Cortex XDR: Security Operations and Integration

What if you could take all the security measures you have in place for your company and make them even more secure? What if there was a solution that could do just that? There is one: it's called Cortex XDR.

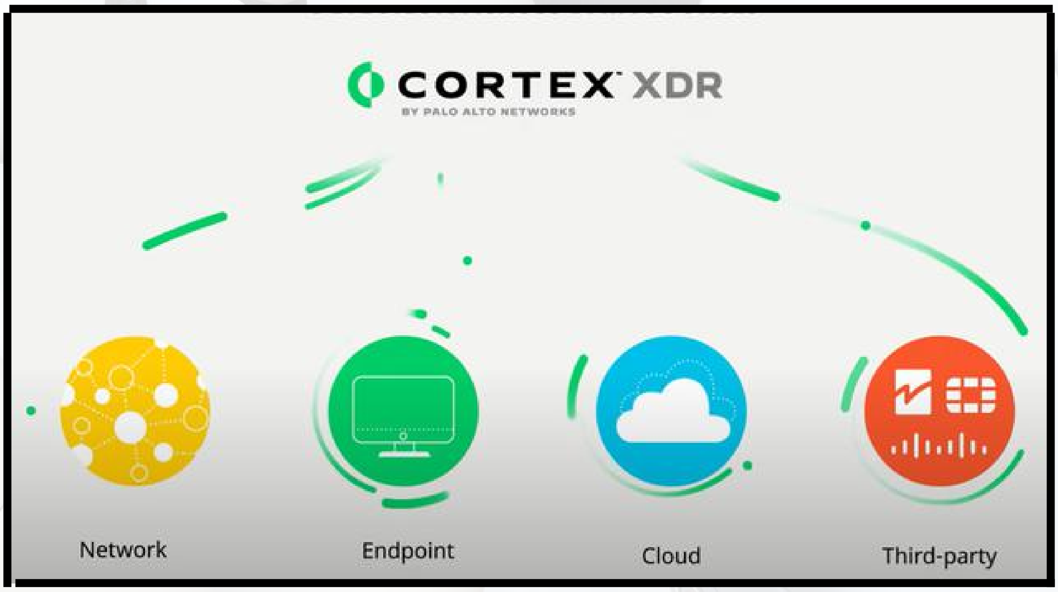
Palo Alto Networks Cortex XDR is the world's first extended detection and response platform, natively integrating data from network, endpoint, cloud, and third-party devices to identify and prevent cybersecurity threats. It's the next evolution in security technology and the future of securing your business and data.

What is Cortex XDR?

Can your security team keep up? Modern cybersecurity threats target your users, endpoints and servers. They are sophisticated and multi-layered, making detection and response difficult. The Cortex XDR solution unifies detection and prevention, with investigation and response, into a single platform.

The Cortex XDR solution collects and automatically correlates data across multiple security layers, including endpoints, servers, cloud workloads, and third-party firewalls. Cortex XDR secures your endpoints using multi-method malware and exploits protection, capabilities. Cortex XDR simplifies alert investigation and incident management, enabling you to find threats faster and make immediate responses.

In this guide, we'll explore some of the benefits of implementing and using the Palo Alto Networks Cortex XDR management console and how to overcome issues with skilled instructor led training and incident management techniques.



Cortex XDR

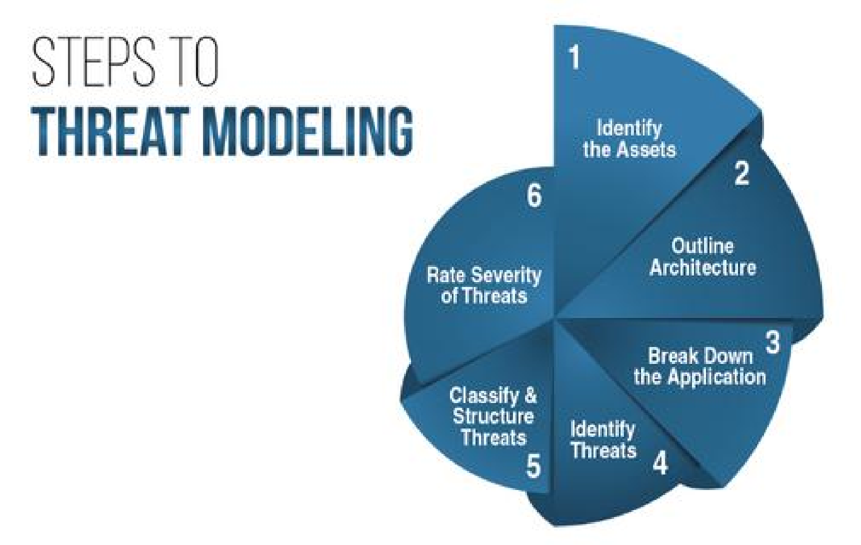
The XDR management console, systems, and Cortex XDR alerts are designed to work with various data sources. These include security information, event management (SIEM) systems, Security Orchestration, Automation and Response (SOAR) platforms. XDR technology can detect and respond to various threats, including malware, phishing, ransomware, and malicious insiders. Security analytics platforms and XDR systems are often used to give a complete picture of an organization's security posture. This technology can also support other security functions, such as incident response and forensics. However, these systems are not without challenges. Implementing an XDR solution can challenge Security Operations Centre (SOC) teams and security operations specialists.

What are some of the key business benefits?

By consolidating data from disparate security tools, XDR enables businesses to detect and respond to threats more quickly and effectively. Here are five benefits of implementing XDR:

1. Improved detection:

XDR can help businesses identify threats that would otherwise go undetected. The Cortex XDR management console can provide a more comprehensive view of activity across the IT environment by consolidating data from multiple sources.

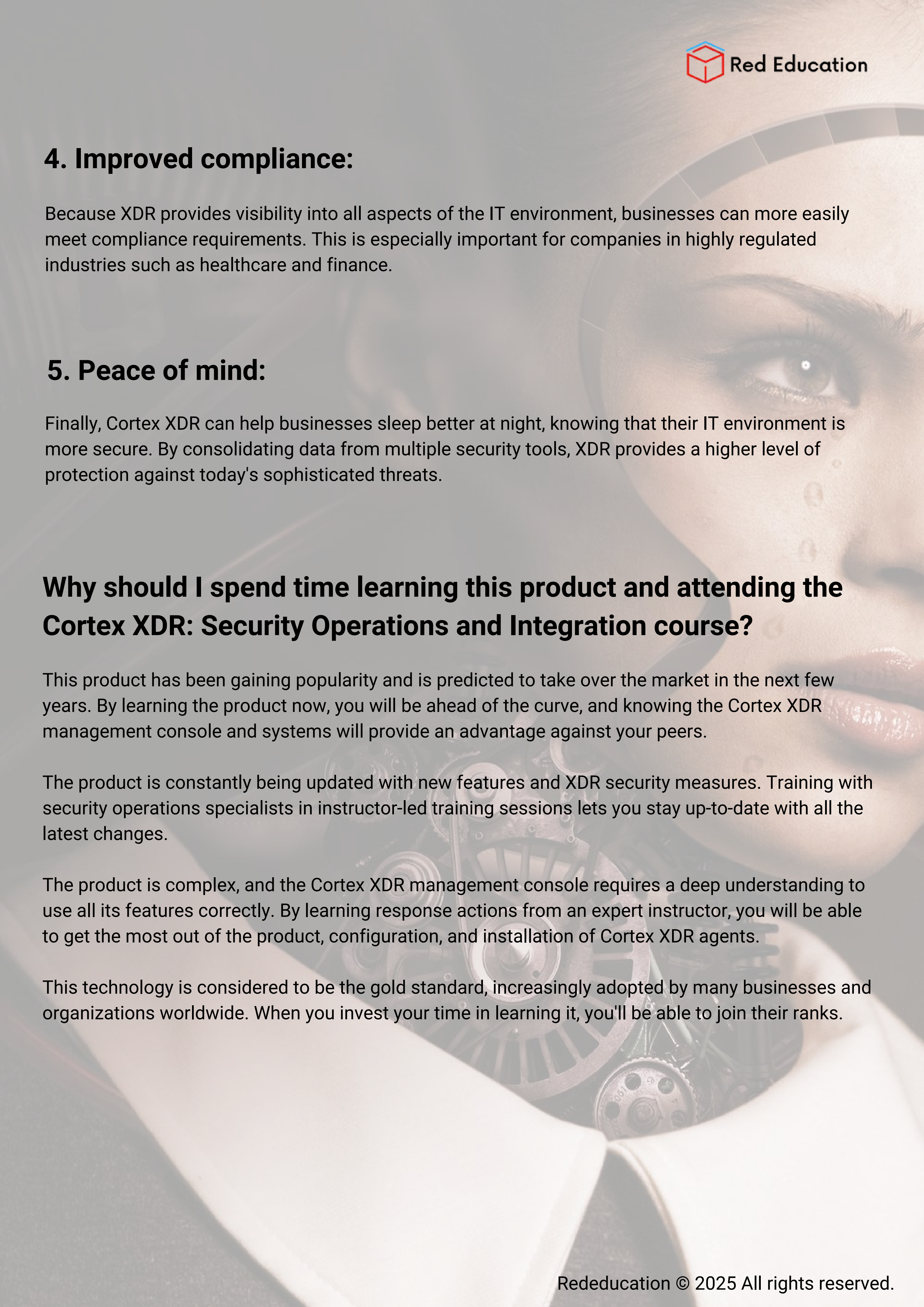


2. Faster response:

Because XDR provides visibility into all aspects of the IT environment, businesses can quickly identify Cortex XDR alerts and respond to threats. This can help minimise the impact of an attack and minimise downtime.

3. Reduced costs:

By consolidating data from multiple security tools, XDR can help businesses reduce the number of tools they need to purchase and maintain. In addition, Cortex XDR can automate many tasks that are currently performed manually, resulting in further cost savings.



4. Improved compliance:

Because XDR provides visibility into all aspects of the IT environment, businesses can more easily meet compliance requirements. This is especially important for companies in highly regulated industries such as healthcare and finance.

5. Peace of mind:

Finally, Cortex XDR can help businesses sleep better at night, knowing that their IT environment is more secure. By consolidating data from multiple security tools, XDR provides a higher level of protection against today's sophisticated threats.

Why should I spend time learning this product and attending the Cortex XDR: Security Operations and Integration course?

This product has been gaining popularity and is predicted to take over the market in the next few years. By learning the product now, you will be ahead of the curve, and knowing the Cortex XDR management console and systems will provide an advantage against your peers.

The product is constantly being updated with new features and XDR security measures. Training with security operations specialists in instructor-led training sessions lets you stay up-to-date with all the latest changes.

The product is complex, and the Cortex XDR management console requires a deep understanding to use all its features correctly. By learning response actions from an expert instructor, you will be able to get the most out of the product, configuration, and installation of Cortex XDR agents.

This technology is considered to be the gold standard, increasingly adopted by many businesses and organizations worldwide. When you invest your time in learning it, you'll be able to join their ranks.

Okay, I'm interested, tell me more about the course now.

The Cortex XDR: Security Operations and Integration instructor-led course is either a virtual or face-to-face delivery occurring over three days. This instructor-led training provides access to a skilled tutor who uses approved courseware materials to expedite learning. The instructor can give immediate feedback, answer any questions, and tailor the pace of the training to the needs of the students. Virtual labs provide a realistic environment for practising what is being learned, such as installing Cortex XDR agents, updates, and configuration. The extensive lab activities will provide hands-on experience using Red Education’s Cortex XDR instance.

This 3-day instructor-led course provides in-depth training on Cortex XDR, Palo Alto Networks' powerful extended detection and response platform. You will gain hands-on expertise in security operations, incident investigation, and system optimization to effectively protect modern environments. Throughout this course you will explore the key features of Cortex XDR.

- Describe the role of Cortex XDR components, including endpoint agents, XDR collectors, NGFWs, and Broker VMs, in securing networks and devices.
- Utilize XQL to query and analyze logs for effective data ingestion and threat detection.
- Design and implement workflows to streamline security operations.
- Apply External Dynamic Lists and indicator rules to enforce security policies.

The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to configure security integrations, develop workflows, manage indicators, and optimize dashboards for enhanced security operations.

What are the prerequisite skills I need to attend?

Before attending this course, participants should have a solid understanding of cybersecurity principles, including network and endpoint security concepts, as well as a basic knowledge of networking and security fundamentals. Familiarity with their organisation's infrastructure and deployed products is recommended, along with a clear understanding of deployment goals and the role of each team member. Having this foundation ensures that attendees are well-prepared to gain maximum value from the course and apply the skills successfully in their environment.

Why are certifications so important to my career and job?

Many people enter the workforce without certifications, and while they may be able to find a job, they will likely face several obstacles. For starters, they will be less productive than their certified counterparts, and they will also be more likely to make mistakes. Also, it will be hard for them to get the respect of their peers, and they might not be able to get specific promotions or raises in pay. While certifications may seem unnecessary, they can provide several benefits that make them worth the investment. With the proper certifications, you can be more productive, make fewer mistakes, and gain the respect of your peers. In addition, certifications can lead to higher salaries and more significant opportunities for advancement.

So why should I choose Red Education?

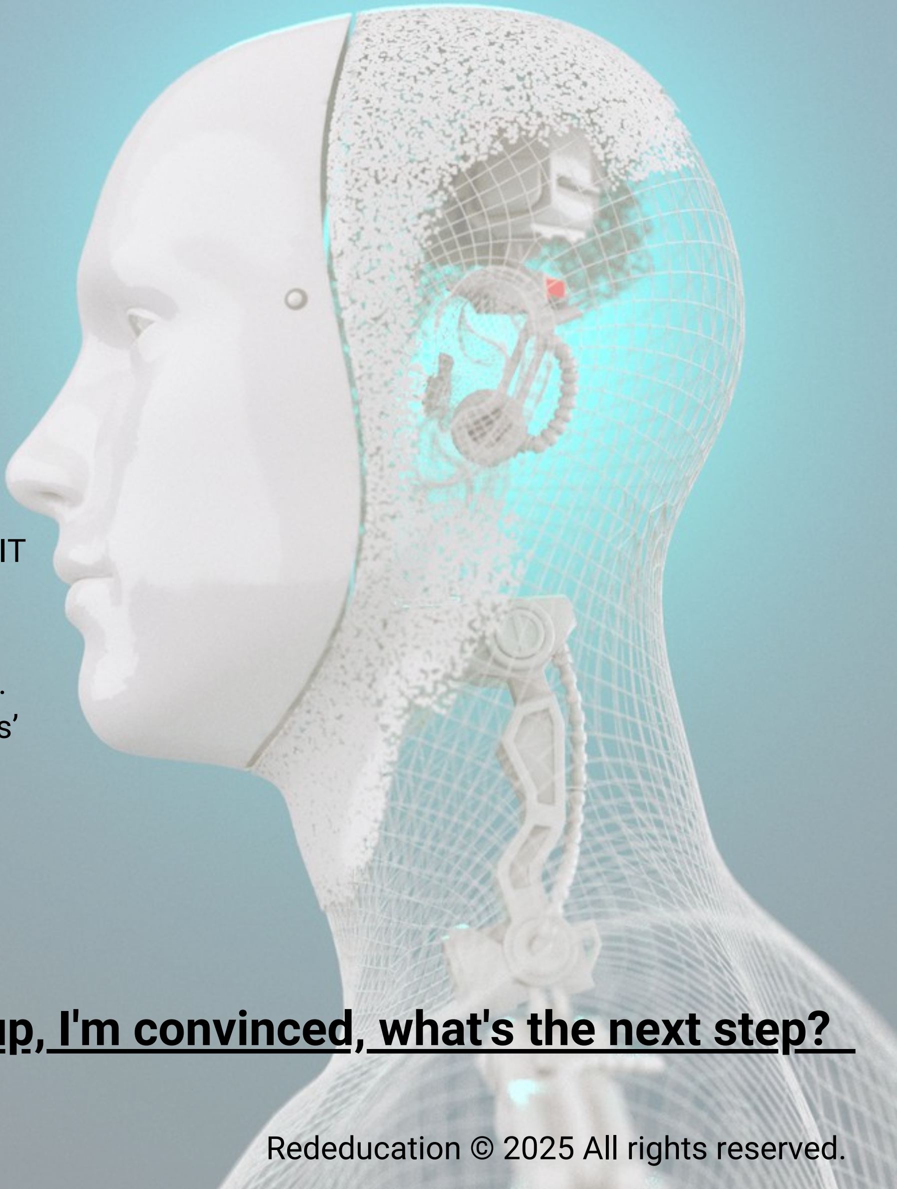
paloalto
Authorized Global Training Partner
Red Education wins Palo Alto Networks Authorised Training Partner and Instructor of the Year 2022 JAPAC
paloalto NETWORKS

Red Education is an information technology accredited certification training company, commonly known as an ATC. A winner of numerous Palo Alto Networks ATC and Instructor of the Year awards, they are an industry leader supporting Palo Alto Networks certification training at a global level.

Serving the global IT community

Red Education exists to serve the global IT community, specialising in cyber security training. Since opening its doors in 2005, Red Education has taught more than 100,000 students worldwide. These students come from many different places, cultures, languages, and time zones. Red Education employs a highly qualified and experienced team of local instructors with the communications skills to deliver a premium training outcome. Using certified courseware materials and allowing students to practice what they learn in our award-winning simulated virtual "lab" environment, this technique is the perfect blend of conceptual training reinforced and backed up with a hands-on lab-build approach to ensure complete understanding.

Recently, Red Education has become a critical delivery partner to the global security industry. At the start of 2020, governments around the world mandated responses to COVID-19, forcing businesses to spend money updating their computer systems and processes as they rushed to support virtual point-of-sale (VPOS) operations and replace more traditional brick-and-mortar businesses. These fast changes put businesses in danger, giving cybercriminals the chance to break into networks through identity theft, malware, phishing, data theft, and cryptographic operations.



The purpose of Red Education is twofold.

- **For their students**: to empower them through learning
- **For organizations:** to ensure their protection against cyber threats by providing highly skilled personnel to implement the latest cybersecurity technology solutions.

They do this by providing a training framework that supports and upskills the IT community they serve, with the essential technical knowledge that underpins their respective companies' operating systems. These outcomes greatly enhance students' understanding of the implementation process, maintenance, and best practice standards to support the relevant technology in the field.

Okay sign me up, I'm convinced, what's the next step?