Nine questions to ask cybersecurity AI vendors

1. **Machine learning algorithms**
   What type of machine learning algorithms does your product use?

2. **Volume of machine learning algorithms**
   How many machine learning algorithms does your product have and how are they categorized? How frequently do you update them and release new algorithms?

3. **Machine learning times**
   How long until machine learning algorithms can trigger detections in a new environment? How many algorithms require a learning period, and how long does that take?

4. **Risk prioritization**
   How does your product prioritize critical and high-risk hosts that require immediate attention from an analyst?

5. **Incident response workflow**
   Does your product integrate seamlessly into existing detection, alerting, and incident response workflow?

6. **Third-party response integration**
   What firewall, endpoint security, or NAC integration does your product provide to block or contain detected attacks? How does your product integrate with these platforms?

7. **Workload reduction**
   What is the workload reduction your product provides for security analysts? What kind of efficiency increase can be expected?

8. **Red-team testing**
   Does your product support running red team exercises to prove the value of machine learning algorithms and AI work in real world scenarios? Will you pay for the red team if your product doesn’t detect anything?

9. **Remote vendor access**
   Do you recommend that human analysts have remote access to the product during the evaluation? Why?