RAPID7

# 7 BEST PRACTICES FOR CYBERSECURITY

## [ APPLYING DEFENSE IN DEPTH TO DETECTION AND RESPONSE ]

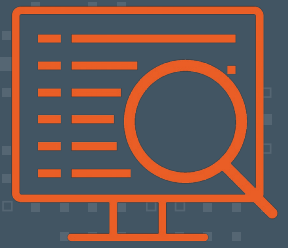
Cyber-attacks **are on the rise,**

as more companies undergo digital transformation and customers demand easier and more convenient access to information and services.

That means the risks and the stakes for companies responsible for data security are also on the rise, and focusing exclusively on preventing breaches is no longer enough.

Detecting active compromises inside IT environments as part of an incident detection and response (IDR) program is critical for effective cybersecurity.

# 1 VISIBILITY



**Defense starts here,** with a comprehensive view of both internal and external network activity and workloads. After all, it's impossible to secure data if you don't know where it is and what it is.

Visibility starts with the full knowledge of all the systems and data used by your organization. A common challenge is monitoring actions taken off the corporate network, such as through cloud services or traveling/remote workers.

This intelligence is the foundation on which the rest of your IDR plan should rest.

# 2 DATA COLLECTION

Centralized logging and endpoint monitoring are **key components** of a successful IDR plan.

Collecting and analyzing logs as well as installing endpoint monitoring solutions may require a significant initial investment. However, just as with gaining visibility into your systems and the data on them, data collection is essential for knowing what's going on in your systems, both historically and in real time. This makes deep analysis of threats and proactive hunting, as well as coordinated responses by your organization, possible.

# 3 MONITORING THE ENTIRE ATTACK SURFACE

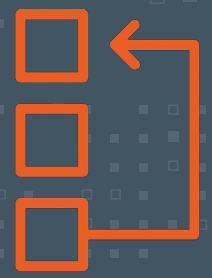
Cloud-based tools have made today's workforce more productive than ever before. Employees can now work wherever and whenever they choose, benefiting professionals and enterprises alike.

But this added convenience comes with a price: greater exposure to cybersecurity risk. The solution is not to stop using these important tools or to prevent employees from using outside networks—without them, you cannot remain competitive—but to properly monitor and manage their use. In addition to properly securing endpoints and access to outside networks, applying advanced analytics to your data allows you to detect stealthy behavior and prioritize where to hunt.

# 4 WORKING WITH YOUR PEOPLE

Security tools, no matter how good, can only be **as effective** as the people and strategy behind them.

That's why a healthy IDR plan also calls for tight coordination between IT and security teams, as well as key stakeholders across the company. IT teams must be incentivized to give security the same importance as optimizing the systems under their care. This vital "people" element is every bit as important as any other part of a well-developed IDR program.



# 5 RECOGNITION OF THE ATTACK CHAIN

Attackers typically work through **five steps** on their way to hacking the systems and data that they've placed in their crosshairs.

1. Infiltration and persistence
2. Reconnaissance
3. Lateral movement
4. Mission target
5. Maintaining presence

Most organizations have solid detection around Mission Target, unauthorized access to critical assets. However, many struggle to detect lateral movement and network reconnaissance. Map your detection program to the attack chain—where are your gaps today?

# 6 UNDERSTANDING LIKELY THREATS

An understanding of the specific kinds of threats that your organization will most likely encounter given its line of business—whether it's a hack on customer data or on trade secrets—is one of the most important parts of an **effective** IDR program.

This allows you to focus your resources and planning where they will do the most good, for example securing the specific systems holding the most sensitive information.

# 7 AN ORGANIZATION-WIDE WORKFLOW

A cyber-attack threatens not just the IT organization; it can impact **every area** of your enterprise.

It's vital to build an incident response plan, review it, and put it to the test. This includes when to loop in external parties and expectations around responding to incidents. Planning and testing your workflows will give your team the muscle memory to take swift action and lead with confidence.

# LEARN MORE

about how IDR can help secure your data.

rapid7.com/idr

RAPID7


CONTACT US OR CONNECT WITH US

North America: +866.7.RAPID7 | sales@rapid7.com

EMEA: +44.(0)118.207.9300 | emeasales@rapid7.com

APAC: +65.3159.0080 | apacsales@rapid7.com

twitter.com/rapid7