DATAPRISE

The Cybersecurity Playbook:

Crafting a Champion-Level Defense

The Cybersecurity Playbook:

Crafting a Champion-Level Defense

Olympic athletes train for years to reach the pinnacle of their abilities. As their body changes and their stamina grows, they adapt their routines so they're constantly improving. If they have a setback, they find ways to push through the challenges, using their innate drive to keep moving.

There are some essential parallels that a cybersecurity team can draw from if they want to improve their defenses in an increasingly interconnected world. Here, we look at champion-level frameworks that address everything from employee awareness to risk mitigation.

Table of Contents

Introduction

With both Olympic athletes and cybersecurity teams, there is no progress without a solid commitment, rigorous training, and strategic planning. An athlete may not be able to predict every muscle twist or irregular landing, but they can strengthen their bodies so they're more resilient against the unknown. Here, we look at how cybersecurity teams can flesh out their playbooks to drastically reduce risk.

Risk Assessments

The sophistication of vulnerabilities, with AI leveraged tools means organizations of all sizes need to tighten up and perfect their threat triage strategy. Recent security breaches targeting major organizations, such as T-Mobile, serve as reference points in figuring out gaps within an organizations posture.

assessment, an organization can understand their weaknesses and gaps prior to malicious actors taking advantage. In parallel, much like Olympians are vigilant about their environments, including the safety of their equipment and their competitors, organizations need to have a strong handle on assessing both the scope of the threats, and the likelihood that they will occur.

Understanding Threats

It is easier to defend your business wholly when you know what is being sought after.

- **Financial Gain:** Statista reports that as of the end of 2023 (hyperlink this, the average cost of a data breach in the United States amounted to $9.48 million, up from the previous year. Cybercriminals use phishing, ransomware, and malware to extract funds from individuals or organizations.
- **Political Chaos:** In today's day and age, cybercriminals act on behalf of nation-states to engage in espionage, aiming to leverage critical information against another country to position themselves in power.
- **Revenge:** Disgruntled employees or affiliates may use their insider knowledge to maliciously target a company.
- **Disruption:** Hacktivists may disrupt or expose a company to promote their ideological views.

Identifying Vulnerabilities

As athletes push their bodies to the limit, preparing for the once-in-a-lifetime accomplishment of playing in the Olympics, they take care to treat their 'vulnerabilities'. Identifying areas of rehab to ensure they are fully fit and ready to go when the time arises, is a critical step of the preperation process. Similarly, cybersecurity teams need to regularly overview their password policies, software patching schedules, access controls, and system configuration. A lack of preparedness is exactly what malicious actors target - so if an organization rarely exhibits strong IT posture, they can be viewed as a prime target for threat actors.

Assessing Impact and Likelihood

In order to be the best, a critical step is to understand and acknowledge what makes the best actually, 'the best'. For an athlete, they study their competitions' game to gain a competitive edge in a split second advantage - which could be enough to make the pivotal difference as they drive forward for the Olympic gold. For cybersecurity teams, that may look like:

- Scenario analysis to walk through the most likely consequences of different threats.
- Assigning values to potential losses, such as the projected monetary cost of a security breach.
- Assessing the odds of each threat and prioritizing resources (e.g., labor hours, budget, etc.) based on both likelihood and potential losses.

Developing a Risk Mitigation Plan

The goal of a Risk Mitigation plan is to outline what the assigned team will do, to block or reduce the impact of the threat when it arrives. For an Olympic athlete, risk mitigation would look like regular physical therapy and rehab to ensure their body is in tip top shape to respond to risks, changing their diet for a period of time to ensure they are properly fueled, or even cross-training to prepare for an unexpected outcome. A cybersecurity team wishing to establish a strong, cohesive risk mitigation plan would aim to consistently test backup and recovery services, regularly penetration test alongside patching, and even better constructing their defenses with stronger firewalls.

Employee Training

An Olympian would be next to nothing without a strong support system. They heavily rely on teammates, even in solo competitions, to provide motivation and act as a pillar of support. Everyone on both an Olympic team, and a cybersecurity team, has to be working towards the same goals for constant improvement to land that Gold status.

Building a Security-Aware Culture

Fostering awareness amongst your teammates, even if they are not in a technology facing role, can led to a stricter posture. In order to build a more security aware culture within an organization, consider the following tips:

- **Lead by Example:** It may sound cliche, however as a leader, if you prioritize secure initiatives, that mentality will trickle down to your reports.
- **Clearly Outline Policies:** Protocols should be clearly and regularly explained and reviewed to employees, to secure buy in. Also, clear documentation and ease of reference can lead to less questions.
- **Encourage Feedback:** Employees should feel comfortable speaking up if they see potential security incidents — without worrying about repercussions.

Effective Training Programs

Olympic athletes spend their entire lives preparing for a once-in-a-lifetime opportunity by rigorously and r egularly training, creating strong routines. Similarly, effective cybersecurity training programs should cover the core fundamental security practices, including password management, how to recognize phishing attacks and safe internet usage. These programs should be tailored based on employee rule and it should include hands-on exercises, so employees can test what they're learning.

Continuous Education and Awareness

Whether it's a relay race or cybersecurity defenses, the game is always changing. Cybersecurity experts are faced with a Catch-22: they have to lay down laws without ever really knowing exactly what they're up against. To keep up, an organization may have to implement refresher courses and improve your security incident detection. This way, businesses can track new threats in real-time and adjust your employee training accordingly.

Advanced Defense Techniques

nothing without their support systems. Take Lebron James, Hall of Fame NBA player for the Los Angeles Lakers. It's reported that Lebron James spends upwards of $3 million annually on just his health, doctors, and nutrition. Athletes leverage the best sports doctors and coaches to get the best results. In parallel, layered security architectures can safeguard you from the most sophisticated threats. Here are some examples:

- **Perimeter Defenses:** In addition to firewalls, you can strengthen your network perimeter with intrusion prevention and intrusion detection systems (IPS and IDS).
- **Internal Traffic:** Segment and monitor your networks for anomalies for more secure internal communication.
- **Endpoint Checkpoints:** Anti-malware and endpoint detection and response help you monitor individual devices for security.
- **App Security:** Better coding practices, reviews, and application firewalls keep your apps safe.

Threat Detection and Response

When an athlete gets a twinge in their leg during an intense workout, they have to assess whether that twinge is a warning sign of a potential injury or just a normal reaction to the movements. This analogy is not unlike a cybersecurity team's assessments.

Security information and event management systems (SIEM) and endpoint detection and response (EDR) are both industry standards that can help you identify and mitigate attacks in real-time. SIEM tools both collect and analyze data from different sources to detect incidents. EDR solutions can provide more visibility into devices, so it is easier to spot anything from anomalous behavior to unprotected systems in individual devices.

In addition to threat detection methodologies, regardless of tactics, organizations of all sizes need robust incident response plans in place to reduce the impact of a breach. Your team should be empowered to respond quickly according to your response framework.

Encryption and Data Protection

From injury to illness, an Olympic athlete's training and progress can be derailed in the matter of seconds by multiple threats. That is not unlike a majority of businesses as corruption, hacking and accidental loss can expose your sensitive data to several external factors.

With better encryption and recovery, you can stave off data theft and quickly recover critical information from other sources. For example, you might use duplicate machines in case your primary equipment is lost in a natural disaster.

Strong encryption algorithms and airtight data loss prevention systems prevent unauthorized access, protect encryption keys, and prevent unauthorized data transfer. Just as an athlete wouldn't reveal their game-day strategies, cybersecurity teams shouldn't have to give anything up either.

Incident Response and Recovery

Strong encryption algorithms and airtight data loss prevention systems prevent unauthorized access and unauthorized data transfers, while protecting encryption keys. Just as an Olympic athlete would not reveal their game-day strategies to the competition, cybersecurity teams should not reveal strategies.

- **Prepare:** Hone your training, tools, and procedures to ensure you can detect even the smallest threats or anomalies.
- **Detection:** Better vulnerability management and assessment can help you understand the real-life consequences of any threats that spring up.
- **Mitigation:** Containing, removing, and recovering are the only ways to mitigate the impact of the threat and restore your operations.
- **Review:** You should review both the incidents and responses to spot the lessons from the interactions and improve defenses from there.

Threat detection is a careful balance: you don't want to spend too much time in the weeds, or you're liable to miss the big picture. The best thing you can do is consistently assess your evaluations for accuracy so you're better able to spring back into action.

Ready to Go for Gold in Cybersecurity?

Just like Olympic athletes push their limits to stand atop the podium, your organization can achieve champion-level cybersecurity with the right training and strategy. Let Dataprise be your coach in the race against cyber threats.

Contact us today at 1.888.519.8111 to craft your gold-medal defense and ensure your data stays secure on the world stage!