RANGEFORCE

The Key to an Effective Cybersecurity Strategy:

Ensuring Security Orchestration through Hands-on Training

Unoptimized security solutions cost time and money. Take back control of your cybersecurity program by training the people behind your products and processes.

RANGEFORCE

Cybersecurity Success is Built on Orchestration

Cybersecurity teams operate in a world inundated with tools and solutions. There's a constant stream of emerging technology with vendors eager to simplify our work, but the real challenge remains the same: How can I equip my team to effectively use the tools already at their disposal?

When trained teams use the right combination of tools during a cyber incident, threats can easily be identified and contained. It falls to cybersecurity leaders to ensure that their team understands how to successfully use the solutions at hand.

With so much investment in security infrastructure, simulation-based training is key to every cybersecurity team's success and its ability to maximize a return on investment (ROI). Although millions of dollars are dedicated to acquiring and deploying new cybersecurity tools, undertrained teams will fail to use these solutions to their fullest potential.

Real-world training enables teams to create successful security workflows that leverage coordination across multiple optimized tools. In the event that a real threat is detected, teams will be trained to deploy the right tools at the right time in order to better defend the organization.

> "A layered approach to cybersecurity is widely considered to be an industry best practice. It encourages teams to apply an array of best-in-class cybersecurity tools proportionate to the organization's risk."

In theory, organizations are best protected by a layered approach to cybersecurity built on best-in-class security tools. In reality, the desired outcome is rarely achieved. Why? Because most teams are not fully trained to use the technology on which their security program is built.

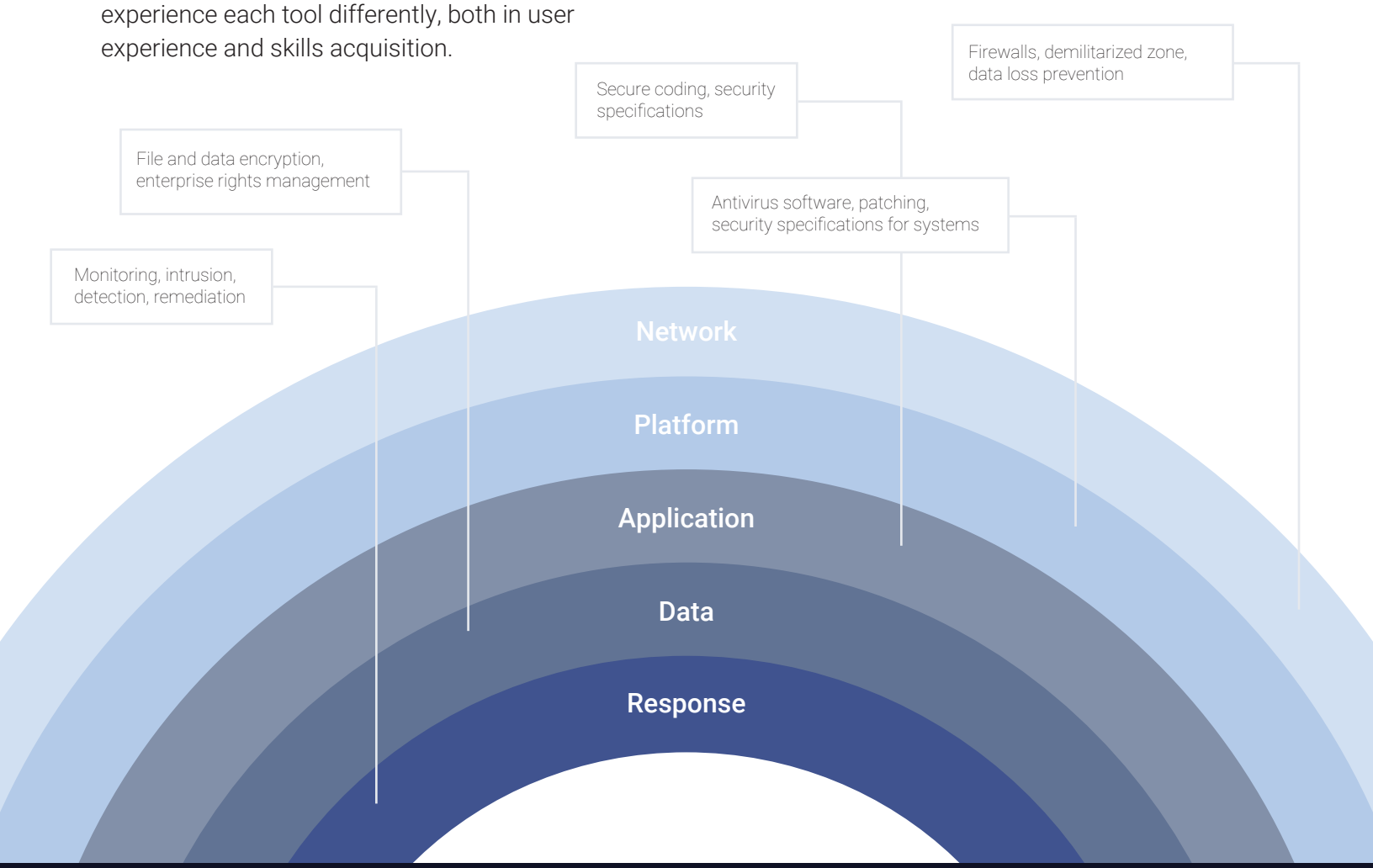
RANGEFORCE

The Importance of Layered Security

A layered approach to cybersecurity is widely considered to be an industry best practice. It encourages teams to apply an array of best-in-class cybersecurity tools proportionate to the organization's risk. If a threat bypasses one solution, it will be discovered and mitigated by another.

This is a sound approach to security, but it relies on strong assumptions about the ecosystem of solutions and their ability to work together. From one tool to the next, security practitioners experience each tool differently, both in user experience and skills acquisition.

Not surprisingly, it's challenging to effectively train teams within this framework. Add to that high turnover rates and a looming cybersecurity skills shortage, and the problem becomes even more complex.



RANGEFORCE

The Pantheon of Security Tools

Most organizations rely on anti-virus software and network firewalls at a minimum. As new threats emerge and existing threats increase in both volume and complexity, the demand for additional cybersecurity tools increases. Traditional anti-virus software is being augmented by endpoint detection and response (EDR) tools that promise to automate endpoint protection, and there's now a variety of application-specific firewalls.

On top of foundational technology, many organizations deploy scanning and monitoring software, encryption tools, packet sniffers, security information event management (SIEM) solutions, password managers, and penetration testing tools. In order to raise actionable intelligence from the thousands of alerts these tools create, security teams are now implementing additional security intelligence tools. Although APIs exist to connect this complicated ecosystem, it does not solve a critical problem at the user level: a lack of effective, hands-on training.

Most security analysts leave a company in **just over two years (26.1 months).**

It can take **over 6 months** to fill open cybersecurity positions.

Calendar Year		
January	February	March
April	May	June
July	August	September
October	November	December

The more robust the tool, the more difficult it is to learn and successfully operationalize. It takes a team of security practitioners to defend an organization. And few organizations can afford the time it takes to learn every available tool in play. While some teams manage to hire specialist roles, cross-training is still imperative. Cybersecurity teams that have cross-functionals skills are becoming an absolute requirement.

Finding cybersecurity talent with the right expertise at exactly the right time is improbable. What's more, 62% of organizations say their cybersecurity team is currently understaffed.[1] Most security analysts leave a company in just over two years (26.1 months), and it can take over six months to replace them.[2] Cybersecurity teams need skills depth in order to absorb the impact of staffing challenges.

1. Ponemon Institute *Second Annual Study on the Economics of Security Operations Centers: What is the True Cost for Effective Results?*, January 2021
2. ISACA *State of Cybersecurity 2020 Part 2*, June 2020

RANGEFORCE

The State of Cybersecurity Training

A cybersecurity strategy that fails to adequately prioritize training is a non-starter. With existing training methods it can take a year to get a new team member up to speed. Even after costly university or third-party training, new hires still face a steep, on-the-job learning curve. Traditional training solutions fail to reflect the real-world environments that cybersecurity practitioners will soon be asked to defend.

IT environments continually evolve. As emerging technology is deployed, the attack surface continues to expand. These changes require training resources at both the technical product level and threat level.

> "The key to ensuring that success is continuous, hands-on training."

Cybersecurity is a team sport. And the only way teams can be expected to win is if they train together. Hands-on, simulation-based training that features real-world scenarios is a requirement for cybersecurity teams. This approach offers teams a dedicated virtual training ground where they can commit playbooks to memory while building the collective reflexes and skills needed to counter cyber threats.

Security Orchestration Training with RangeForce

RangeForce combines simulation-based skills development and highly realistic threat exercises to upskill learners on real cybersecurity tools and solutions. The cloud-based platform is available to teams on-demand and features enterprise level assessments and reporting capabilities for security leaders. Training can be accessed anywhere, at any time, from any browser.

Each RangeForce training module is interactive in nature, designed to keep learners engaged throughout the entirety of the course. The self-paced content ranges from beginner to advanced, covering both vendor and open-source tools. RangeForce training is conducted in entirely emulated environments – featuring real IT infrastructure, real security tools, and real threats.

Security leaders can create targeted learning paths to challenge and upskill their entire team. Prebuilt learning paths include SOC Analyst 1, SOC Analyst 2, Threat Hunter, Web Application Security, and more. RangeForce presents teams with high-intensity threat exercises to train together, as a team.

With RangeForce, security leaders can better understand their team's operational and skills gaps to craft remedial training plans. Teams can expand their program to encompass a wide range of security orchestration training needs.

RANGEFORCE

Maximizing Cybersecurity ROI

Security operations centers (SOCs) are expensive. On average, organizations are spending $2.86 million each year.[3] Employees alone account for a third of these costs.

What's more, investments in cybersecurity as a percentage of the overall IT budget continue to increase. Generally, we trust these investments to be purposeful and strategic, but security leaders face constant pressure to justify their expenses, cut cost, and consolidate resources where possible.

How can security leaders measure a return on cybersecurity investment? The answer lies in the ability to effectively deploy and manage the tools already available to us.

Beginning Your Security Orchestration Program

The increasing complexity of the threat landscape and continued digital transformation trends have made cybersecurity more important than ever before. Cyber threats have become an existential threat to businesses.

Simultaneously, we're witnessing a corresponding evolution of security solutions and emerging technology that are rising to meet these challenges. Training and equipping the human element that drives a team's cybersecurity operations is critical to success.

The key to ensuring that success is continuous, hands-on training. Learn more about implementing a security orchestration training program with RangeForce by visiting RangeForce.com.

Train with RangeForce to:

- Improve the ROI of each technology deployed through more effective training, increasing product usage and maximizing the solution's value
- Improve SOC detection and response metrics by optimizing playbooks across vendor technologies
- Quickly (in weeks, not months or years) train junior staff to be effective security analysts
- Accurately measure and assess team skills, identifying and correcting weaknesses, while also discovering top talent to cross-train and specialize
- Prepare a cross-functional team to better respond to actual cyber threats through repeated simulation-based practice sessions
- Develop learning paths that increase retention and create clear career paths for analysts, engineers, and other team members throughout IT and security
- Reduce the cost of conventional instructor-led training programs

Visit RangeForce.com

Learn more about starting a security orchestration training program for your team.

3. Ponemon Institute *The Economics of Security Operations Centers: What is the True Cost for Effective Results,* January 2020

RangeForce empowers team cyber readiness at scale. Refine your defensive capabilities against the latest threats with a continuous approach to cybersecurity skills development. See real threats in action and sharpen the skills needed to defend your organization with interactive modules, challenges, and team-based threat exercises that reflect the real world.

Visit www.rangeforce.com to learn more.

rangeforce.com | sales@rangeforce.com