Integrating Technology, Driving Growth

TechTalk

GALAXY Integrating Technology | Driving Growth

GALAXY OFFICE AUTOMATION PVT. LTD. Issue No. 119, May 2022

Galaxy & VMware showcased "Ways to achieve Zero Trust Security" at Data Center Summit

Galaxy & VMware were platinum sponsors of the 11th Edition Datacentre Summit & Awards 2022 organised by UBS Forums, where 200+ senior IT professionals converged for a day long seminar covering varied subjects such as the shifting landscape of datacentres and the best techniques for keeping them relevant to changing business settings.

MD SPEAKS

Anoop Pai Dhungat
Chairman & Managing Director

Dear Readers,

Over the past couple of years we saw companies rapidly adopt digital ways of doing business due to the lockdowns that absolutely prevented the erstwhile physical methods. Secure work from anywhere solutions were implemented, cloud migrations happened and a lot of projects that were previously delayed due to lack of initiative or budgetary constraints were taken up. Necessity, indeed, is the mother of not only invention but in this case implementation of innovative solutions also. The current energy crisis in Europe due to the over dependence for oil, gas and coal from Russia should trigger a push towards renewable energy sources and move away from the polluting hydrocarbons. Given the extreme weather fluctuations being experienced all over the globe, this is long overdue. That may be the only good that comes from this horrible situation that ordinary people have to suffer in the clash of the titans.

This year we have added a lot more productivity and IT modernisation solutions to our portfolio. Please call us to find out more about how we can help your digital transformation in the Galaxy way. At Galaxy, we believe that true digital transformation is not just converting existing processes to use the latest digital technologies but to re-imagine and re-create processes, products and new offerings using the currently available technologies.

Stay safe and happy reading.

APDhungat

Future Is Now

A new scientific device creates electricity from falling snow

UCLA researchers and colleagues have designed a new device that creates electricity from falling snow. The first of its kind, this device is inexpensive, small, thin and flexible like a sheet of plastic. "The device can work in remote areas because it provides its own power and does not need batteries," said senior author Richard Kaner, who holds UCLA's Dr. Myung Ki Hong Endowed Chair in Materials Innovation. "It's a very clever device — a weather station that can tell you how much snow is falling, the direction the snow is falling, and the direction and speed of the wind."

The researchers call it a snow-based triboelectric nanogenerator, or snow TENG. A triboelectric nanogenerator, which generates charge through static electricity, produces energy from the exchange of electrons. "Static electricity occurs from the interaction of one material that captures electrons and another that gives up electrons," said Kaner, who is also a distinguished professor of chemistry and biochemistry, and of materials science and engineering, and a member of the California NanoSystems Institute at UCLA. "You separate the charges and create electricity out of essentially nothing." Snow is positively charged and gives up electrons. Silicone — a synthetic rubber-like material that is composed of silicon atoms and oxygen atoms, combined with carbon, hydrogen and other elements — is negatively charged. When falling snow contacts the surface of silicone, that produces a charge that the device captures, creating electricity. "Snow is already charged, so we thought, why not bring another material with the opposite charge and extract the charge to create electricity?" said co-author Maher El-Kady, a UCLA assistant researcher of chemistry and biochemistry. "While snow likes to give up electrons, the performance of the device depends on the efficiency of the other material at extracting these electrons," he added. "After testing a large number of materials including aluminum foils and Teflon, we found that silicone produces more charge than any other material."

About 30 percent of the Earth's surface is covered by snow each winter, during which time solar panels often fail to operate, El-Kady noted. The accumulation of snow reduces the amount of sunlight that reaches the solar array, limiting the panels' power output and rendering them less effective. The new device could be integrated into solar panels to provide a continuous power supply when it snows, he said. The device can be used for monitoring winter sports, such as skiing, to more precisely assess and improve an athlete's performance when running, walking or jumping, Kaner said. It also has the potential for identifying the main movement patterns used in cross-country skiing, which cannot be detected with a smart watch. It could usher in a new generation of self-powered wearable devices for tracking athletes and their performances. It can also send signals, indicating whether a person is moving. It can tell when a person is walking, running, jumping or marching. The research team used 3-D printing to design the device, which has a layer of silicone and an electrode to capture the charge. The team believes the device could be produced at low cost given "the ease of fabrication and the availability of silicone," Kaner said. Silicone is widely used in industry, in products such as lubricants, electrical wire insulation and biomedical implants, and it now has the potential for energy harvesting.

https://bit.ly/3yHMtp1

Offensive and defensive cybersecurity: which approach will you take?

Cybersecurity is becoming a more important business requirement. The cybersecurity specialist's duty of keeping corporate and personal data safe is affecting more people than ever before as technology becomes more integrated with the professional and personal lives. Professionals in the field of cybersecurity are more likely to concentrate just on the defensive side of the equation. After all, it is the essence of the job to defend when attackers attack.

However, defense is really only half the story. Hackers are constantly refining their skills. They're looking for innovative ways to get into systems and networks, and they're growing rather skilled at evading defenses. With all of the new strategies, techniques, and procedures that attackers are employing, the conventional are recognizing the importance of creating offensive and defensive tactics. But which is more important: playing offense or defense?

The offensive aspect

The threat landscape has dynamically changed throughout the years. Hackers are evolving threat craft effectively. "As they say in war 'Know thy enemy, it holds true for cybersecurity as well. It is important to know your adversary and it is important to understand the tactics, techniques, and procedures, or the TTP as we call them", Venkatesh Subramaniam, Group CISO & Privacy Head, Olam International said. Knowing the adversary is best done through threat intelligence and offensive security. This is one of the key reasons why organizations are keen on changing their cybersecurity landscape from an offensive to a defensive one. With the explosion of digital transformation and its initiatives, the attack surface has increased exponentially. Systems, data, and the users are not just in the data centers now, like in older times, they are everywhere. "To compound all of it, there is a demand for an anytime and anywhere access. So what basically happened is that it is virtually getting impossible to prevent bad things to happen in such a highly distributed and dynamic environment", he adds. Early detection and rapid response are two things that can be done to tackle cyberattacks and minimize the scale of damage. This is where offensive security comes into play again.

Offensive strategies also help and improve defensive strategies in terms of bringing in all the learnings and feeding them back as an input to build the defense mechanism. They are used to identify weaknesses in defensive strategies in the form of threat hunting, red teaming, or anything otherwise. "Imagine a chess game, you want to go offensive. For that, you need to have a solid defense before you go offensive. The feedback that you get from going offensive is then fed back into fortifying the defenses", this is what Satish Chandran, Director, GainCredit, had to say. The mindset of organizations has changed. They are no longer only trying to prevent cyber attacks from occurring but to head-on tackle them. The offensive and defensive strategies are used in conjunction to help protect and enable businesses.

Technology Focus

Red teaming strategies

Before talking about strategies, let us talk about the different teams in brief. A red team is a team that is trying to emulate an external threat, like someone who's trying to hack into a house. A white team is a team that oversees the engagement between the red and blue teams. Likewise, a blue team is an in-house team that monitors the security controls and defenses against attacks. So, what's the work of a red team here? Ideally, its work is to assess the security posture of the organization, the effectiveness of control put in place, the gaps in control, quantify businesses into most real terms, identify weaknesses and help fortify them. "The strategy people use here in most of the cases depends on the organization actually", Chandran said.

Technologies used for attacks

Certain technologies like bots, AI, and cognitive intelligence are being built into the attack vectors. Many times when organizations do not have an executable routine coming, these attacks sneak in and then start looking for power shells within the organizations to exploit them at the right time based on the information they collect. Companies have witnessed patterns in the past where certain ransomware have been sitting in environments, waiting for over 6 months to gather intel before they even declare themselves as ransomware. "The challenges for organizations today are multi-fold, not even fold. Organizations are exponentially expanding their digital footprints. What that does mean is, organizations acquire a larger surface area and therefore a larger surface area needs to be protected and controlled," Pradeep Rangi, CRP, Airtel Payments Bank said. Cybercriminals are resorting to advanced tools to attack, which includes offensive artificial intelligence. This makes their attacks more productive, efficient, and successful across all the various stages of cyberattacks. Areas like automating the reconnaissance, crafting tailored impersonation attacks, or hiding identities by going under the radars have become a situation of a regular occurrence. "When we talk about offensive artificial intelligence, what we are saying is that the machine learning algorithm is being utilized, supervised, and are incorporated with deep learning technologies", Rangi added.

So, what can be the solution? The core solution to the problem is in the fundamental strategy that organizations adopt as a risk-management framework. Businesses should respond, detect, and identify both on a proactive and reactive basis. Organizations need to hold on to the opportunities that they get in terms of their ability to identify, interpret, and then respond to these attacks. Even the subtlest of the opportunities need to be seized to ensure that these attacks do not breach their systems. Unless organizations resort to the very same technology that is giving them a challenge, they won't be able to keep up with these attacks and will eventually fall prey to many more cyber attacks.

https://bit.ly/38fzq2Y

Special Focus

Breach and Attack Simulation (BAS)

Merely having a security operations center (SOC) is not enough to guard against catastrophic attacks given the nature and magnitude of today's security breaches. Protecting an organization requires constant vigilance coupled with controls and cross-functional education. SOCs vary in size, scope and staffing across various industries, with the common thread being that they exist to monitor, detect, and respond to evolving threats to their respective organizations.

With Cymulate Know How You Can Be Breached

Continuous Automated Red Teaming (CART) implements MITRE ATT&CK® TTPs to discover cloud and infrastructure misconfigurations, vulnerabilities, and lack of cyber and IT hygiene. Like an ethical hacker, CART enables you to:

- Mitigate attack surface risk
- Mitigate risk created by lack of IT and cyber hygiene
- Quantify risk of specific security gaps and attackable vulnerabilities

For companies that want to assure their security against the evolving threat landscape. Cymulate is a SaaS-based breach and attack simulation platform that makes it simple to know and optimize your security posture any time, all the time and empowers companies to safeguard their business-critical assets. With just a few clicks, Cymulate challenges your security controls by initiating thousands of attack simulations, showing you exactly where you're exposed and how to fix it—making security continuous, fast and part of every-day activity.

Optimize Your Security Defenses

Breach and Attack Simulation (BAS) automates purple teaming to discover security gaps caused by product deficiencies, misconfigurations, and new threats.

Simple to deploy and use, Cymulate BAS enables you to:

- Quantify organizational cyber risk
- Assure security control efficacy
- Prioritize and rationalize spend
- Prioritize remediation based on attackable vulnerabilities
- Rationalize security spend

BAS Platform Capabilities

Proven framework: Offers a framework for testing an exhaustive range of attack vectors and threat scenarios, creating customized testing templates, and defining the testing scope, if any.

Industry recognized threat modeling: Models threats based on the cyber-attack tactics and techniques as described in the MITREATT & CK™ framework.

Complete coverage: Challenges controls across all vectors of the cyber kill chain, including pre-exploitation, exploitation and post-exploitation.

Threat intelligence: Enables incorporating daily threat intelligence on the latest cyber-attacks seen in the wild, be they ransomware, Trojans, APTs, crypto miners, worms or other threat types.

Automation: Offers repeatability and continuous coverage, BAS enables you to automate testing, alerting and reporting to run daily, weekly, or on demand for nonstop security control validation.

Remediation guidelines: Gain immediate remediation and mitigation guidelines for rapid, accurate response.

Metrics and reporting: Receive immediate auto-generated and delivered reports, that include metrics describing the full attack story and the techniques used. Benchmark control effectiveness against others in your industry and measure the impact of changes overtime.

Galaxy as a IT Solutions Provider strives to maintain and help the end customers to enhance their security compliance with the BAS tools. To talk to our experts, email us at marketing@goapl.com

Tech News

India's IoT market to reach $9.28 billion by 2025: Frost & Sullivan

"IoT solution deployment for manufacturing industries, including automotive, energy and utilities, smart cities (government), retail, and other industries such as logistics, will drive investments for enterprise IoT products and services," said Apalak Ghosh, Associate Director, Information & Communications Technologies, Frost & Sullivan.

NEW DELHI: The Indian Internet of Things (IoT) market is projected to reach $9.28 billion by 2025 from $4.98 billion in 2020, driven by increasing internet penetration, surge in smart application adoptions, and initiatives such as smart city, according to Frost & Sullivan. Adoption of IoT by enterprises as well as verticals' focus on automation are other factors "IoT solution deployment for manufacturing industries, including automotive, energy and utilities, smart cities (government), retail, and other industries such as logistics, will drive investments for enterprise IoT products and services," said Apalak Ghosh, Associate Director, Information & Communications Technologies, Frost & Sullivan. "Use cases such as industrial automation, building automation, security, and surveillance account for the majority of the market revenue. Telcos may benefit from a share of this revenue, depending on their strategic partnerships with hardware providers and their roles in the IoT value chain," Ghosh added. As per the Texas, United States-based firm, Indian telcos should focus on marketing the benefits of Private LTE or P-LTE to create awareness and approach enterprises with vertical-specific P-LTE solutions.

https://bit.ly/3I0GzXQ

Microsoft to set up fourth datacenter region in Hyderabad

Microsoft today announced its intent to establish its latest datacenter region in Hyderabad, Telangana.

This investment is aligned with Microsoft's commitment to help customers thrive in a cloud and AI-enabled digital economy and will become part of the world's largest cloud infrastructure, according to the company's announcement. Customer demand for cloud as a platform for digital transformation, driving economic growth and societal progress across India, is increasing. According to IDC, Microsoft datacenter regions in India contributed $9.5B revenue to the economy between 2016 and 2020. Beyond GDP impact, the IDC report estimated 1.5 million jobs were added to the economy, including 169,000 new skilled IT jobs. The Hyderabad datacenter region will be an addition to the existing network of three regions in India across Pune, Mumbai, and Chennai. It will offer the entire Microsoft portfolio across the cloud, data solutions, artificial intelligence (AI), productivity tools, and customer relationship management (CRM) with advanced data security, for enterprises, start-ups, developers, education, and government institutions.

"Cloud services are poised to play a critical role in reimagining the future of business and governance and enabling overall inclusion in the country. The new datacenter will augment Microsoft's cloud capabilities and capacity to support those working across the country," said, Anant Maheshwari, President, Microsoft India

https://bit.ly/3MUqyyC