RAPID7

THE ANATOMY OF AN ATTACK: HOW MDR DETECTS & RESPONDS IN REAL-TIME

Building and maintaining a SOC from scratch is a massive undertaking. It requires significant investment in skilled personnel to ensure 24/7/365 global coverage - plus the ongoing cost of evolving security tools, platforms, and threat intelligence. Rapid7 MDR delivers the people and technology your SOC wishes it had. In this infographic we will look at how Rapid7's MDR gives you the tools and expertise to secure your entire attack surface through the lifecycle of an attack. We'll also show you what would have happened without Rapid7 MDR.

THE LAUNCH OF AN ATTACK

An attack targeting an unenforced MFA policy is launched by an unknown assailant. The clock starts now.

WITH RAPID7 MDR	WITHOUT RAPID7 MDR
<5 MINUTES TO DETECTION Rapid7's defense-in-depth approach ensures telemetry across endpoints, identities, network, and cloud is continuously gathered and enriched to quickly detect malicious activity.	**~~<5 MINUTES~~ ~~TO DETECTION~~** Unlikely. An overworked, understaffed SOC is often drowning in alerts. Identity attacks often appear as normal activity — it could take days to surface this one if it's seen at all.
AI-LED TRIAGE KICKS IN Rapid7's AI kicks in helping correlate telemetry threat intel, and attacker behaviors to filter the noise and confirm the threat as a true positive.	**~~AI-LED~~ ~~TRIAGE KICKS IN~~** Nope, Rapid7 MDR has AI-powered triage that dispositions alerts with 99.93% accuracy and filters noise to keep SOC experts focused on real attacks at the speed of AI.
A SOC ANALYST IS NOTIFIED WITHIN MINUTES Agentic AI proactively compiles pre-investigative context and delivers it directly to the Rapid7 SOC analyst, providing a full picture of the threat before the attacker can make any lateral movements.	**~~A SOC ANALYST IS NOTIFIED~~ ~~WITHIN MINUTES~~** Without Rapid7's agentic AI workflows laying the investigative groundwork, this poor SOC analyst may still be sifting through alerts, compiling context, and falling behind the attacker.
<12 MINUTES TO CONTAINMENT The SOC analyst executes a response playbook to quarantine the impacted asset and contain the threat — essentially cornering the attacker. Active Remediation with Velociraptor empowers them to remove lingering remnants of the attack.	**~~<12 MINUTES~~ ~~TO CONTAINMENT~~** Again, unlikely. The attacker is still appearing as a valid user. You can't contain what you don't know is there. We're probably looking at days here.
CUSTOMER IS NOTIFIED The SOC analyst delivers an incident report which is then walked through by your Cybersecurity Advisor, detailing the intrusion, containment actions, and recommendations for future prevention. Within 24 hours a detailed forensic report and root cause analysis is delivered to the customer ensuring transparency.	**~~CUSTOMER~~ ~~IS NOTIFIED~~** An analyst discovers suspicious behavior on other affected assets, meaning the attacker has moved laterally. What hope you had at an early containment is all but gone. Time to alert leadership.
1 EXPLOIT, CONTAINED WITHIN MINUTES Within minutes, an attack is contained with 0 data loss.	**~~1 EXPLOIT,~~ ~~CONTAINED WITHIN MINUTES~~** What started as a minor foothold has probably evolved into days of lateral movement with affects across your assets and systems.

THE BOTTOM LINE IS RAPID7'S MDR IS MORE THAN AN EXTENSION OF YOUR TEAM, IT'S A CRITICAL PARTNERSHIP OF TECHNOLOGY AND EXPERTISE THAT IS NEVER OUTMATCHED AND CAN SHUT DOWN THREATS IN MINUTES, NOT DAYS.

WANT TO KNOW MORE? TRY OUR FREE DEMO →

RAPID7