CISO GLOBAL

XDR Extended Detection and Response Buyer's Guide

XDR – Spot the Genuine Article

Extended Detection and Response (XDR) has become something of a buzz-phrase in the IT security world. It's being used to describe a wide range of technologies and solutions, which vary wildly in their nature and capabilities. So much so that we'd say some aren't really XDR at all.

Use this checklist as you look into alternative XDR offerings, to make sure you get the the real deal, not a wannabe.

☐ Scope

Be sure your solution covers all platforms and data points, and doesn't exclude anything. CISO XDR solutions deliver inclusive, clear, centralized data visualization and response for networks, endpoints, cloud, user behavior, email, applications, SaaS and PaaS.

☐ Data Best Practices

Too much or too little data weakens security. XDR should help you identify, visualize and analyze the right data.

☐ Experienced Analysts

While automation, orchestration and ML highlight events of interest, experienced, trained analysts are still key to effective response and remediation. Is the solution founded on a legitimate, trusted SOC using analyst-directed tools?

☐ Automation and Orchestration

Automation, orchestration and customizable playbooks accelerate initial processes, reducing dwell time. Choose a solution that will adapt to your processes and support your compliance requirements and business case; don't get stuck with analog processes or having to conform to the provider's approach.

☐ SOC Staffing

Some SOCs rely on less experienced teams, especially out of hours, degrading service, increasing your workload and driving up the risk of breaches. Check that the SOC is fully staffed by experienced, certified analysts, around the clock, 365 days a year.

☐ Compliance

Check the SOC's location, its analysts' certifications and the residency of your data to be sure they satisfy your compliance requirements.

☐ SOC Capacity

Your needs may grow over time. Check that the SOC has sufficient capacity to scale its service in line with your requirements.

☐ Staying Open

"Vendor-centric" or "closed" XDR solutions only accept telemetry from a restricted range of platforms. Choose an open solution that won't force expensive rip-and-replace during solution architecting, or limit your future technology choices.

☐ Is the SOC Actually a SOC?

Some SOCs are in reality specialized call centers, passing alerts straight through to you for assessment and action. Check that you'll get the full benefit of experienced analyst service, reducing your workload, accelerating responses and cutting the risk of breaches.

Talk to the Experts

Contact us for expert advice on how XDR can improve your security stance, reduce risk and cut your workload.

e: sales@ciso.inc
t: 866-430-2595

ciso.inc