SALT TECH
Cyber Security Intelligence: Reality & Defense

NOVEMBER 12, 2021 / EDUCATION

Cyber Security Intelligence: Reality & Defense

As technology continues to advance, cyber security threats are becoming more prevalent. With the rise in cyber attacks, mobile devices, and cloud computing, employees are more vulnerable than ever before.

The reality of cyber security threats is that most organizations will never be completely protected from all possible attacks.

However, it is crucial to educate your workforce about the risks involved with using technology. This means companies need to take action to protect themselves against cyberattacks, including educating employees on what constitutes a threat and how to prevent them from happening.

What should organizations look for in a security solution? Why is it's important to understand the reality of cybersecurity threats? How should organizations approach the issue?

First, we should know what cyber threats are.

What Are Cyber Threats?

SPY
VIRUS
DATA
CYBER

Cyber threats are the vulnerabilities to a computer, network, or information system that an attacker may exploit to gain access and cause harm. Cyber threats can take many forms, including viruses, malware, phishing, and spam.

The definition of a cyber threat is broad because it refers to hacking attempts and any computer-related breaches like data theft or unauthorized use.

They are a significant concern for most organizations as the threats can often come in the form of cyberattacks, which both criminal groups and state actors can initiate.

Also, it's not just hackers who pose a risk to organizations; insiders also pose a significant threat. An insider attack occurs when someone within an organization uses their legitimate credentials to access systems or networks without authorization.

Although many organizations work to make themselves secure, they often fail because of a lack of information about what is happening on their networks. A cyber threat can be anything from a discovered exploit shared with the public or even something as simple as malware infection.

The most important thing is understanding how these threats are carried out to prevent them before it's too late and stop hackers from infiltrating your system for personal gain.

Why Is Cyber Threat Intelligence Important?

Organizations need to educate themselves on cyber threat intelligence in order to protect their networks from any potential cyber threats. It helps to understand their vulnerabilities and find ways to prevent hackers from taking advantage of them.

For example, if you have an employee who works remotely, you must ensure that they are aware of the risks associated with working outside the office.

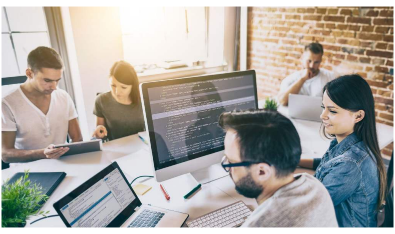
Cyber threat intelligence is crucial to combat cyber attacks and understand the threats that exist effectively. Without understanding security vulnerabilities, indicators of compromise, and how threats are carried out, it is impossible for organizations to detect them in real-time or develop effective defenses against them.

The most significant benefit of investing in real-time cyber threat intelligence is detecting threats earlier than ever before. By using this technology, organizations can quickly spot malicious activity and block it before it spreads further. This allows them to mitigate the impact of an attack and reduce its severity.

It also significantly reduces the cost of cyberattacks as organizations will be able to identify new threats before they become widespread. In addition, the more time spent identifying threats means less time spent dealing with damage once they do occur.

There are several reasons why organizations need to invest in cyber threat intelligence.

Who Can Benefit From Cyber Threat Intelligence?



Employees concerned about security would want to learn more about how to protect themselves. This would help organizations in assessing the risk of potential threats, prevent data breaches, and react accordingly.

It is important to know that cyber threats can be mitigated by implementing best practices, but it's also vital to stay up-to-date on current trends in cybersecurity intelligence. In reality, it adds value across security functions for organizations of all sizes.

Threat intelligence is not just for the elite. It's actually a broad category of information that can benefit almost anyone in any employee role or organization size. For instance, cyber threat intelligence has been used by marketing teams to gain insight into what personal data they need to protect their customers and identify whether it would be worth spending money on cybersecurity solutions like encryption software.

It provides an effective way for security teams to prioritize vulnerabilities to reduce the time it takes, lowering costs and improving their effectiveness. With threat intelligence, vulnerability management teams can more accurately prioritize the most critical vulnerabilities that are at risk of being exploited by cyber attackers.

It is a cost-effective strategy because companies don't have to pay as much when they can rely on information from multiple sources instead of having only one source with limited data available about potential threats.

Situational Cyber Security Awareness

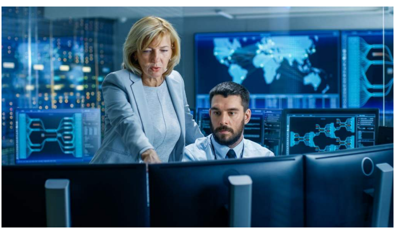
Cyber-security situational awareness is a challenge because of the diverse and expansive networks that make it difficult for IT to protect all devices with sophisticated software.

Therefore, continuously assessing the environment, understanding the changing nature of the threat, and developing a strategy to mitigate risk effectively means that you'll always be ahead of the game. You'll never miss anything if you're constantly monitoring your network and looking for suspicious activities. You'll be able to see patterns and anomalies that may indicate a breach is imminent.

This is especially true for large organizations where it's challenging to keep track of everything that happens on the network. Threat intelligence helps you monitor every aspect of your infrastructure.

The goal for cybersecurity situational awareness is to conduct a comprehensive threat analysis that can help identify potential risks within an organization's IT infrastructure. The best practices for cyber security are managing risks, developing a resilient strategy, and staying vigilant on your network to avoid any attacks from happening.

Excel on How You Handle Incidents



If you don't know what to do next or how to prepare, we will be organizing a cyber security basic practitioner program whereby we share our knowledge and experience on how you can protect your organization from cyber-attacks.

We will discuss the importance of keeping abreast of new developments in cyber security and provide tips and strategies on how to prevent such incidents from occurring.

FREE CYBER SECURITY BASIC PRACTITIONER* PROGRAM

✅Fully Funded Prog under Penjana HRDF initiative Under IR4.0.

✅Limited to 25 participants/ session only.

✅Open for all [Working Malaysians Only].

✅4 days program in Penang.

✅Breakfast, Lunch & Tea Breaks provided throughout the 4 days program duration.

✅Certificate will be given after the completion of the program.

✅Bring your OWN Laptop💻.

📅 18 Nov to 21 Nov 2021

📍 Penang Island

⏰ 9 am to 5 pm

✔ Physical class.

✔ Strictly adhere to SOP (25 pax/session).

✔ First-come, first-served basis only.

Check out our previous event :

https://youtu.be/y-i8oRxI_Dc

More inquiry – CONTACT/WHATSAPP us at 📲 012-528 8582

Click the link below to register:

https://bit.ly/CS18Nov

TALK TO US

Related Posts

Top 3 Eye-Catching CNY Commercial Video Ads

JANUARY 28, 2022

Top 3 Eye-Catching CNY Commercial Video Ads

SALT TECH, Your Partner in Virtual Events

JANUARY 14, 2022

SALT TECH, Your Partner in Virtual Events: Make It Easier and More Cost-Effective With Technology

SALT TECH x AVANSER
Announcing Our Strategic Collaboration Between SALT TECH & AVANSER

DECEMBER 31, 2021

Announcing Our Strategic Collaboration Between SALT TECH & AVANSER

Feeling virtual with Virtual Reality (VR) and Augmented Reality (AR)

NOVEMBER 26, 2021

Feeling Virtual With Virtual Reality and Augmented Reality

SALT TECH

Want To Work With Us

enquiry@salttech.my

+604-2913088

+011-17226988

+6017-853 4188 (Whatsapp only)

Be Part Of Us

Web Developer Senior Executive

Digital Marketing Senior Executive

E-Commerce + Digital Marketing Executive

Sales & Marketing Executive

Internship

Our Office

PENANG

No 16, 2nd Floor, Lebuh
Bishop, 10200 Georgetown,
Penang

KUALA LUMPUR

B-3-1, Northpoint,
Mid Valley City,
No. 1, Medan Syed Putra
Utara,
59200 Kuala Lumpur,
Malaysia.

Copyright©2021 | Salt Tech Solutions Sdn. Bhd. (1396089-K)