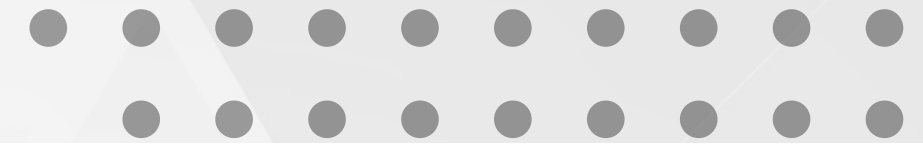


# UNLOCKING THE VALUE

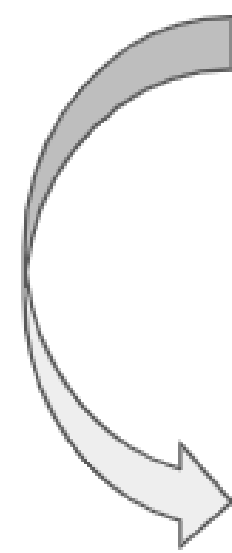
---

OF YOUR SECURITY INVESTMENTS





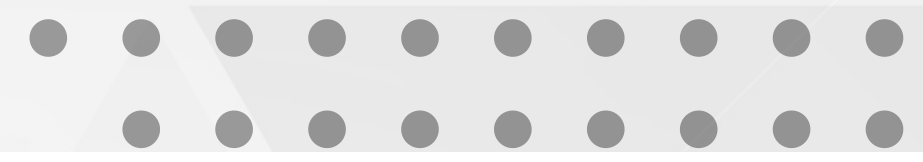
# The key to unlocking value from Security solutions



**1** **What Does it do?**  
The user needs to understand what the desired solution is designed to and AND not do

**2** **What do I need it for?**  
Based on the function of the solution what do I need it to do to support my business

**3** **What are my workflows?**  
What are my processes and workflows and how can I integrate / configure the solution to fit designed workflows



# The EDR example



## What does it do

Edr is designed to capture threat telemetry from different angles and correlate the data to give indications of an attack in progress - It enables proactive threat hunting, so you can find and stop advanced attacks before they cause damage or data loss.

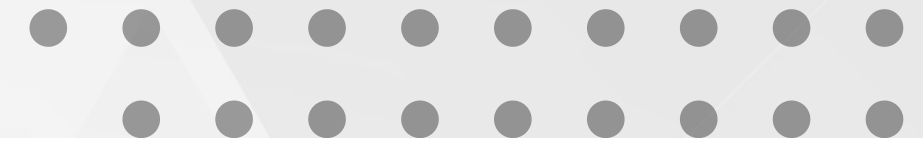
- It automates incident response, so you can contain and remediate threats faster and more efficiently.

## What do I need it for

- Prevent data breach
- Reduce impact of cyberattack /isolate infected endpoints/remove malware and restore to normal operations as quickly as possible.
- Improve security posture
- comply with Threat visibility requirements
- Measure and improve security KPI's

## My workflows

IDENTIFY the threat through Monitoring and alerts  
CONTAIN the threat by isolation of the threat  
/investigate the scope,threat type /impact  
REMEDIATE by removal of threat artifacts,restore from known good state. Confirm BAU  
REPORT how threat was identified,contained.How KPI was met and how workflow can be improved



# The VM example



## What does it do

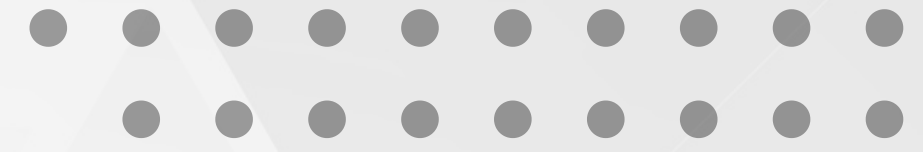
Vulnerability management is a process driven solution that helps identifying, assessing, prioritizing, and remediating security weaknesses in an organization's IT infrastructure. VM solutions are tools that automate and streamline this process, providing risk scores and recommendations, and integrating with other security tools and workflows.

## What do I need it for

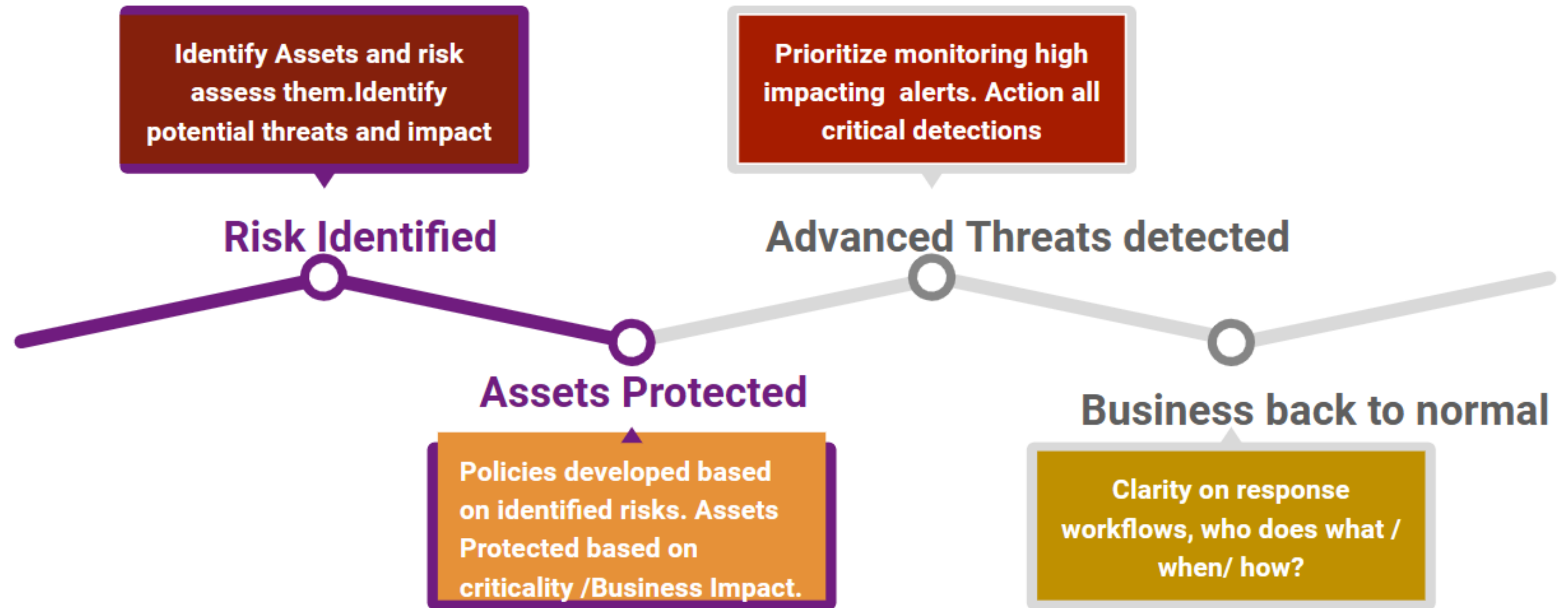
- Continuous and up to date visibility of infrastructure vulnerabilities to include mobile/cloud /IoT
- Accurate and contextual data about network Vulnerabilities
- Score based prioritization of Risks with suggestions for remediation
- Flexible reporting of resolved and unresolved issues

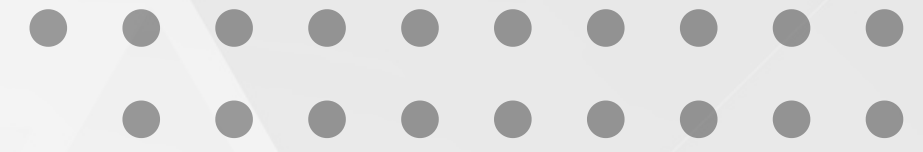
## My workflows

- SCAN IT assets for vulnerabilities
- ANALYZE results and determine risk /impact
- PRIORITIZE results based on analyzed data
- ASSIGN remediation tasks to IT teams
- REMEDIATE - Patch high risk vulnerabilities and "virtual" patch the rest until full patch can be achieved
- REPORT and communicate results to all stakeholders



# Outcomes of a good Workflow





**PARTNERSHIP**



Using defined workflows can help a lean IT team identify capacity gaps and bring in external resources to do specific things at specific times.  
**Productive Partnership**

Outsourced ●



Customer ●

**VALUE**



Cost effective:  
Saves time hiring/ training.  
Enhance security culture through continuous engagements.  
Access to experts  
**Security goals achieved**