FRIDAY, 3RD APR. 2026

www.suffix.solutions
engage@suffix.solutions

SUFFIX SOLUTIONS

WEEKLY DIGEST

DID YOU KNOW -

"Typewriter" is the longest word you can type using only the top row?

While "TYPEWRITER" is the most famous example, it actually shares the top-row throne with words like "PROPRIETOR" and "REPERTOIRE." This quirk of keyboard geometry dates back to the 1870s. Legend suggests Christopher Sholes arranged the layout so salesmen could impress customers by quickly Pecking out the brand name "Typewriter" using only the uppermost letters. *It was said that the keyboard got so tired after work because it put in too many "shifts"!*

Technically, even longer words like "RUPTUREWORT" (a small herb) exist, but they lack the poetic irony of the machine's own name. This layout remains a fossil of mechanical necessity, proving that 19th-century marketing still dictates how we communicate today.

LOCAL INDUSTRY UPDATES

- A massive breach allegedly from Remita has been leaked on a popular cybercrime forum.
- Huawei + Tetracore $400M AI-ready data centre project announced in Ogun State.
- FGN announced plans to establish the National Cybersecurity Coordination Council.

GLOBAL INDUSTRY UPDATES

- Amazon Reports 40% Efficiency Gain Using AI Pentesters.
- Microsoft to invest $10B in AI & cloud infrastructure in Japan.
- Google Unleashes Gemini AI Agents on the Dark Web.

INSIGHT OF THE WEEK

The QWERTY layout proves that efficiency often yields to habit. We still type on a 19th-century mechanical workaround because collective "muscle memory" is more powerful than technical perfection.

Local Industry Updates

A massive breach allegedly from Remita has been leaked on a popular cybercrime forum.

Reports from early April 2026 indicate a massive alleged data breach involving **Remita**, a prominent Nigerian payment platform. A threat actor known as **ByteToBreach** has claimed responsibility for leaking approximately **3TB of data** on a popular cybercrime forum.

Key Details of the Alleged Breach

Total Size & Source: Roughly 3TB of data allegedly stolen from improperly secured Amazon S3 cloud storage.

Data Types Exposed: The leaked information reportedly includes over 800GB of sensitive KYC documents (passports, bank statements), internal source code/Docker registries, and database exports containing 35,000+ password hashes.

Cause: Reports suggest a critical cloud misconfiguration left storage buckets publicly accessible.

Official Response and Current Status

Remita's Action: The company advised its partners/users to **re-generate API credentials** on March 31, 2026, citing system improvements.

Company Stance: While advising on security steps, Remita has not officially confirmed the 3TB breach, stating their core infrastructure is secure.

Verification: Independent verification of the full, alleged 3TB dataset is still pending, with some analysts noting potential, mix-in data from older incidents.

Recommendations for Users

Update Security: Immediately regenerate API keys for business integrations.

Enable MFA: Activate Multi-Factor Authentication (MFA) on all related accounts.

Monitor for Fraud: Watch for phishing attempts, as leaked KYC data can facilitate identity theft.

Huawei + Tetracore $400M AI-ready data centre project announced in Ogun State.

Tetracore Energy Group (TEG) announced a strategic partnership with **Huawei** and **Inspirive Technologies** to develop a **$400 million** AI-ready data centre in Ogun State, Nigeria.

Project Overview

The facility, named the **20MW Tier III Fusion Block Data Centre**, is designed to be the backbone of Nigeria's digital ecosystem.

Location: Situated within the Tetracore Energy Park in Atakobo, Ijebu East LGA, Ogun State.

Capacity: A **20MW** facility built to global **Tier III** standards for high redundancy and operational resilience.

Energy-to-Digital Model: The project uses an innovative model to bypass national grid limitations by drawing power from an on-site **100MW Independent Power Plant (IPP)**.

Key Features and Goals

AI & High-Performance Computing: Purpose-built to handle AI-driven workloads, advanced analytics, and cloud adoption.

Data Sovereignty: Aims to reduce Nigeria's reliance on offshore hosting and improve national data security in compliance with the **Nigeria Data Protection Regulation (NDPR)**.

Target Sectors: Will serve fintech, telecommunications, e-commerce, government agencies, and tech startups.

Timeline: Scheduled for completion within **10 to 12 months**.

The project marks Tetracore's first venture into the data centre market, leveraging its existing gas-to-power infrastructure to solve the perennial challenge of power instability for digital infrastructure.

FGN announced plans to establish the National Cybersecurity Coordination Council.

Federal Government of Nigeria announced plans to establish the **National Cybersecurity Coordination Council (NCCC)** to serve as a multi-stakeholder platform for strengthening the country's collective digital defense.

Objectives and Mandate

The council is envisioned as a non-statutory body designed to bridge the coordination gap between government agencies and the private sector.

Collective Defense Model: Shifts Nigeria's strategy from isolated institutional responses to a unified "collective defense" approach.

Information Sharing: Facilitates real-time, trusted sharing of threat intelligence among banks, telecommunications companies, and government bodies.

Advisory Role: Provides strategic guidance to the government on evolving cyber threats and national response mechanisms.

Implementation Structure

Technical Secretariat: A dedicated secretariat has been established within the **National Information Technology Development Agency (NITDA)**.

Collaborative Agencies: The initiative is a joint effort between NITDA, the Nigerian Communications Commission (NCC), Galaxy Backbone Limited, and the Nigeria Data Protection Commission (NDPC).

Industry Roundtable: A national cybersecurity industry roundtable is scheduled for **April 2026** to formally co-create the council's operational framework with private sector stakeholders.

Drivers for Establishment

The proposal follows a surge in sophisticated cyberattacks targeting Nigerian financial institutions, including alleged breaches at Sterling Bank and a ₦3 billion fraud attempt at FCMB. The council aims to address these risks by improving early threat detection and streamlining recovery across the digital economy.

Global Industry Updates

Amazon Reports 40% Efficiency Gain Using AI Pentesters.

At the **RSA Conference** in early April 2026, Amazon's Chief Information Security Officer, **CJ Moses**, revealed that the company has achieved a **40% efficiency gain** by integrating AI-powered tools into its penetration testing (pentesting) workflows.

Key Strategic Shifts

Continuous Testing: Unlike traditional "point-in-time" assessments, Amazon's AI agents enable **continuous vulnerability testing** that runs 24/7, even after products have launched.

Scale Without Headcount: The efficiency gain allows Amazon to maintain high security standards across a rapidly expanding portfolio of cloud services and codebases while **holding security hiring flat**.

Human-in-the-Loop: While AI handles data-intensive tasks like vulnerability identification and mapping attack chains, **humans remain responsible** for final decision-making and high-level strategy.

New "Frontier Agents" for Customers

Coinciding with this report, AWS announced the general availability of the **AWS Security Agent** on March 31, 2026.

Autonomous Attack Scenarios: These agents analyze source code and architecture to build tailored, multi-step attack paths to find weaknesses missed by traditional scanners.

Speed of Remediation: Customers like **HENNGE K.K.** reported reducing typical testing durations by over **90%**, while **Scout24** noted that the tool identified critical vulnerabilities that traditional DAST tools overlooked.

Availability: The service is initially available in six AWS Regions, including **US East (N. Virginia)**, **US West (Oregon)**, and **Europe (Ireland)**.

Microsoft to invest $10B in AI & cloud infrastructure in Japan.

Microsoft announced its largest-ever investment in Japan, pledging **$10 billion (approximately ¥1.6 trillion)** over the next four years to accelerate the country's AI and cloud infrastructure development. The initiative was unveiled during a meeting in Tokyo between Microsoft Vice Chair and President **Brad Smith** and Japanese Prime Minister **Sanae Takaichi**.

Strategic Investment Pillars

The funding, spanning from **2026 to 2029**, is built around three core pillars: **Technology, Trust, and Talent**.

Infrastructure Expansion: Microsoft will reinforce its own data centres and collaborate with local partners **SoftBank Corp.** and **Sakura Internet Inc.** to expand Japan-based AI computing capacity.

Data Sovereignty: The partnerships allow businesses and government agencies to process and store sensitive data domestically while accessing Microsoft Azure services, addressing national security and residency requirements.

Cybersecurity Cooperation: The company will deepen information sharing with Japan's **National Cybersecurity Office** and the **National Police Agency** to enhance national threat detection and crime prevention.

Workforce Development: Microsoft committed to training **one million engineers and developers** by 2030 in collaboration with major IT firms like **NTT Data, NEC, Fujitsu, and Hitachi**.

Market and Economic Impact

Local Ecosystem: Shares of Sakura Internet jumped **20.2%** following the announcement, reflecting its role as a key infrastructure provider.

Asia Strategy: This move follows recent major Microsoft investments in the region, including **$5.5 billion** in Singapore and **$1 billion** in Thailand.

Addressing Talent Gaps: The training initiative aims to mitigate a projected shortfall of over **3 million** AI and robotics workers in Japan by 2040.

Google Unleashes Gemini AI Agents on the Dark Web.

Google Cloud integrated Gemini AI agents into its Threat Intelligence platform to monitor the dark web autonomously. This replaced keyword-based alerts with contextual reasoning to identify specific threats to an organization.

How Gemini "Crawls" the Dark Web

These agents find relevant risks early in the attack lifecycle by processing millions of daily events.

Scale: The agents process between 8 and 10 million events daily.

Precision: Internal tests by Google threat hunters show an accuracy rate of 98%, compared to the 80–90% false-positive rate typically seen in traditional regex-based monitoring.

Contextual Profiling: Upon first use, Gemini builds a comprehensive "organizational profile" to distinguish between general noise and a targeted attack. This profile includes VIP names, internal technology stacks, and business partners.

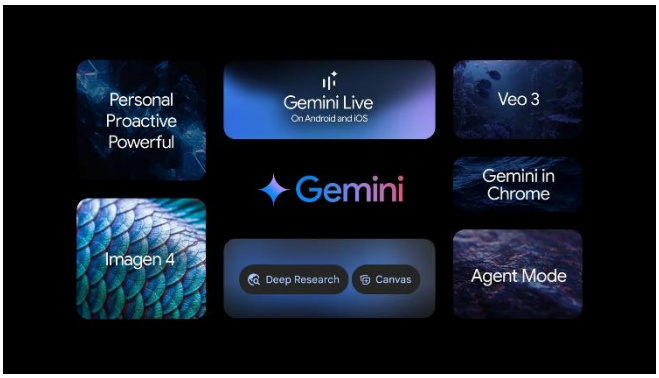
Targeted Threat Detection

The agents are trained to identify high-severity activities that often lack obvious keywords:

Initial Access Broker (IAB) Activity: Detecting hackers selling access to a company's specific VPN or portal types, even if the company name isn't explicitly mentioned.

Unverified Data Leaks: Identifying claims of stolen data by mapping contextual signals like revenue brackets or geography against the user's profile.

Insider Threats: Monitoring forums for solicitations or "insider for hire" posts that match a company's specific infrastructure.



The "Agentic SOC" Vision

At the RSA Conference 2026, Google highlighted this as part of the broader Agentic Security Operations Center (SOC). AI agents handle the "rote work" of gathering and correlating data, while human analysts focus on strategic validation and final judgment.

Top gainers in stock market as at Saturday, 4th April, 2026.

(Source: tradingview.com)

Symbol 33		↓ Change %	Price	Volume
UNILEVER	Unilever Nigeria PLC	+10.00%	103.4 NGN	879.08 K
FTGINSURE	Fortis Global Insurance ...	+9.82%	1.23 NGN	7.82 M
MULTIVERSE	Multiverse Mining & Ex...	+9.81%	20.15 NGN	256.27 K
LEGENDINT	LEGEND INTERNET PLC	+9.38%	6.30 NGN	6.48 M
ZICHIS	Zichis Agro-Allied Industrie...	+9.02%	14.14 NGN	4.52 M

Contact Us

www.suffix.solutions

engage@suffix.solutions