CYBERSAINIK

The Importance of XDR

An Overview of Extended Detection & Response (XDR)

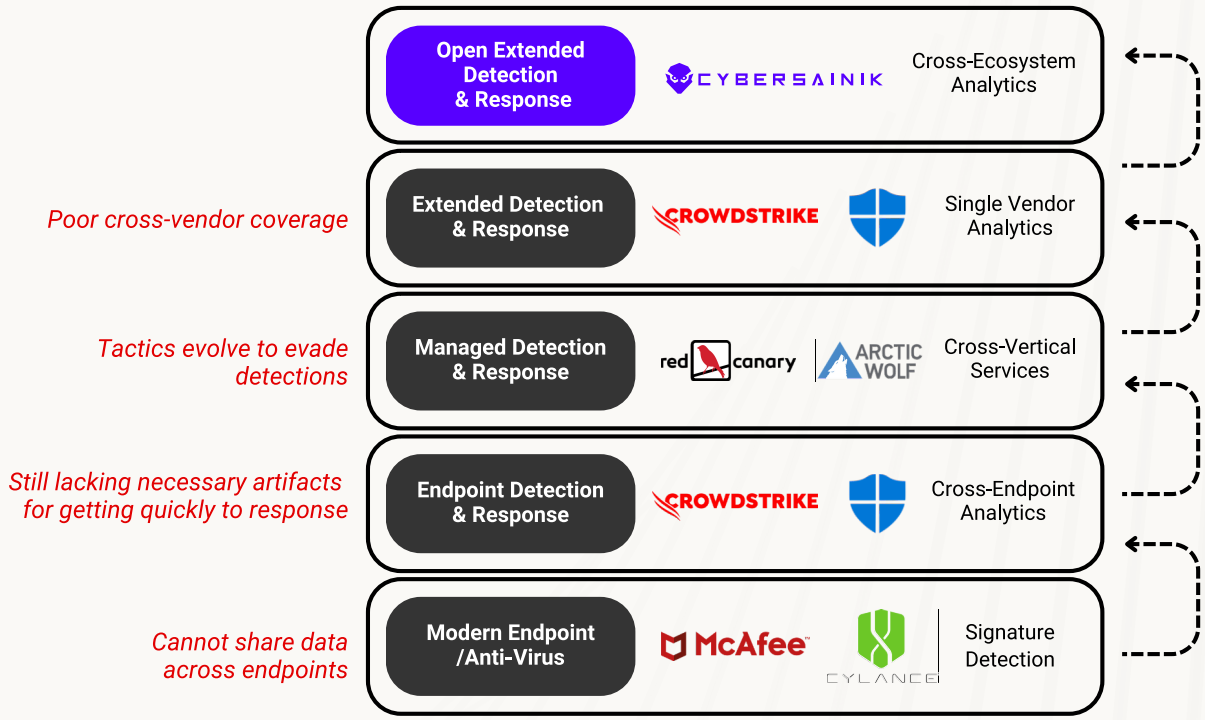
info@cybersainik.com | www.cybersainik.com | 303.867.7500

Contents

info@cybersainik.com | www.cybersainik.com | 303.867.7500

01 | Introduction

While XDR is a new acronym, Extended Detection and Response, the core practice is a more rigorous twist on several long-recommended activities. Moving forward from Endpoint Detection and Response (EDR), XDR extends capabilities broadly by pulling data from other sources, such as network switches and firewalls. XDR also extends detection by depth, through more detailed analytics, and through time, pushing detection to a full 24x7x365 period.



info@cybersainik.com | www.cybersainik.com | 303.867.7500

02 | How XDR Works

By detecting data from regular endpoints (workstations, laptops, servers), as well as other non-endpoints, it is possible to trace an attacker's actions through the network. Traditional EDR detections are typically limited to a specific endpoint. Identifying what happened at a more holistic level can be very difficult, especially given that attackers use different attacks on different types and will often use systems that can't run anti-malware /EDR agents to hide their presence from detectors.

By connecting detection practices to every point in an environment that can be queried, it is possible to both follow an attack through the network and, more importantly, to detect them more quickly. After all, the more sensors you have in an environment, the harder it is for an attacker to evade detection – so if you can turn every device in your environment into a sensor, the better off you'll be.

03 | How XDR is Used

Once data is received by the XDR systems, events can be correlated and matched against known-malicious signals, as well as checked against normal behavior, to identify unusual activity. It is one thing to detect a malicious file, as antivirus solutions have been capable of doing for decades.

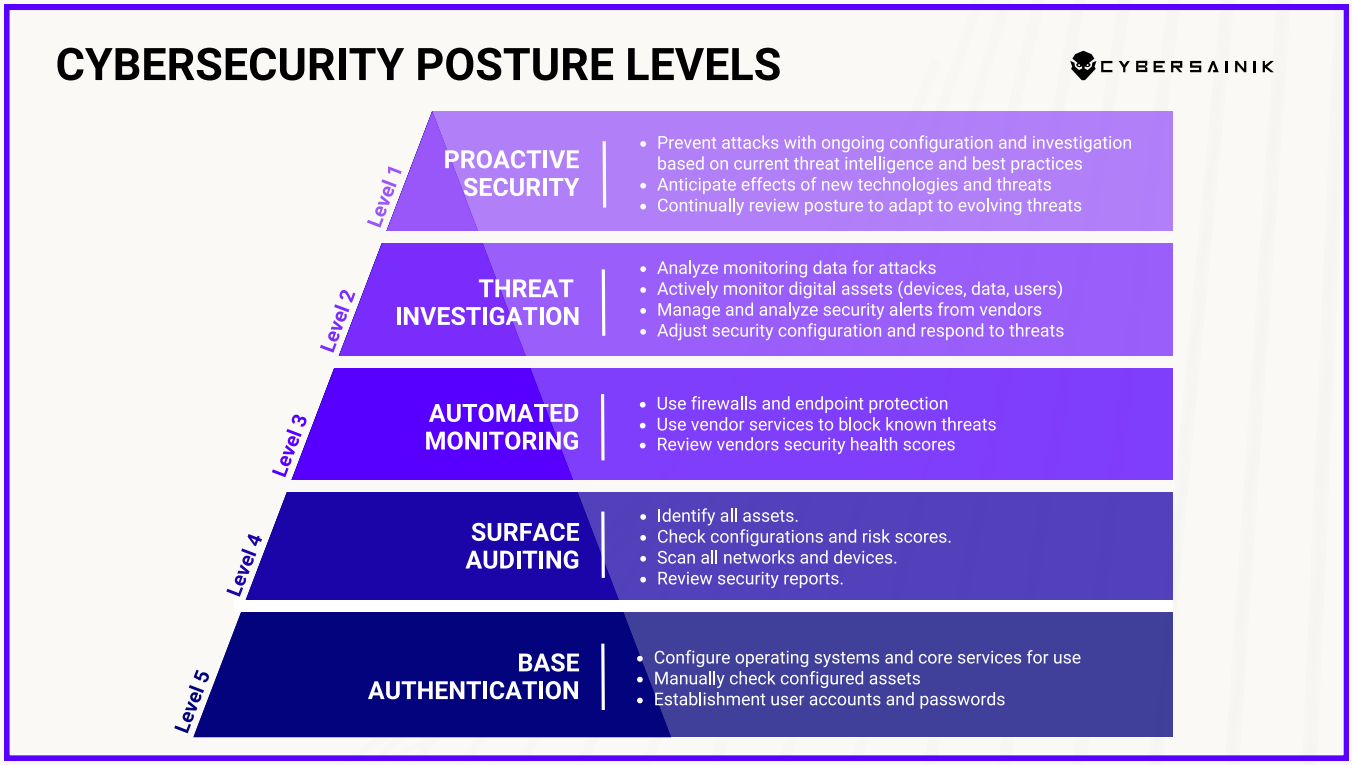
However, detecting that an individual ran a script on one system that connected to a network device as a different user, and then used that network device to connect to different servers, enumerating file shares, databases, and user accounts – is the purview of XDR.

The more advanced the analysis technology, and the capabilities of the team using that technology, the more actions that can be detected – even in environments that are traditionally difficult to monitor, such as OT/IoT, mobile, and cloud environments.

03 | How XDR is Used

By monitoring through time, it is possible to shorten response time which, in turn, reduces dwell time. “Dwell time”, or the amount of time an attacker can have a presence in your environment before they are detected and removed. Prior to the invention of EDR and XDR, it wasn’t uncommon for attackers to spend months to years in a network prior to detection.

Since this technology has become more accepted, however, dwell time has been shrinking to weeks-to-months. In many environments, in fact, XDR technology can detect attackers in real time – a fact that we observe regularly when pentesting environments that run XDR.



info@cybersainik.com | www.cybersainik.com | 303.867.7500

04 | Recommendations

It is important to recognize that not all 24/7/365 environments are the same. Some companies structure their Security Operations Center (SOC) team with standard eight-hour shifts, with three shifts covering the 24-hour period. In fact, it's common in some teams to only staff for two of those shifts and trust the technology to alert people after hours when critical events are detected, leaving less critical events to be analyzed in the morning.

A better model is one that "follows the sun". Most people are more energized and able to focus when the sun is up. By having multiple SOCs, in different time zones, analysis can be optimized, as the people analyzing events are fresh. Moreover, by staggering shifts so that each shift overlaps the others by an hour, proper handoffs can be done, so critical work isn't lost

05 | The Role of Automation

Finally, it is important to understand the role that automation can play. Because attackers use both automated attacks and manual investigation – sometimes manually writing their own attack automation to live in the environment, it is important to structure the team accordingly.

As defenders, automation can be extremely powerful, removing attackers from the environment, near-simultaneously, across all infected devices. However, the same automation can be mis-used, kicking legitimate users out of systems in the same way. Comparably, the automation used to make system changes at scale and speed can also be used to magnify mistakes, making errors happen at speed and scale, too.

To avoid the problem of error at scale, as well as to reduce analysis time and improve accuracy, an outsourced XDR team must function as partner, not just as a service. By working to profile an environment to provide context to their analysis and working with individuals to verify the intent and function of any automation, it is possible to function with both the rigor needed for success as well as with the creativity needed to block attacks and eliminate attackers.

06 | Conclusion

Once in place, XDR can be tested with penetration testing, and environmental weak points can be detected and corrected with a functional vulnerability management and patching program. Iteration through this loop, with vulnerability management hardening the environment and making attacks more difficult to execute, XDR monitoring the environment and making detection harder to evade, and penetration testing driving both practices to increased efficacy, you can improve faster and faster, to the point where attackers can quickly determine that it is better worth their time to target someone else.

CYBERSAINIK

Interested?

So, are you ready to learn more about XDR? Contact us today, and let's embark on this thrilling journey together. Together, we'll revolutionize the way you experience cybersecurity, creating a safer digital world for everyone.