Integrating Technology, Driving Growth

TechTalk

GALAXY
Integrating Technology | Driving Growth

SPEED UP

GALAXY OFFICE AUTOMATION PVT. LTD.

Issue No. 140, February 2024

We are proud to announce that Galaxy has been awarded the prestigious title of

APJ Cloud Partner of the Year

by Checkpoint at CPX Bangkok! This recognition underscores our relentless dedication to pioneering innovation and excellence in security solutions for the cloud.

Galaxy a prominent player in the cloud services sector showcased Cisco's, hyper-converged solutions in an exclusive event. Technology professionals across verticals explored the intricacies of multi-cloud strategies and their impact on businesses, offering a seamlessly managed and supported experience, fostering innovation and accelerating customers' hybrid multi cloud journeys.

MD SPEAKS

Anoop Pai Dhungat
Chairman & Managing Director

Dear Readers,

One of my top picks for technologies that will see widespread adaption during this year was Data Governance. The reason for that is that with Artificial Intelligence becoming more and more relevant and accessible, effective data governance is practically mandatory for navigating the complexities of AI-driven innovation while upholding ethical standards and regulatory compliance. AI algorithms rely on vast quantities of data to generate insights and make decisions. It is imperative that the quality of such data is highly reliable. By prioritizing data quality assurance, privacy protection, ethical data use, and regulatory compliance, businesses can harness the transformative potential of AI technology while safeguarding individuals' rights and welfare of the community in general. As we continue to grab the opportunities and face the challenges of Generative AI, robust data governance practices will serve as the cornerstone of responsible and ethical data management.

At Galaxy, we are at the forefront of bringing these solutions to you. Do reach out to our experts and evangelists to have a conversation around these technologies and how they could help your business.

Happy reading.

Paving the Future: Self-Healing Roads Revolutionize Infrastructure Maintenance

The onset of rains is a good sign for the planet as a whole because water signifies life. However, for the citizens of metropolitan cities, rains can spell disaster. Trains get delayed, as there are so many people using public transport that it seems like every citizens has decided to come out of their houses simultaneously and take a journey. Worst of all, the roads basically become motocross racetracks, making them dangerous and nearly impassable.

Over the years, we have shifted from asphalt to concrete in terms of road-building. Despite that, nothing is resistant to weathering. No matter how well a material is mixed, the concrete will always crack and degrade.

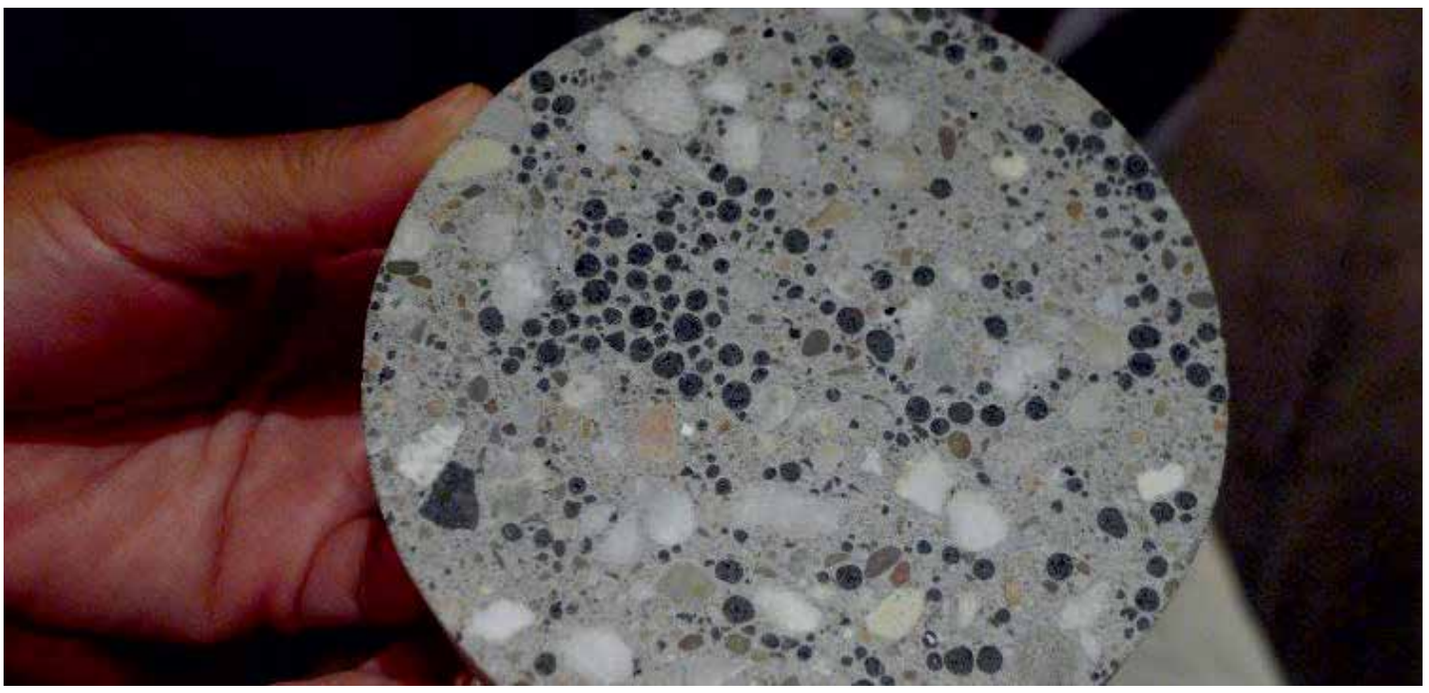
Researchers at the University of Bath, Cardiff University, and the University of Cambridge have created a concrete blend that is full of bacteria hidden in tiny capsules. This healing principle is based on our body's mechanism of healing bones through mineralization. Essentially, researchers tried to employ this same principle to concrete. The concrete was mixed with limestone-producing bacteria and it was observed that the cracks formed in concrete were patched over.

The bacteria, either Bacillus pseudofirmus or Sporosarcina pasteurii, are found naturally in highly alkaline lakes near volcanoes, and are able to survive for up to a staggering 200 years without oxygen or food. These bacteria are triggered as soon as they come in contact with water, using the calcium lactate present in water as a food source, thus producing limestone. The limestone seals up the cracks formed on the roads. The concept is pretty neat, and might be just what we've been looking for all these years.

The bacteria are placed in tiny biodegradable capsules before blending them in with concrete. When cracks develop in the concrete, water seeps in and comes in contact with the capsules. These capsules break, allowing the water to come in contact with the bacteria and its food source (water), thus initiating the healing process. The bacteria then feed on the calcium lactate, blending the calcium with carbonate to form limestone, fixing the crack.

This technology will reduce the overall cost of maintaining the roads by about 50%.

This mixture can also be used to mix in a liquid and be sprayed on buildings, thus protecting these structures from cracks. This will increase the life of concrete buildings and greatly improve public safety, particularly after accidents or natural disasters.



http://tinyurl.com/ytp986pw

Security Operations Center

In a world where cyber threats grow more sophisticated and relentless every day, organizations must adapt and take action to protect their valuable digital assets. Enter the Security Operations Center (SOC), a powerful shield against the constant barrage of cyberattacks. In this engaging and easy-to-read article, we will delve into the world of SOCs and explore what they are, why they are essential for businesses of all sizes, and how they operate to keep your organization safe. Our mission is to provide you with valuable insights that outshine the competition while offering a uniquely human and approachable reading experience.

What is a Security Operations Center (SOC)?

A Security Operations Center, or SOC, is a centralized facility where a team of cybersecurity experts works together to monitor, detect, analyze, and respond to various security incidents within an organization's digital infrastructure. The primary objective of a SOC is to minimize the impact of cyberattacks, protect sensitive data, and ensure the confidentiality, integrity, and availability of your organization's information assets.

Why Your Business Needs a SOC

With cyberattacks becoming increasingly sophisticated and frequent, a SOC is essential for businesses of all sizes. Here's why:

- Proactive Threat Detection: SOCs continuously monitor your organization's network, systems, and applications to identify potential vulnerabilities and detect any signs of malicious activity.
- Rapid Incident Response: When a security incident is detected, the SOC team quickly takes action to contain the threat and minimize damage, ultimately reducing the overall impact on your business.
- Compliance Assurance: By implementing security best practices and industry-standard frameworks, SOCs help your organization adhere to regulatory requirements and maintain compliance with data protection laws.
- Improved Security Posture: The combination of advanced technology, skilled personnel, and well-defined processes in a SOC helps your business maintain a strong security posture in the face of evolving threats.

Key Components of a Security Operations Center

A successful SOC relies on several critical components, including:

- **People:** A SOC team is composed of cybersecurity professionals with various skill sets, such as security analysts, incident responders, threat hunters, and forensic experts. These individuals collaborate to monitor, detect, and respond to security threats in real time.
- **Processes:** Clearly defined processes and workflows are essential for the efficient functioning of a SOC. These processes include incident management, threat detection, vulnerability management, and threat intelligence.
- **Technology:** A SOC employs a variety of advanced security tools and technologies to monitor and analyze vast amounts of data. These tools include Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), firewalls, endpoint protection platforms, and threat intelligence feeds.
- **Threat Intelligence:** SOC teams use threat intelligence to stay up-to-date on the latest threat actors, attack techniques, and vulnerabilities. This information allows them to proactively identify and respond to potential threats before they can cause significant harm.

Types of Security Operations Centers

There are various types of SOCs, each with its advantages and drawbacks:

- **In-house SOC:** An organization builds and operates its own SOC, employing a dedicated team of cybersecurity professionals. This approach offers complete control over security operations but can be resource-intensive.
- **Outsourced SOC:** A third-party provider monitors and manages an organization's security. This can be a cost-effective solution for businesses with limited resources or expertise but may result in less control and visibility into security operations.

- **Hybrid SOC:** This model combines the benefits of both in-house and outsourced SOCs. Organizations maintain an internal SOC team while leveraging an external provider's expertise and resources. This approach offers a balance between control, cost, and access to specialized skills.

Building a Successful Security Operations Center

To build a successful SOC, consider the following best practices:

- **Define clear objectives:** Establish the goals and objectives of your SOC based on your organization's unique needs, risk tolerance, and regulatory requirements. This will help you design and implement an effective security strategy.
- **Assemble a skilled team:** Hire experienced cybersecurity professionals with diverse skill sets, including security analysts, incident responders, and threat hunters. Invest in ongoing training and development to keep your team's skills up-to-date.
- **Implement robust processes:** Develop and document well-defined processes for incident management, threat detection, vulnerability management, and threat intelligence. Continually review and refine these processes to ensure optimal performance.
- **Leverage advanced technology:** Deploy a range of security tools and technologies, such as SIEM systems, XDR, firewalls, and endpoint protection platforms. Regularly update and fine-tune these tools to ensure they remain effective against evolving threats.
- **Foster a strong security culture:** Promote a security-first mindset throughout your organization by providing regular security awareness training, encouraging collaboration between teams, and rewarding proactive security behaviors.
- **Measure SOC performance:** Establish Key Performance Indicators (KPIs) to measure the effectiveness of your SOC. Monitor these KPIs closely and use them to identify areas for improvement.
- **Continuously improve:** Regularly review and assess your SOC's performance, and make necessary adjustments to address any gaps or weaknesses. Stay abreast of industry trends and best practices to ensure your SOC remains at the forefront of cybersecurity.

The Future of Security Operations Centers

SOCs must adapt and innovate as cyber threats evolve to stay ahead of the curve. Emerging trends and technologies that will shape the future of SOCs include:

- **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML can augment human analysts by automating routine tasks, analyzing vast amounts of data, and identifying patterns that may indicate a cyber threat. This allows SOC teams to focus on higher-level strategic activities and respond more effectively to incidents.
- **Extended Detection and Response (XDR):** XDR platforms consolidate and correlate data from multiple security tools, providing a holistic view of an organization's security posture. SOC teams can detect and respond to threats more quickly and efficiently.
- **Cloud-based SOCs:** As more organizations move to the cloud, the need for cloud-based SOCs will grow. These SOCs must be designed to secure cloud-native applications, infrastructure, and data while maintaining the cloud's flexibility and scalability.
- **Cyber Threat Intelligence Sharing:** Collaborating with industry peers and sharing threat intelligence helps SOCs stay informed of emerging threats and respond more effectively to attacks.

Conclusion

A Security Operations Center (SOC) is critical to any organization's cybersecurity strategy. By combining skilled personnel, robust processes, advanced technology, and a proactive approach to threat detection and response, SOCs help enterprises maintain a strong security posture in the face of ever-evolving cyber threats. Organizations can better protect their digital assets and ensure business continuity by understanding the key components, types, and best practices for building a successful SOC. As the cybersecurity landscape continues to change, SOCs must adapt and evolve to remain at the forefront of enterprise security.

http://tinyurl.com/4etv6kj5

The Rise of Hybrid and Multi-Cloud Computing

The rise of hybrid and multi-cloud computing is a significant trend in the IT industry. These strategies offer several benefits that can help businesses to improve their flexibility, resilience, scalability, and cost savings. Galaxy works with customer in defining the right strategies and partner in journey of adopting hybrid and multi cloud.

Overview of Hybrid cloud and Multi-cloud computing.

- **Hybrid cloud computing:** Hybrid cloud computing combines public cloud and onpremises infrastructure. This allows businesses to take advantage of cloud computing and on-premises infrastructure benefits. For example, companies can use the public cloud for elastic computing and storage resources and on-premises infrastructure for sensitive data or applications requiring low latency.
- **Multi-cloud computing:** Multi-cloud computing is the use of multiple public cloud providers. This allows businesses to get the best features and pricing from different providers. For example, a company might use AWS for compute resources, Azure for storage, and Google Cloud Platform for machine learning services.Here are some of the latest trends in hybrid and multi-cloud computing, Galaxy provides solution to customers for below trends:

- **The rise of edge computing:** Edge computing is a distributed computing model that brings computing resources closer to the end user. This can improve performance andreduce latency for applications that require real-time processing. Hybrid and multicloud computing can be used to deploy edge computing solutions.
- **The growth of containerization:** Containerization is a technology that allows applications to be packaged and deployed standardized. This can make it easier to move applications between different cloud providers. Hybrid and multi-cloud computing can be used to deploy containerized applications.
- **The adoption of artificial intelligence (AI) and machine learning (ML):** AI and ML are becoming increasingly crucial for businesses. These technologies can automate tasks, improve decision-making, and personalize experiences. Hybrid and multi-cloud computing can be used to deploy AI and ML solutions.

The benefits of hybrid and multi-cloud computing

There are many benefits to using hybrid and multi-cloud computing. These benefits include:

- **Flexibility:** Hybrid and multi-cloud computing allows businesses to choose the right cloud solution. This can help businesses to save money and improve performance.
- **Resilience:** Hybrid and multi-cloud computing can help businesses improve their strength in outages and disasters. By spreading their workloads across multiple clouds, companies can reduce the impact of an outage on their operations.
- **Scalability:** Hybrid and multi-cloud computing can help businesses to scale their IT infrastructure as needed. This can help businesses to meet the demands of growth and changing business needs.
- **Cost savings:** Hybrid and multi-cloud computing can help businesses save on IT costs. Companies can choose the right cloud provider and negotiate better pricing.

How to choose the right hybrid or multi-cloud strategy for your business

- Your business needs and requirements
- The type of applications you need to run
- The level of security and compliance you need
- Budget and Pricing
- The features and services offered
- The level of support offered
- The security and compliance measures in place

Hybrid and multi-cloud computing offer several benefits for businesses of all sizes. If you are considering adopting a hybrid or multi-cloud strategy, please reach out to trusted partners like Galaxy in adopting hybrid cloud or multi cloud journey. To talk to our experts, email us at **marketing@goapl.com**

Tech News

Union Budget 2024: Tech industry upbeat

The unveiling of the 2024 Union Budget has been met with widespread acclaim from industry leaders, particularly for its focus on innovation, digital infrastructure, R&D, and skill enhancement.

"The introduction of the Rs 1 lakh crore corpus, along with 50-year interest-free loans for the private sector to boost research in sunrise domains, marks a significant stride towards unlocking the potential of innovation.," Arun Balasubramanian, VP & MD, India & South Asia, UiPath, stated. He also emphasized the importance of equipping the youth with skills in AI, automation, and robotics.

The recently introduced National Deep Tech Startup Policy (NDTSP) acts as a roadmap for building a supportive ecosystem for start-ups. Moreover, in the interim Budget 2024-25, the Union Minister has announced a new scheme for strengthening deep-tech technologies for defense, which will further promote the growth of indigenous manufacturing in the country.

Beerud Sheth, Co-founder and CEO, Gupshup.io, and Sandeep Dutta, Senior Managing Director and Lead - India Business, Accenture, both recognized the budget's potential to spur innovation and entrepreneurship. Sheth applauded the 1-lakh crore corpus for interestfree loans towards R&D as "a very progressive move," while Dutta highlighted the budget's commitment to sustainable and inclusive development.

Gopichand Katragadda, President - Institution of Engineering and Technology (IET), called for effective execution of deep-tech-related funds. He also stressed the need for industry adaptation to value diploma holders and foster gender diversity in the workforce.

http://tinyurl.com/5n7uae7f

GenAI to contribute $100 bn in healthcare savings in APAC by 2025

Generative AI (GenAI) will free up to 10% of clinicians' time, translating into an estimated $100 billion in annual healthcare savings in Asia/Pacific excluding Japan (APEJ) by 2025, to realize more workflow automation and efficiency.

By the end of 2027, driven by the demand to scale hyper-personalised patient experiences, improve collaboration, and foster equity, 60% of Asia/Pacific healthcare organizations will double GenAI investments, according to an IDC report.

GenAI is emerging as a transformative force in healthcare and is set to impact workforce efficiency and hyper-personalisation in the care processes. "With the advent of GenAI and the need for consumerization of care, the next five years are set to be the defining period for the healthcare sector, and we are currently at the starting point of this exciting journey," said Manoj Vallikkat, senior research manager, healthcare insights, IDC Asia/Pacific.

Driven by the need for improved diagnostic accuracy, speed, and workflow efficiency, care providers in Asia/Pacific will see a 60% increase in AI solution adoption by 2026. By 2027, 50% of the healthcare industry in Asia/Pacific will leverage GenAI to address data and workflow fragmentation across care settings to improve diagnosis and patient safety to scale care anywhere, the report mentioned.

By 2026, a doubling of hospital-at-home patients will propel a 55% growth in investments in tech-enabled integrated care initiatives to address patient safety, workforce, and care access concerns in Asia/Pacific.
"In the healthcare sector, the unique risks associated with AI are significant, which necessitates a greater focus on explainability and data security," added Vallikkat.

http://tinyurl.com/4nwn35kc

A-23/24, Ambika Towers, Ground Floor,
Off. Jijamata Road, Nr, Pump House,
Andheri (E), Mumbai - 400 093, India.

91-22-42187777
marketing@goapl.com
www.goapl.com