management

- Weekly scanning / Monthly Reporting
- Endpoint, Network, Cloud Visibility
- Measurable Program Results
- Custom Remediation Options

## Endpoint Detection & Response

- Fully managed EDR or BYO
- Signature & Behavior Detection
- SOAR Automation – Drop, Disable, Contain

## Training & Phishing

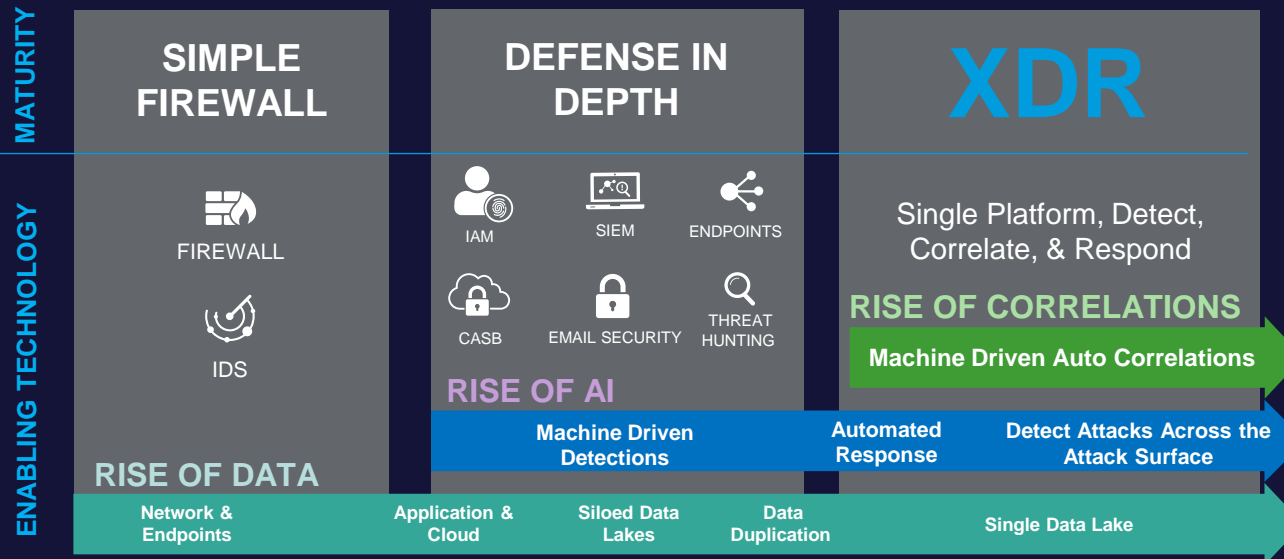
- KnowBe4 Platform
- Fully Customized
- Measurable Program Results

# XDR Service



Extended Detection & Response (XDR), All-in-One Security Operations services.

Turnkey detection and response service to ingest, enrich, contextualize, hunt, and respond with 100% threat visibility. Block hot and fast attacks. Detect slow burn attacks. Respond with decisive actions 24x7x365.




## Outcomes

- Improve incident decision support for security operators with prescriptive remediation actions
- Reduce Mean Time to Respond and Recover with native and 3rd-party responses
- Automate uniform remediation & recovery across the organization



# Service Matrix

## Level of Protection



	Vulnerability Scanning	Endpoint Detection & Response	RSM Defense Foundations	RSM Defense MXDR
24x7x365 SOC		✓	✓	✓
Asset Risk Identification	✓	✓	✓	✓
Endpoint & Network Vulnerability Scanning	✓			✓
Threat Intelligence Enrichment	✓	✓	✓	✓
Monthly Industry Focused Threat Intelligence Newsletter				✓
Realtime DNS Threat Protection			✓ <sup>1</sup>	✓ <sup>1</sup>
Full Function EDR Agent Included		✓	✓ <sup>2</sup>	✓ <sup>2</sup>
Email & Identity Protection			✓ <sup>3</sup>	✓
Signature and Behavior Detection		✓	✓	✓
Autonomous Response		✓	✓	✓
Threat Hunting Automation by Senior Analysts				✓
Incident/Case Handling		✓	✓	✓
Client Portal Access		✓	✓	✓
Access to 24/7/365 SOC Hotline	✓	✓	✓	✓
Static Log Collection(Sensor and API Integrations) <sup>4</sup>				✓
RSM Defense Monthly Newsletter	✓	✓	✓	✓

<sup>1</sup> RSM defense-provided agent or client-provided

<sup>2</sup> Eligible for BYOEDR or RSM Defense provided agent

<sup>3</sup> Domain Controllers will receive a Log Collection sensor in hybrid environments

<sup>4</sup> Log sources (API, syslog, custom) are all ingestion based. Fees may vary on a month-to-month basis