Staying Current with Latest Cybersecurity Trends of 2022

Security is one of the significant aspects of today's world. Threats and breaches have become the new normal due to hacks or industrial espionage. As companies double down on security, productivity is restricted, and various challenges crop up. DevOps and other processes which foster collaboration have their fair share of challenges as the renewed focus on security bogs down productivity with tight and restrictive security controls.

With time of the essence, companies have adopted DevSecOps. With security as its middle name, DevSecOps is one of the approaches which most companies rely upon. DevOps is a term you might have heard even if you actively follow the IT trends.

While waterfall kept every department in various siloes, DevOps, which took cues from the agile production approach, paved the way for collaboration and quality deliverables. Agile and DevOps are siblings as there aren't many distinctive traits. While agile has its

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

eyes on production alone, DevOps focuses on delivering the products with automation ingrained in its products.

Useful link: Waterfall Vs. Agile Vs. DevOps

Harnessing the values of agile and DevOps, DevSecOps has set out to better the scenario by dealing with security concerns. Traditionally, a product is built entirely, and then security is bolted or integrated at the end-stage. This shunting process doesn't go well with the product, and it is not the perfect approach to proceed with as security won't be adequately integrated. As a result of this improper execution, there is a high chance that your solution possesses gaping holes, which would be a potential inlet for hackers and saboteurs.

To avoid these embarrassments, DevSecOps has introduced a change that reimagined the development and production processes. Instead of reinforcing the product with security at the end stage, DevSecOps perpetuates the approach that security should be ingrained at every crucial stage. This careful integration allows the developers and operational staff members to rectify crucial errors and close the gaps as a stitch in time saves nine.

The DevSecOps process is favored by most for its advantages as cybersecurity incidents have shot up exponentially. Be it ransomware attacks or flaws in the source code; threat actors are finding new methods to overcome the security mechanisms of a product and a company. While the incidents may not be significant, the shock significantly stunts a company's morale, productivity, and reputation.

Useful link: Pros and Cons of DevOps Methodology and its Principles

---

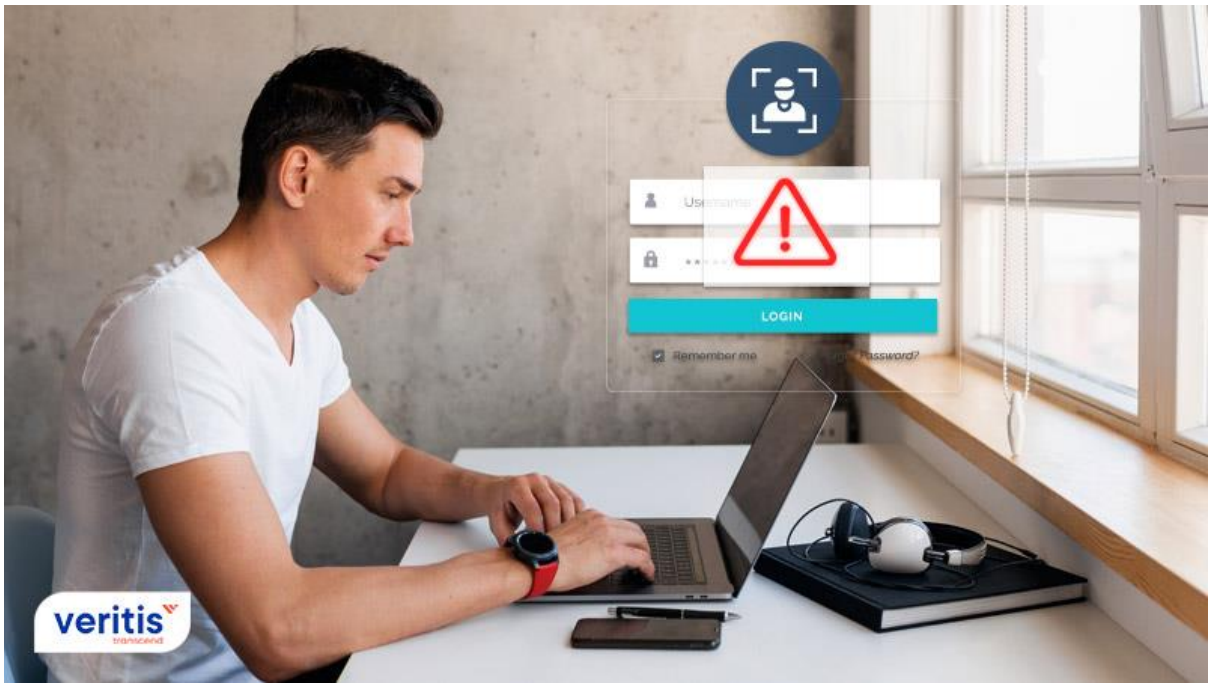
As the year kicked off, we predicted that there would be an increased focus on security due to the increasing undesired cybersecurity crimes. Mid-way through the year, we realized the prediction has come true as people have a higher appetite for automated security practices and managed security services. Also, one should acknowledge the

possibility that production methodologies are not the solution for every security issue. Some of them need an MSP or a change in attitude at an individual level.

While MSPs' are the go-getters who stay atop the game, it is tough to keep up with the changing trends in the IT arena.

This blog will explore the latest things we ought to watch for in the IT Cybersecurity arena.

Work from Home Vulnerabilities



Let's face it. Most, if not all, have unencrypted broadband connections in our homes. While you may think it is not a big deal, this is an easy target for hackers. Therefore, it is always wise to employ a strong VPN connection to shield you from attacks.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

What underscores this observation is the Gartner finding which observed that 60% of the surveyed workforce are working remotely, and 18% of them shall not head back to the office environment.

These findings outpoint how branched out our workforce has become after the pandemic, and due to the paradigm shift in the working culture, the infrastructure is spread out. Be it access or increased reliance on public cloud usage; there is a greater chance of attacks from these ‘surfaces.’

One should go the extra mile to ensure that there is no stone left unturned regarding security. Be it monitoring or MFA; the companies should not only enforce those mechanisms. Still, they should also educate their employees about the existing threats rather than forcing them to go through age-old security courses annually.

Weak Identity Systems

Identity systems are supposed to keep the threat actors. However, if the best defense crumbles away, then the inevitable happens. Be it SolarWinds or the recent hacks that brought forth the misuse of credentials.

Be it due to the carelessness of an employee or due to the mismanagement of the company; identity systems are meant to be bolstered by the internal support of an organization. One should consider changing passwords from time to time, especially after an employee resigns from the organization. While there is room for innovation on this front, the companies will have to be vigilant for now until better security solutions emerge.

Crippling Attacks on Supply Chains

Supply chains are one of the most favored targets as crippling them sends in a shockwave and as the attacked company contemplates meeting the hackers demands to regain control of its operations.

Echoing this observation is Gartner's prediction that 45% of companies will have experienced a software supply chain attack by 2025. This is quite disturbing as the percentile has tripled when compared to 2021.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

One can fend off these attacks by fortifying their infrastructure by roping in an MSP such as Veritis to unearth the flaws and better the security posture against potential attacks.

Useful link: [DevOps vs DevSecOps: Approaches Which Amplify Automation and Security]

Consolidation

The myriad of features and services are bamboozling many. To address this issue, cloud providers are bundling the features and security tools into their services. All may not like this, as some prefer to select their tools and negotiate with the MSP.

The bundling does negotiate the user's power to negotiate, but the complexity is reduced as all the tools would be compatible with each other due to the consolidation. Nevertheless, this trend is picking pace, and one can expect this to gather higher momentum as time passes.

Rise of Cybersecurity Mesh

A contemporary framework for security infrastructure called the cybersecurity mesh enables scattered enterprises to expand and deliver protection where it is most required.

By implementing the cybersecurity mesh infrastructure, businesses would, according to Gartner, would minimize the cost role of personal security events by an average of 90% by 2024.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

Decentralization of Security Decisions

To realize the goals of the digital company, executive executives want a quick and agile cybersecurity role. The work is growing too enormous for a centralized CISO post, though, as more company functions go digital.

As a result, leading businesses are creating CISO offices to support dispersed cyber judgments.

While cybersecurity executives are positioned in various corporation sectors to decentralize security choices, the CISO and the centralized function will still oversee setting policies.

Useful link: **Top 10 DevOps Tools to Pick for Your Business**

To Err is Human

Human errors are one of the causative factors of unwanted cybersecurity incidents, and these instances are rising. However, one cannot entirely blame the employees as companies worldwide don't educate their employees on the rising security risks. Companies need to upskill their employees on the security front by providing them with time-appropriate learning material and drills.

Final Thoughts

The world's ever-evolving and new trends will outdate the existing trends and infrastructure. Be its a production process or security, time shall inevitably beckon the change, and it is imperative not to become outdated as time is always of the essence in this fast-paced world.

Most companies focus on productivity and keep innovating by roping in an MSP. Stevie Award winner Veritis is the preferred choice of Fortune 500 and emerging companies. Acknowledged for its DevOps excellence, **Veritis** shall help you better your business

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

and unlock the untapped potential in you. So, reach out to us and stay current with the trends.

Services