Whitepaper

DevSecOps

An Ultimate Defense To Organization's Software Security

VERITIS

INDEX

The Matter of Concern Security Remains a Challenge

Digital transformation has brought about a significant change in the way IT business operates. However, one key concern continues to haunt many organizations in their digital journey i.e. ‘Security!

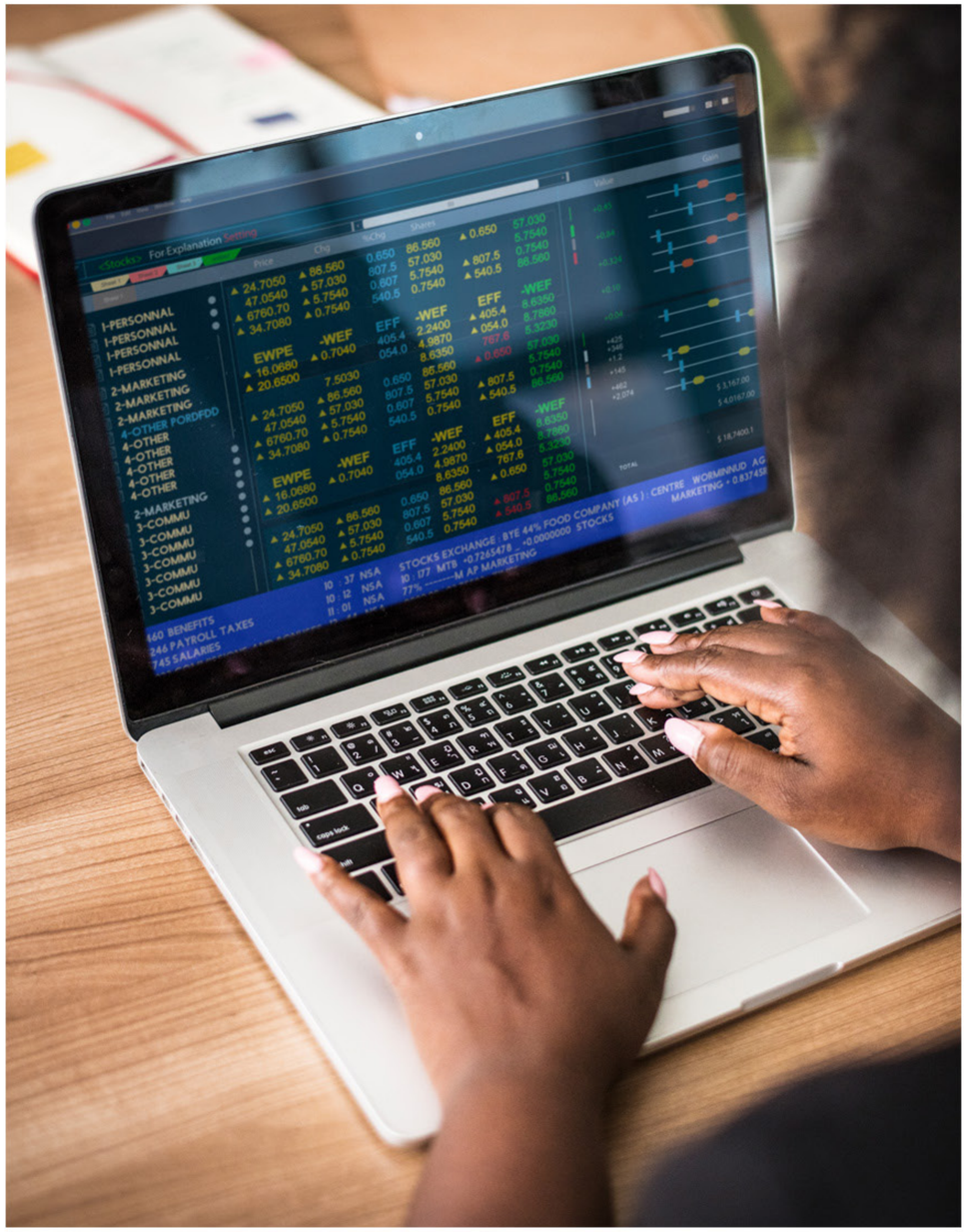
Run for fast-paced service delivery and continuous customer satisfaction often leads to minimized focus on security. But its noteworthy that ‘security is as important as to time-to-market of a product’, and any compromise on this impedes the fast-paced cycle of trade and commerce.

Cybercrimes reported over the period prove this, showing us how essential the security is for a product life cycle.

Its High Time!
Security in Business Strategy

In general, we tend to focus on something only when we feel the dire need of it. Same has been the case with security!

Though history presents many stories on disasters caused by cybercrimes, we still see many firms overlooking security. 2018 formed the recent basis for this fact by reporting severe legal battles and intense loss faced by many firms due to ‘security’ during the year!



‘Where is Security?’

Facebook is a classic example that faced 'questions over security’ when close to 50 million of its users were threatened by a security breach. The security breach took place after hackers attacked APIs for access to information including names, genders and localities of users, says Facebook CEO Mark Zuckerberg.

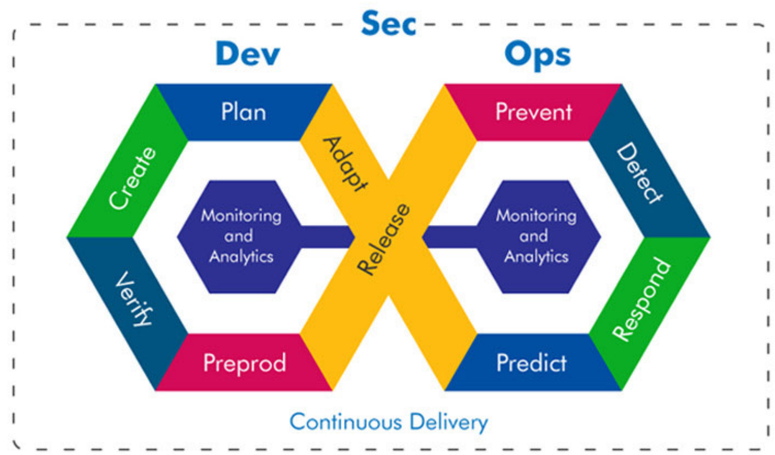
Uber was another victim of security breach that reported the loss close to GBP 133 million in legal settlement, after the firm failed to protect 57 million customer and driver data. Additionally, the transportation network giant had to pay USD 100,000 for hackers to get the stolen data deleted.

Considering many such incidents happening on a larger scale, it is estimated that cybercrime will cost the world over USD 6 trillion per year by 2021.

Given this fact, its high time for companies to rethink on security inclusion in their business strategy to achieve expected goals!

Future of Secure Business... DevSecOps Turns Savior!

Technology advanced to the level of self-defense. This nature of technology is clearly reflected in DevSecOps principles, which strive for ‘security integration’ throughout the product lifecycle.



The DevSecOps Approach!

Most security and compliance tools haven’t been able to keep up with the fast-paced rapid development, making security the biggest obstacle.

Although DevOps has been sought-after for its abilities in improving application build, speeds and driving IT innovation, security remained a challenge. Organizations continued to face data loss, IP theft, business disruptions, increased expenditure and competitive disadvantage.

That’s where DevSecOps arrived as a step beyond DevOps and with a different approach to security!

As an extension to DevOps, DevSecOps secured the collaboration process with security functions that check vulnerabilities and risks at every step of SDLC.

In a nutshell, DevSecOps principles look at security as an integral part of the Software Development Life Cycle (SDLC) and not as a process that comes at the end.

DevSecOps Value Addition to Business

With security integration across the product life cycle, DevSecOps adds some unique value to the business.

- **Cost Reduction:** DevSecOps reduces risks and their losses by identifying and fixing issues early in the development phase, boosting the software development process. According to a report, automated application performance analysis in the ‘Design and Architecture’ (26 percent of the companies) and ‘Development’ stages (52 percent) nullified the chances of security breach and resultant losses for many firms.

- **Increased Security:** DevSecOps uses rigid infrastructure to reduce vulnerabilities, insecure defaults, increase code coverage and enhance automation. In the event of an attack, immutable infrastructure allows companies to tear down the infrastructure and rebuild it with new credentials. This type of infrastructure also favors a shift to the cloud, which eliminates the need for usage of vulnerable hardware.

43 percent of surveyed organizations have adopted infrastructure-as-a-code.

- **Scope for Innovation:** Regular security audits and monitoring helps organizations stay ahead of any hacking attempts. Any suspicious activity can be tackled right away, presenting room for innovation in terms of best security enhancements against cybercrime. 81 percent of respondents reported that they have a cybersecurity incident response plan in place.

- **Speed for Recovery:** Security personnel employ templates or pet/cattle methodology to deal with a security incident. In this methodology, servers are either replaced or nurtured to keep the needs of the business running.

- **Secure by Design:** Automation is driving the success of almost every business. DevSecOps enhances security by using automated security review of code, application security testing, educating and encourages developers to use secure design patterns.

- **Every Individual is responsible:** By harnessing a culture of openness, DevSecOps presents room for enhanced security right from the early stages of development. Better the collaboration, better will be the approach to security measures and enhancements. All the stakeholders' approach and insights can enhance the security firewall against breaches.

Who is Responsible for DevSecOps?

Security: A Collaborative Effort

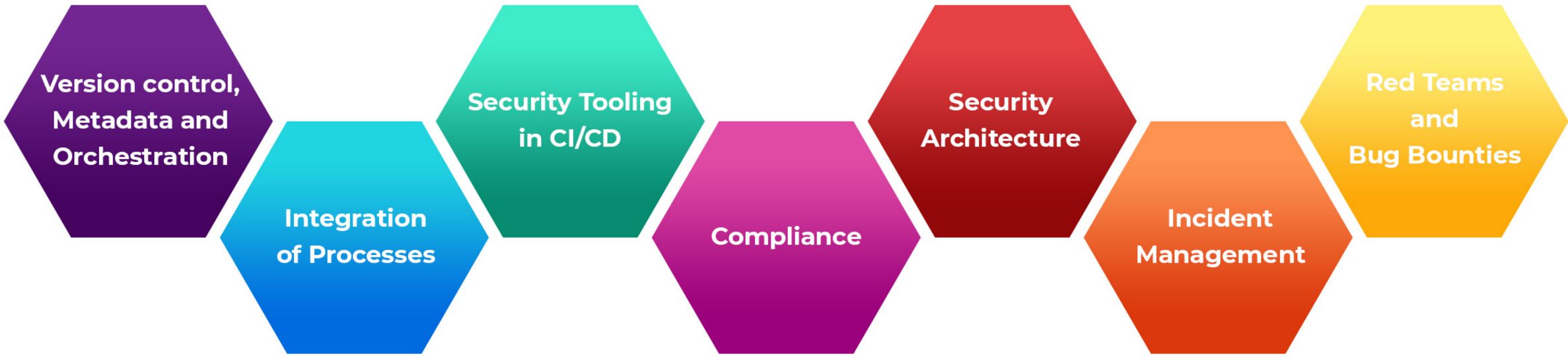
The DevSecOps responsibility is not limited to security personnel alone. It is a collaboration of people and processes including development, operations & security personnel and technology.

People: Security personnel are no more out of the main DevOps process. A succesful DevSecOps strategy brings together every individual along the length and breadth of the organization including Managers, Chief Information Officers, colleagues and peers. This allows security personnel to identify possible loopholes and prepare development and operations professionals accordingly to develop a secure product that improves sales and customer satisfaction. Security personnel training other DevSecOps teammates about the potential risks and safe practices also brings in a culture of safety and utmost quality across the cycle.

Processes: Processes are as crucial as people. They define the effectiveness of the product by ensuring everything and everyone collaborates to deliver quality output.

DevSecOps makes this possible by eliminating the siloed approach of working as individual entities and promotes the culture of collaboration.

Key aspects of DevSecOps process include:

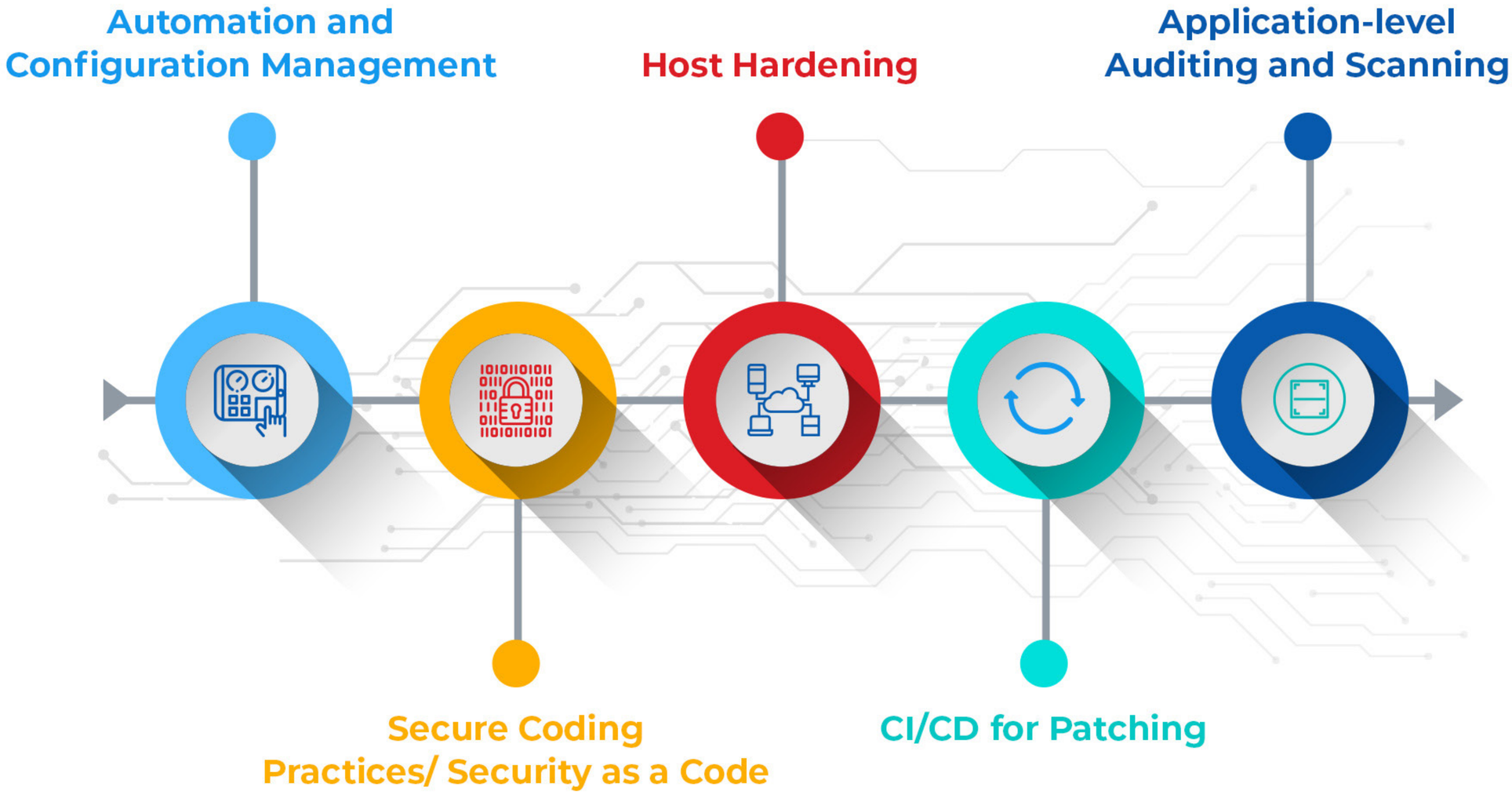


Development and Operations teams maintain a blueprint of past processes, thus saving DevSecOps practitioners the time to recreate projects from scratch. They also help maintain a common reference point within the organization that is accessible to everyone involved and available at any given time.

Similarly, DevSecOps increases the response time to security by making short, feedback-based security loops.

Technologies: Technologies are designed and driven to ensure hassle-free operations.

Following are the key implementations associated with the DevSecOps process:



Government: In 2015, when cyber security became a national alarm with the breaches of US federal agencies- IRS and the Office of Personnel Management, President Obama declared a national emergency against cybercrime.

The US Government announced a major investment of USD 19 million in security following the aftermath!

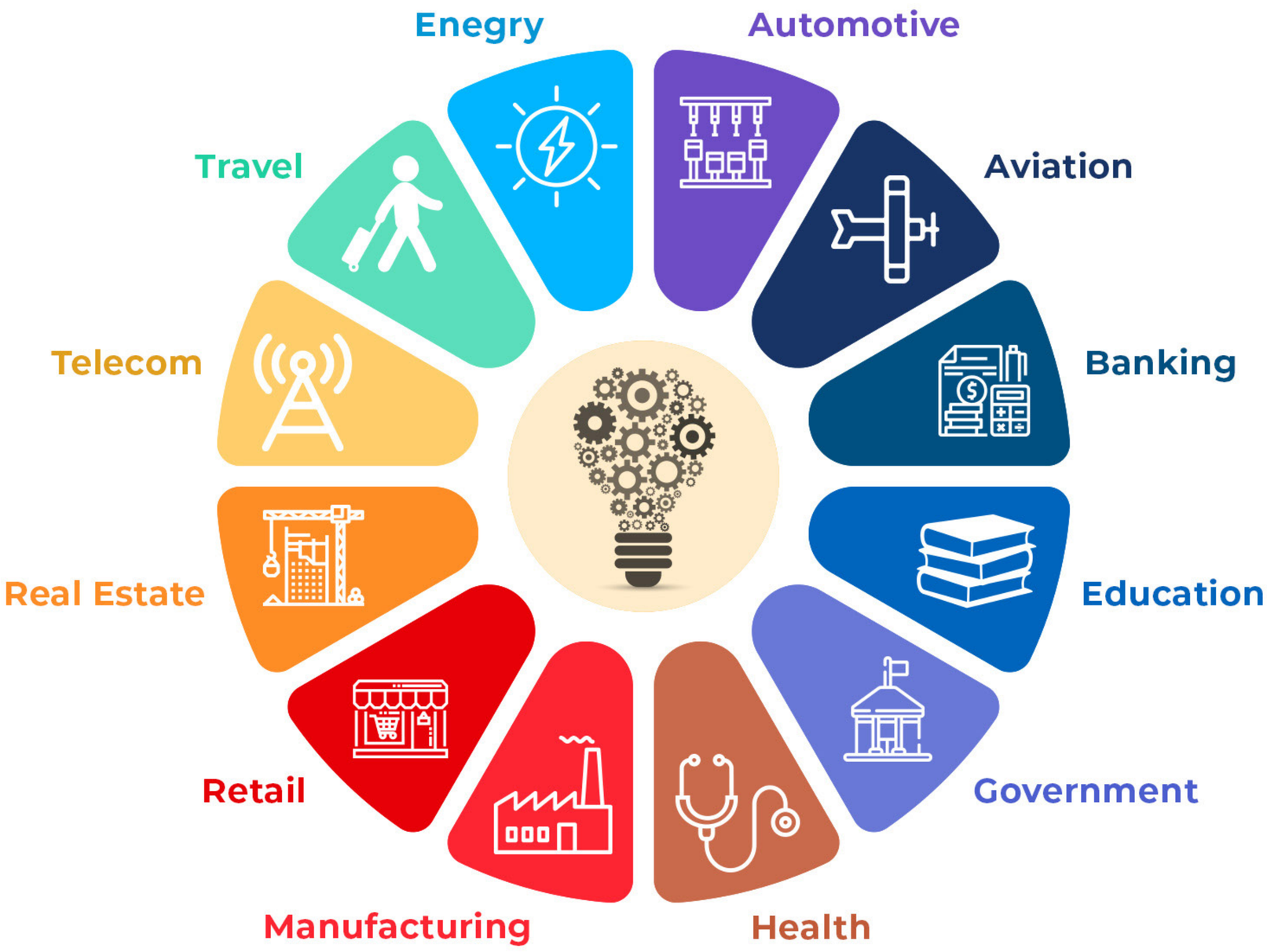
Alongside governments, major businesses have decided to combat cybercrime with increased budgets for cybersecurity including Bank of America, JP Morgan Chase and Microsoft, who announced the annual cybersecurity research and development investment of USD 1 billion.

This scenario shows how important is government's role in combatting cybercrime!

As part of policy initiatives, governments should introduce stringent measures against cybercriminals and take action against organizations that fail to protect customer data. This will pave way for saved costs through better security and security risk management practices.

Industries Benefiting from DevSecOps:

DevSecOps is making its way into following industries that consider security as utmost priority:



DevSecOps Tools And Implementation:

Listed below are the top DevSecOps tools that help enhance the DevSecOps process:

aqua

continuumsecurity

CONTRAST SECURITY

CHECKMARX

IMMUNIO

ca technologies

VERACODE

Dome9 SECURITY

ThreatModeler
• Security Starts Here •

evident.io

GAUNTLT
BE MEAN TO YOUR CODE AND LIKE IT

WhiteSource

DevSecOps Market Share and Growth Up To 2023

The global DevSecOps market is poised to grow from USD 1.5 billion in 2018 to USD 5.9 billion by 2023 at a CAGR of 31.2 percent, driven by the growing need for highly-secure continuous application delivery and the focus on security and compliance.

However, DevSecOps is faced by some challenges including:

- Unavailability of Skilled Professional
- Organizations' Reluctance to Adopt New Tools and Technologies

DevSecOps Trend Forecast (2018-23):

- **Cloud-based DevSecOps:** Cloud-deployed DevSecOps will propel enhanced infrastructure scalability and performance. Cloud deployments help professionals go through the process with improved speed, security and scalability.

  Moreover, DevSecOps practices will reduce operational expenditures by using standardization and automation, while providing complete control in line with user needs.

- **Retail and Consumer Goods Will Hold the Largest Market Share:** The forecast period will observe retailers align their application security processes with cloud-based application development and deployment processes, with a prime focus on security-centered business culture.

A high adoption rate of DevSecOps solutions and services has been observed in the retail sector with a vision of achieving:

- Operational Efficiency and Productivity
- Reliable and Secure IT Environment
- Faster Time-to-Market
- Enhanced Customer Experience

- **APAC to Hold Largest Market Size and High Growth Rate:**
  The Asia-Pacific region is expected to offer immense growth opportunities for DevSecOps during the forecast period.

  Driven by:
    - Advancements in Cloud Computing
    - IT Infrastructure Services
    - Internet of Things (IoT)

  Furthermore, the increasing adoption of cloud technologies, rising demand for business functions, adoption of secure software development and deployment tools will increase significantly in the forecast period.

Global DevSecOps Market: Recent Developments

- In June 2018, leading DevSecOps tool ThreatModeler announced the launch of Threat-Modeling-as-a-Service (TMaaS) solution. TMaaS is a managed solution that aims to transform organizations' cybersecurity and risk management needs using the automated, collaborative threat modeling solution.

- In September 2018, Aqua Security introduced risk assessment controls for server-less functions and container encryption.

- In May 2018, Micro Focus launched the ITOM Platform, which integrates DevOps with AIOps to speed up service delivery across large-scale hybrid IT environments.

Conclusion:

DevSecOps, not only redefines the software development process but also improves product/service quality and efficiency through security.

Mitigated risks and enhanced performance will drive the successes of many businesses to come.

With benefits such as cost reduction, improved security and attack-driven defense, the business redefining process of DevSecOps will give organizations the much-required reputation upliftment and smooth business operations.

While DevSecOps is already writing the success of many businesses, are you still thinking of adoption?

Waste no time further, security is a crucial element to business survival.

Get in touch with Veritis!

Veritis has been among the early DevSecOps service providers and has more than a decade-long experience in dealing with and understanding the pain-points and security challenges of over a 100 organizations including those in the Fortune 500 list.

You could be next!

info@veritis.com

1-877-VERITIS (283-7484)

972-753-0033

US Corporate Headquarters

1231 Greenway Drive

Suite 1040

Irving, TX 75038

India Headquarters

#607, 6th Floor,

Ashoka Bhoopal Chambers,

S P Road, Begumpet

Hyderabad – 500003, India.

Phone no: 040 42211730

For more information, contact info@veritis.com

www.veritis.com