Video transcript

What is endpoint detection and response (EDR)?

What is EDR? The acronym stands for endpoint detection and response, which is increasingly an essential part of any competent cybersecurity strategy.

Over the next few minutes, I'll go through how it works and why it's so essential these days.

I'm Sam Hector from the IBM Security team and what I think EDR is really doing is endpoint threat detection and response. After all, the point of EDR is not to go around detecting all of the laptops, phones, and servers on your network; but rather it's to proactively detect threats on those end points, when they occur, and respond to them in real time.

To do this effectively it needs to do four things really well.

1. Collect security data from the end points using an agent, which is a small light weight application that runs on each of these devices to enable data gathering, detection, and then response actions to take place, even when that endpoint isn't connected to the internet. It needs to collect security relevant to telemetry, like what processes are they running, what servers are they connecting to, and what files are being accessed, and lots more information that can be useful to detect the presence of a threat. All to use in forensic analysis and investigation after an attack has occurred.

2. The second thing it needs to do is detect and respond to threats in real time and automatically. It does this mainly in two different ways. One for threats we've seen before and one for threats we've never seen. When we detect attacks in the wild, security teams can gather what's called indicators of compromise or IOCs. In order to take a unique fingerprint of a piece of malware, like a run somewhere tool that has been around for a while, for example. In this case the EDR tool can act like the bouncer on the door of a night club denying entry to a list of bad actors before they even get in. Traditionally this is what anti-virus would have been known for doing. But what about threats we've never seen before or how would an EDR solution protect against the growing number of fileless attacks (ones which never download malicious malware or leave any trace). Well, even threats we've seen before use similar tactics and techniques to past attacks we're already aware of. So, in order to detect them without a fingerprint, it's a case of using advanced algorithms to look for those behaviors. For example, a really common method of distributing malware is by hiding it in the macro code of an innocent looking Microsoft office file. An EDR tool could stop this by noticing when the excel application tries to alter the systems security settings, something it would never normally need to do. So, the EDR can block the attempt before it's successful.

3. The third thing it needs to enable is forensic investigation and threat hunting. Cause I’m afraid to say that no EDR tool will stop one hundred percent of attacks. But by capturing lots of security relevant information they can help security teams understand how attacks were successful and how to change their approach to ensure their detected and blocked in the future. This can also enable security teams to perform threat hunting activities. To go and proactively investigate all of their end

points at once for the presence of a new threat that's not yet detected automatically so they can manually take action to reduce their risk.

4. And finally, an EDR tool needs to integrate and report. For a security analyst, it needs to integrate into their existing workflow. They're often inundated by alerts; they need to triage from lots of different tools. An EDR should help them prioritize incidents to look at urgently, present them with all of the potentially relevant information in a friendly interface, and speak the same language as other security tools by adopting common vernacular like the MITRE ATT&CK framework. For a security team, an EDR tool needs to integrate with all of their existing capability and feed additional telemetry into a management platform, like a sim tool for threat detection, a sort tool for instant response, or an XDR platform that combines these capabilities. It also needs to enable reporting, both on the importance of your organizations mean time to respond to an attack, but also reporting against compliance to regulatory frameworks.

So, to finish, if you're looking for an EDR tool, here's a few things you should really look out for. The best ones like IBM's ReaQta will be highly resilient to attack ideally by being invisible and inaccessible to running malware on the operating system. They should use advanced AI to learn from the decisions your analysts have made in the past and recommend that in future that alert is automatically handled to drastically reduce the analyst workload by more than eighty percent. They should have log in capabilities that use as little data as possible to save money on the cost of bandwidth, and offer multiple deployment models between SaaS, on-prem, and even air-gapped environments to give you as much flexibility as possible.

To talk to IBM about adopting EDR or even optimizing your approach, click the link in the description*, and get involved in the conversation in the comments below. Check out our other cybersecurity videos and subscribe to see more in the future.

*Resources:
Learn more about QRadar EDR:
https://www.ibm.com/products/qradar-edr

Dive deeper into EDR solutions: https://securityintelligence.com/posts/what-is-endpoint-detection-response