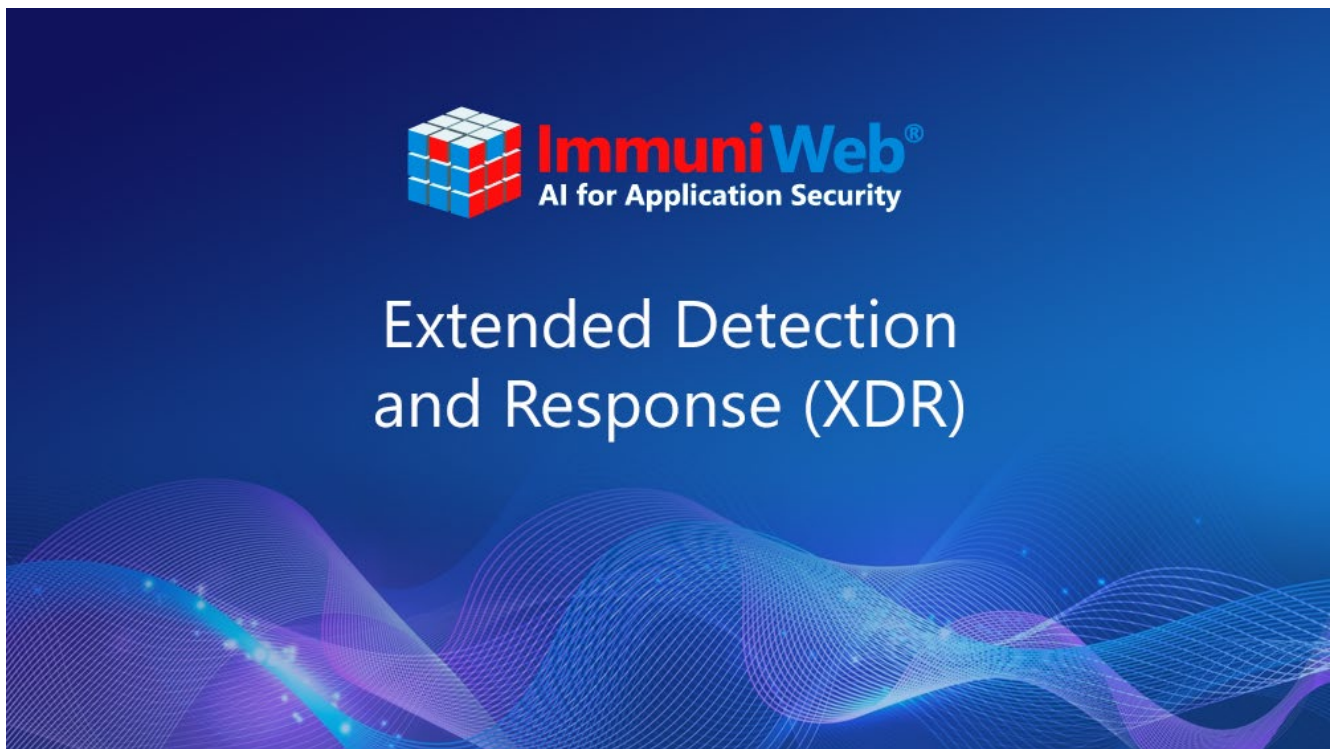# Extended Detection and Response (XDR)

Extended detection and response (XDR) provides a more comprehensive approach to threat detection and response by collecting and analyzing data from a wider range of sources across your network.

Extended Detection and Response (XDR) is another key player in the cybersecurity realm, working alongside Security Information and Event Management (SIEM) and Data Security Posture Management (DSPM) to fortify an organization's defenses.

Try ImmuniWeb Discovery to boost your Extended Detection and Response (XDR) strategy

Extended Detection and Response (XDR) Core Function

Extended Detection and Response (XDR) goes beyond SIEM by offering a more comprehensive approach to threat detection and response. It unifies security data from various sources across your network, endpoints, cloud environments, and applications.

Extended Detection and Response (XDR) Key Features

- ✓ **Broader Data Ingestion:** XDR collects data from a wider range of sources than SIEM, providing a richer picture of potential threats.
- ✓ **Advanced Analytics:** XDR utilizes advanced analytics to correlate data from disparate sources, identify hidden patterns, and detect sophisticated threats.
- ✓ **Automated Response:** XDR can automate incident response actions, allowing security teams to react faster and more efficiently to threats.

Extended Detection and Response (XDR) Benefits

- ✓ **Improved Threat Detection:** XDR's broader data view and advanced analytics lead to more effective identification of complex threats.
- ✓ **Faster Incident Response:** Automated response capabilities enable security teams to neutralize threats quicker.
- ✓ **Reduced Alert Fatigue:** XDR helps prioritize real threats from false positives, saving security analysts valuable time.
- ✓ **Enhanced Security Posture:** By providing a more holistic view of security, XDR empowers organizations to proactively strengthen their defenses.

Extended Detection and Response (XDR) vs Security Information and Event Management (SIEM)

Here's how XDR compares to SIEM and complements other security solutions:

- ✓ **XDR vs. SIEM:** While SIEM excels at centralized log management and event correlation, XDR offers a deeper level of analysis and investigation across a wider range of data sources.
- ✓ **XDR and Security Tools:** XDR integrates with existing security tools like firewalls and endpoint detection and response (EDR) to provide a unified security platform.

Conclusion

In conclusion, Extended Detection and Response (XDR) is a powerful tool for organizations seeking to elevate their threat detection and response capabilities. By providing a comprehensive view of security data and automating response actions, Extended Detection and Response (XDR) empowers security teams to combat today's ever-evolving cyber threats.

What's Next?

- ✓ Read ImmuniWeb Cyber Law and Cybercrime Investigation Blog.
- ✓ Join ImmuniWeb at the upcoming Webinars and Events.
- ✓ Follow ImmuniWeb on LinkedIn, X (Twitter), and Telegram.
- ✓ Subscribe to ImmuniWeb Newsletter.
- ✓ Try ImmuniWeb Community Edition Free Security Tests.
- ✓ See the benefits of ImmuniWeb Partner Program.

. . . .

ImmuniWeb®
AI for Application Security

The award-winning ImmuniWeb® AI Platform helps over 1,000 customers from over 50 countries to test, secure and protect their web and mobile applications, cloud and network infrastructure, to prevent supply chain attacks and data breaches, and to comply with regulatory requirements.

API Penetration Testing	Continuous Automated Red Teaming	Dark Web Monitoring	Phishing Websites Takedown
API Security Scanning	Continuous Breach and Attack Simulation	Digital Brand Protection	Red Teaming Exercise
Attack Surface Management	Continuous Penetration Testing	Mobile Penetration Testing	Third-Party Risk Management
Cloud Penetration Testing	Cyber Threat Intelligence	Mobile Security Scanning	Web Penetration Testing
Cloud Security Posture Management	Cybersecurity Compliance	Network Security Assessment	Web Security Scanning

One Platform. All Needs.
www.immuniweb.com

. . . .