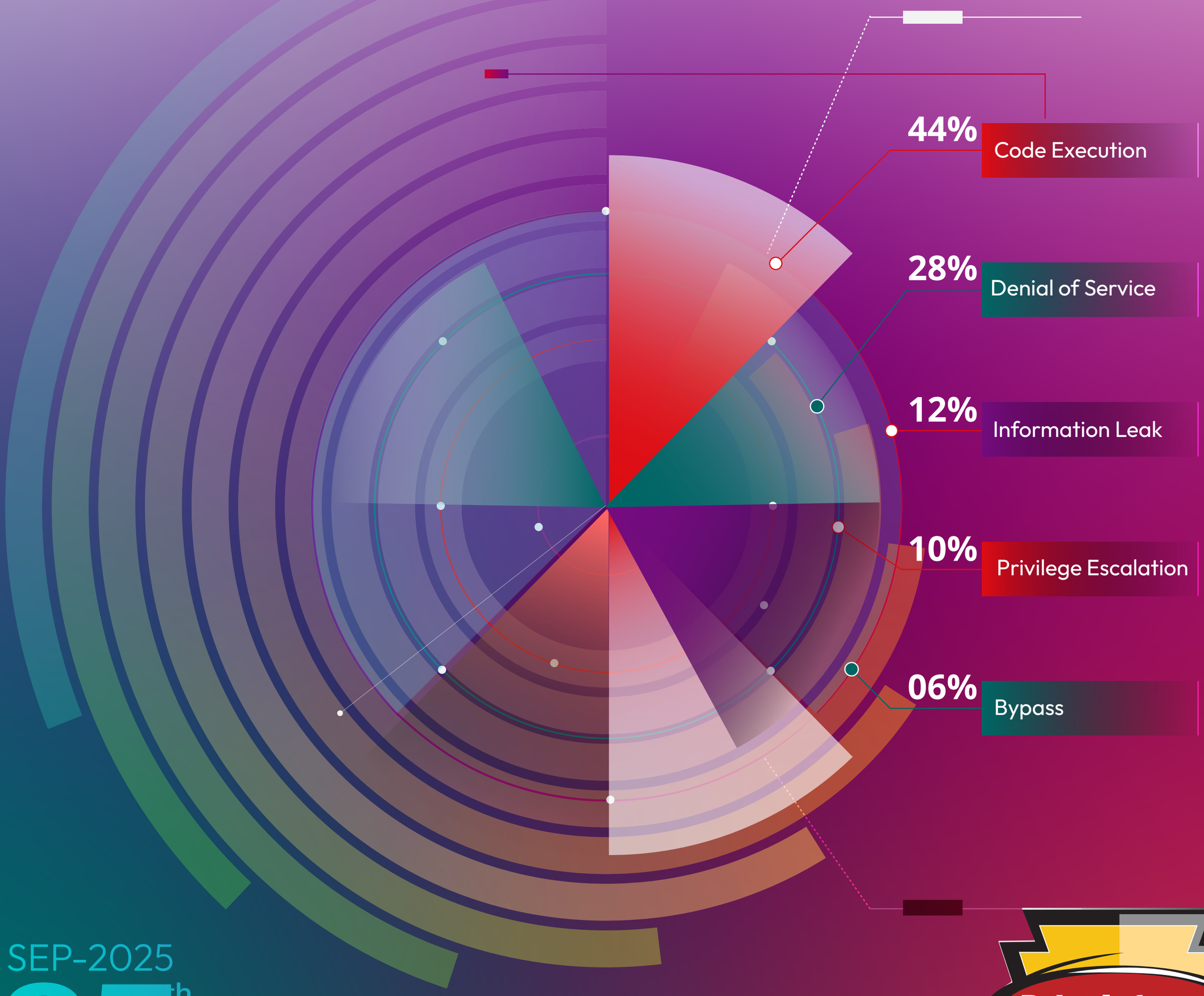
Briskinfosec's

Threatsploit Adversary Report



SEP-2025

85th Edition

BriskInfosec™

Introduction :

Dear Readers,

Why are billions in security investments failing to prevent the most consequential breaches? The answer lies not in technology gaps, but in a complete shift in how adversaries operate, one that renders traditional defensive playbooks obsolete. Organizations continue investing in perimeter security while attackers have moved inside, weaponizing the very tools and trust relationships that enterprises depend on daily

This month's intelligence reveals three critical developments adversaries patching vulnerabilities behind themselves to maintain exclusive access, ransomware groups sharing advanced EDR-killing tools across eight different families, and AI-powered campaigns simultaneously targeting both human psychology and automated security systems. From dam control systems to pharmaceutical R&D operations, from parliamentary databases to airline passenger records, no sector remains untouched.

Success requires immediately shifting from reactive patching to proactive threat hunting, from perimeter defense to zero-trust implementation, and from tool-focused strategies to intelligence-driven operations that can adapt to adversaries who think like chess grandmasters.

Best regards,

Briskinfosec Threat Intelligence Team.

Highlights

1. Recent Cyber attacks in August - 2025
2. 5 Must-Read Books for Every CISO
3. Top Critical CVEs of August
4. BriskInfosec Exhibiting at GITEX Global 2025

Contents :

Qilin Ransomware Paralyzes Pharma Powerhouse Inotiv 176GB R&D Secrets Stolen

In the pharmaceutical sector, Qilin ransomware attackers infiltrated Inotiv's core IT systems on August 8 via system infiltration, encrypting data storage and applications while exfiltrating 162,000 files totaling 176GB of sensitive R&D data. Disclosed on August 20, the breach forced immediate shutdowns, shifting to offline ops with no recovery timeline, severely disrupting drug development timelines, regulatory submissions, and revenue streams. This highlights ransomware's devastating toll on intellectual property and operational continuity in high-stakes industries.

Attack Type : Ransomware

Cause of Issue : System Infiltration

Takeaways : Air-gapped IP backups in pharma, enforce zero-trust, EDR, and quarterly simulations for cyber teams.

UAE Nightmare 200K Daily Attacks from Rogue Apps Stealing Your Life

Targeting the general public, malware from unverified third-party apps surged to 200,000 daily incidents in the UAE, enabling financial theft, identity fraud, and access to personal data like contacts and photos. The Cybersecurity Council's alert stresses official app stores and permission reviews, as these attacks erode privacy, cause monetary losses, and threaten national digital infrastructure, demanding urgent policy updates and awareness.

Attack Type : Malware

Cause of Issue : Third-party Apps

Takeaways : Restrict to official stores and vet permissions, deploy MDM, MTD, and awareness campaigns.

Sneaky Linux Malware Invades Clouds Patches Holes to Lock You Out Forever

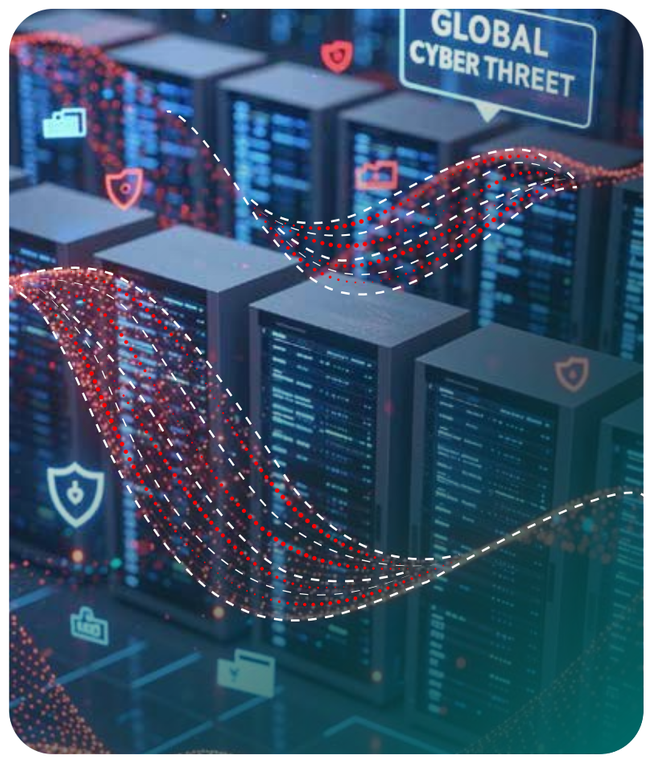
In cloud environments, malware exploited CVE-2023-46604 in Apache ActiveMQ to breach Linux systems, then patched the vulnerability to block rivals while deploying Sliver implants for persistence, SSH root access, and Dropbox-based command downloads. This clever evasion camouflages traffic, leading to exclusive control, detection challenges, and weakened security postures across enterprises.

Attack Type : Malware

Cause of Issue : Patching

Takeaways : Enable behavioral analytics, automate patching, enforce least-privilege, and monitor SSH/Dropbox.

Warlock Ransomware Ravages SharePoint Enterprises Wiped Out in Global Assault



Enterprise-wide, Warlock ransomware targeted unpatched SharePoint servers with HTTP POST web shells, escalating privileges via malicious GPOs and guest accounts, enabling lateral movement, data exfiltration with RClone, and encryption using .x2anylock extensions while disabling security processes. This global campaign causes total operational wipeouts, intellectual losses, and demands immediate patching to avert cross-sector devastation.

Attack Type : Ransomware

Cause of Issue : Unpatched-SharePoint

Takeaways : Patch SharePoint immediately, implement PAM, segmentation, and GPO change detection.

UAE Firm Pays $20M for Phone-Hacking Zero-Days Global Surveillance Armageddon

In surveillance tech, a UAE startup offered up to $20M for zero-day exploits from unknown sellers, enabling remote smartphone compromises via SMS on Android/iOS/Windows/Chrome, with opaque ties to governments and no ethical oversight. This escalates the zero-day market, risking weaponized vulns, cyber warfare, and widespread mobile security erosion worldwide.

Attack Type : Zero-day

Cause of Issue : Unknown-Seller

Takeaways : Promote responsible disclosure, run bug bounties, mobile forensics, and SMS threat monitoring.

iiNet Horror Hackers Steal 280K Customer Details with Stolen Credentials

In telecommunications, attackers used stolen credentials to breach iiNet's order system on August 16, exposing 280K emails, phones, addresses, and modem passwords, though no financial data was hit. This triggers phishing risks, shatters customer trust, and underscores credential vulnerabilities, prompting swift response and notifications.

Attack Type : Data Breach

Cause of Issue : Credential Theft

Takeaways : Mandate MFA, conduct access audits, phishing alerts, and rapid incident response.

GodRAT Haunts Finance Giants Steganography Hides Deadly RAT Invasion

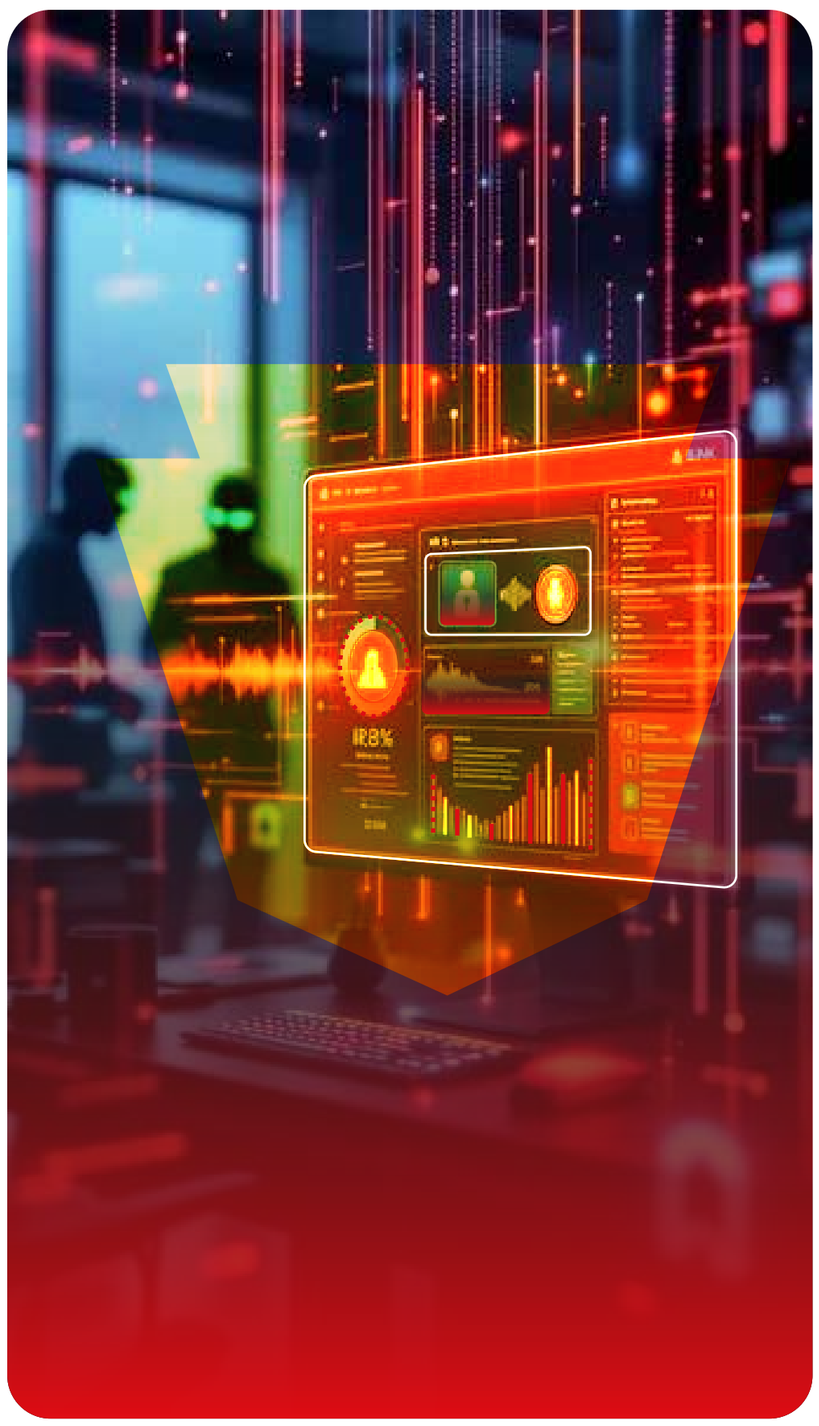
Finance firms in UAE/Asia faced GodRAT, a RAT variant spread via Skype's malicious .scr/.pif files disguised as docs, using steganography in images for shellcode, credential theft, and AsyncRAT persistence, linked to APTs. This breaches confidentiality, enables ongoing espionage, and threatens transaction integrity across brokerages.

Attack Type : Remote Access

Cause of Issue : Social Engineering

Takeaways : Block risky file types, deploy steganography scans, ATP, and APT intelligence.

Workday CRM Cracked by Vishing Onslaught HR Data Exposed to Impersonators



In HR SaaS, vishing and SMS impersonating staff tricked employees into granting OAuth access to Workday's CRM on August 6, exposing contacts for chain phishing, though core data remained secure. This human-factor breach enables impersonation attacks and highlights integration risks, impacting trust and follow-on threats.

Attack Type : Vishing

Cause of Issue : Social Engineering

Takeaways : Train against vishing, review OAuth and enforce call verification protocols.

PipeMagic Backdoor Masquerades as ChatGPT Zero-Day Devastates Manufacturers

Manufacturing in Saudi/Brazil hit by PipeMagic backdoor via fake ChatGPT apps exploiting CVE-2025-29824 for escalation, using DLL hijacking and Azure C2 for lateral movement and persistence. This leads to industrial sabotage, operational halts, and stealthy enterprise compromises.

Attack Type : Backdoor

Cause of Issue : Zero-Day Exploit

Takeaways : Allowlist apps, monitor pipes and deploy zero-day defenses.

Canadian Parliament Hacked via SharePoint Zero-Day Staff Data Ripped Open

Government networks breached on August 8 via SharePoint zero-day CVE-2025-53770, allowing RCE and extraction of staff names, emails, devices, suspected by Salt Typhoon APT. This national security incident enables phishing and impersonation, compromising operations and highlighting IT vulns.

Attack Type : Data Breach

Cause of Issue : SharePoint Zero-Day

Takeaways : Hunt for APTs, log deserialization and apply patches promptly.

Russian Hackers Flood Norwegian Dam Critical Infrastructure on Brink of Disaster!

Energy sector sabotage by pro-Russian hackers exploited weak passwords in April to open Bremanger dam floodgates for hours, disrupting ops though no injuries occurred. This hybrid warfare exposes OT weaknesses, raising fears of escalated infrastructure attacks and control system failures.

Attack Type : Sabotage

Cause of Issue : Weak Password

Takeaways : Segment IT/OT, enforce strong credentials and monitor commands.

Nigeria Customs Crippled by Cyber Strike Nationwid

Logistics platform B'Odogwu hacked on August 14 due to glitches, paralyzing cargo clearances at ports and accruing costs, impacting importers financially amid repeat incidents. This causes supply chain delays, business losses, and calls for upgrades to prevent ongoing vulnerabilities.

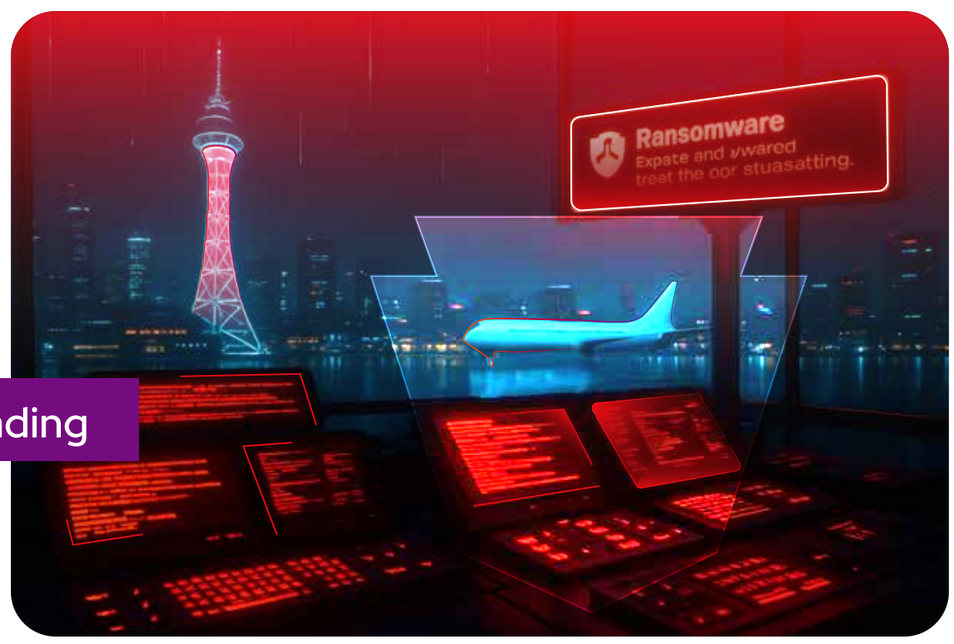
Attack Type : Hacking of ICT Systems

Cause of Issue : Platform Glitch

Takeaways : Build redundancy, perform pen tests and uptime anomaly alerts.

Charon Ransomware Sideloading Nightmare Aviation and Public Sectors Encrypted

Public-aviation targets in Mideast hit by Charon ransomware using Edge.exe DLL sideloading for injection, terminating security, deleting recoveries, and customizing notes. This APT-style attack leads to encryption, extortion, and operational shutdowns with evasion challenges.



Attack Type : Ransomware

Cause of Issue : DLL Sideloading

Takeaways : Validate binaries, detect process injections immediately.

WinRAR Exploit Rampage Dual Groups Deploy Backdoors-Patch or Perish

Financial services exploited via CVE-2023-38831 in WinRAR by two groups using malicious archives for code execution and backdoors, bypassing protections. This escalates desktop risks, enabling malware spread and data access across Windows users.

Attack Type : Exploit

Cause of Issue : RAR Processing

Takeaways : Disable auto-extract, scan archives routinely.

WestJet Breach Terror Passports and PII Pilfered in Airline Data Heist

Airlines suffered unauthorized access in June, stealing names, contacts, travel history, and passports from WestJet, no cards affected, triggering privacy probes and credit monitoring offers. This enables ID theft, erodes trust, and disrupts sensitive travel data handling.

Attack Type : Data Breach

Cause of Issue : Unauthorized Access

Takeaways : Tighten access controls, alert on bulk queries and offer credit monitoring.

Murky Panda APT Assault Chinese Hackers Plunder Gov and Services Data

Government and services in N. America targeted by China-linked Murky Panda exploiting CVE-2023-3519 in SaaS/Microsoft for malware deployment and anti-forensics like web shells. This industrial espionage causes data plunder, detection evasion, and persistent threats hard to detect.

Attack Type : Cloud Exploitation

Cause of Issue : Inadequate Cloud Monitoring

Takeaways : Conduct threat hunting, enhance cloud logs and patching.

AI-Powered Gmail Phishing Evades All Prompt Injection Spells Detection Doom!

Technology sector hit by Gmail phishing using AI prompt injections in source code to mislead SOC tools, with obfuscated JS and redirects for credential theft. This delays responses, exploits humans and automation, leading to widespread breaches.

Attack Type : Phishing with AI

Cause of Issue : Weakness in AI Tools

Takeaways : Layer email security, inspect sources for anomalies.

HTTP Smuggling Breakthrough Hackers Inject Chaos Past Web Defenses

Web and cloud services vulnerable to HTTP smuggling via malformed chunks, injecting requests past WAFs/CDNs for backend access. This flaw causes unauthorized intrusions, app security collapses, and urges HTTP/2 shifts.

Attack Type : HTTP Request Smuggling

Cause of Issue : Inconsistent Parsing

Takeaways : Migrate to HTTP/2, validate parsing configurations.

Native Phishing Hijacks M365 Trusted Apps Turn Into Credential Thieves

Enterprise phishing abuses compromised M365 accounts to share files via OneNote/OneDrive, redirecting to fake portals for creds, bypassing email defenses. This exploits trust, enables lateral movement, and rapid compromises in hybrids.

Attack Type : Phishing

Cause of Issue : Compromised Credentials

Takeaways : Enforce file policies, apply conditional access.

Royal Enfield Ransomware Catastrophe All Data Encrypted, Backups Annihilated

Automotive giant Royal Enfield struck by ransomware exploiting remote files, with attackers encrypting servers, deleting backups, and threatening data auctions under tight ultimatums. This causes downtime, IP threats, regulatory penalties, and potential design disruptions in manufacturing.

Attack Type : Ransomware

Cause of Issue : Exploited Remote File

Takeaways : Secure offline backups, audit MFA and monitor exfiltration.

Fake WhatsApp Libs Wipe Dev Data Supply Chain Sabotage Strikes IT

IT developers targeted by malicious NPM packages posing as WhatsApp libs, executing data-wiping rm -rf commands with kill switches, downloaded over 1,100 times. This supply chain attack destroys files, risks exfil, and undermines API/automation trust.

Attack Type : Supply Chain

Cause of Issue : Unvetted Packages

Takeaways : Scan packages, check dependencies rigorously.

BQTLOCK RaaS Rampant Evasion Tactics Crush Endpoint Security

Professional services face BQTLOCK RaaS with AES/RSA encryption, cred harvesting, backdoors, and evasions like process hollowing/UAC bypasses, linked to hacktivists. This results in persistence, exfil via Discord, and crushing defenses with subscription models.

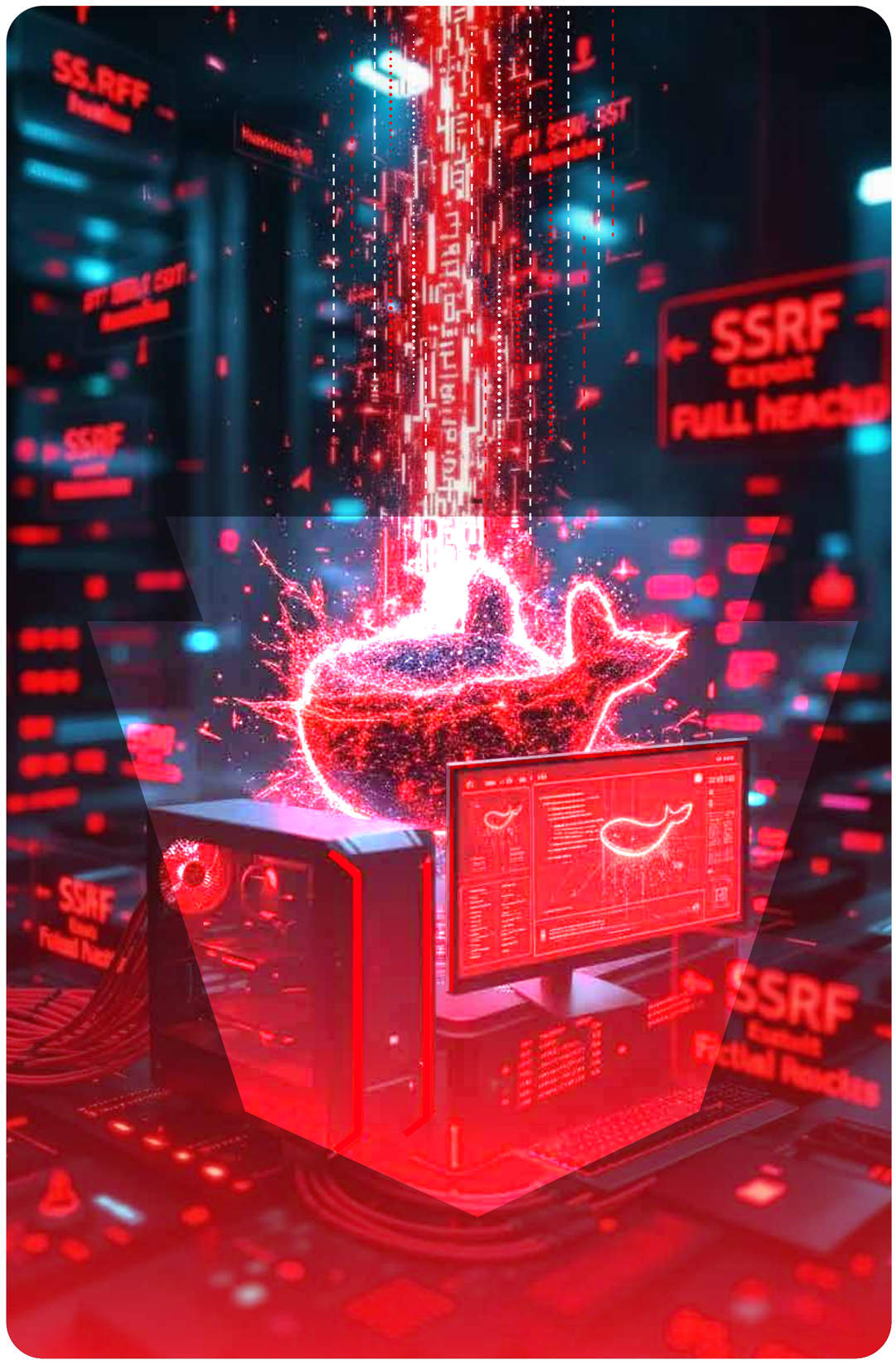
Attack Type : Ransomware-as-a-Service

Cause of Issue : Weak Endpoint Defenses

Takeaways : Deploy behavioral EDR, isolate backups.

Docker Desktop Flaw Exposes Hosts SSRF Grants Total System Takeover

Technology/cloud containerization hit by CVE-2025-9074 in Docker Desktop, allowing unauth SSRF to create privileged containers and mount drives for full access. This breaks isolation, enables easy compromises, and demands urgent updates.



Attack Type : Server-Side Request Forgery

Cause of Issue : Unauthenticated API

Takeaways : Authenticate APIs, monitor SSRF patterns.

Colt Ransomware Extortion Customer Data Dumped on Dark Web

Telecommunications firm Colt attacked on August 12 via vulnerable systems, exfiltrating customer data to dark web for extortion, suspending platforms while networks stayed up due to segmentation. This slows services, amps pressure, and risks further leaks.

Attack Type : Ransomware

Cause of Issue : Vulnerable Systems

Takeaways : Segment networks,watch dark web for leaks.

Quishing QR Code Menace Malicious Scans Steal Secrets via Emails

Cloud services plagued by quishing with nested/split QR codes in emails bypassing security, redirecting scans to phishing sites or malware on mobiles. This exploits trust, weakens endpoints, and leads to data theft.

Attack Type : Phishing

Cause of Issue : Weak Email Security

Takeaways : Train on QR risks, integrate AI detection.

EDR Killer Tool Proliferates 8 Ransomware Gangs Bypass All Defenses

Multiple industries targeted by EDR killer using stolen certs for BYOVD to disable AV/EDR in gangs like Qilin, fostering ecosystem collaboration. This leaves networks undefended, enabling rampant ransomware and total bypasses.

Attack Type : BYOVD-based Ransomware

Cause of Issue : Stolen Certificates

Takeaways : Validate drivers, enable behavioral monitoring.

Cisco Vishing Breach User Accounts Looted in Cloud CRM Heist

Enterprise IT breached via vishing on July 24, tricking staff to export user data from CRM, including names/emails, no passwords hit. This enables phishing chains and stresses human vulnerabilities in cloud setups.

Attack Type : Vishing

Cause of Issue : Social Engineering

Takeaways : Drill vishing scenarios, strengthen CRM controls.

Akira Ransomware Weaponizes CPU Tool Defender Disabled in BYOVD Blitz

Enterprise IT exploited by Akira using ThrottleStop driver in BYOVD via CVE-2024-40766 VPN flaws to edit registry and disable Defender. This grants kernel access, bypasses controls, and facilitates full ransomware deployment.

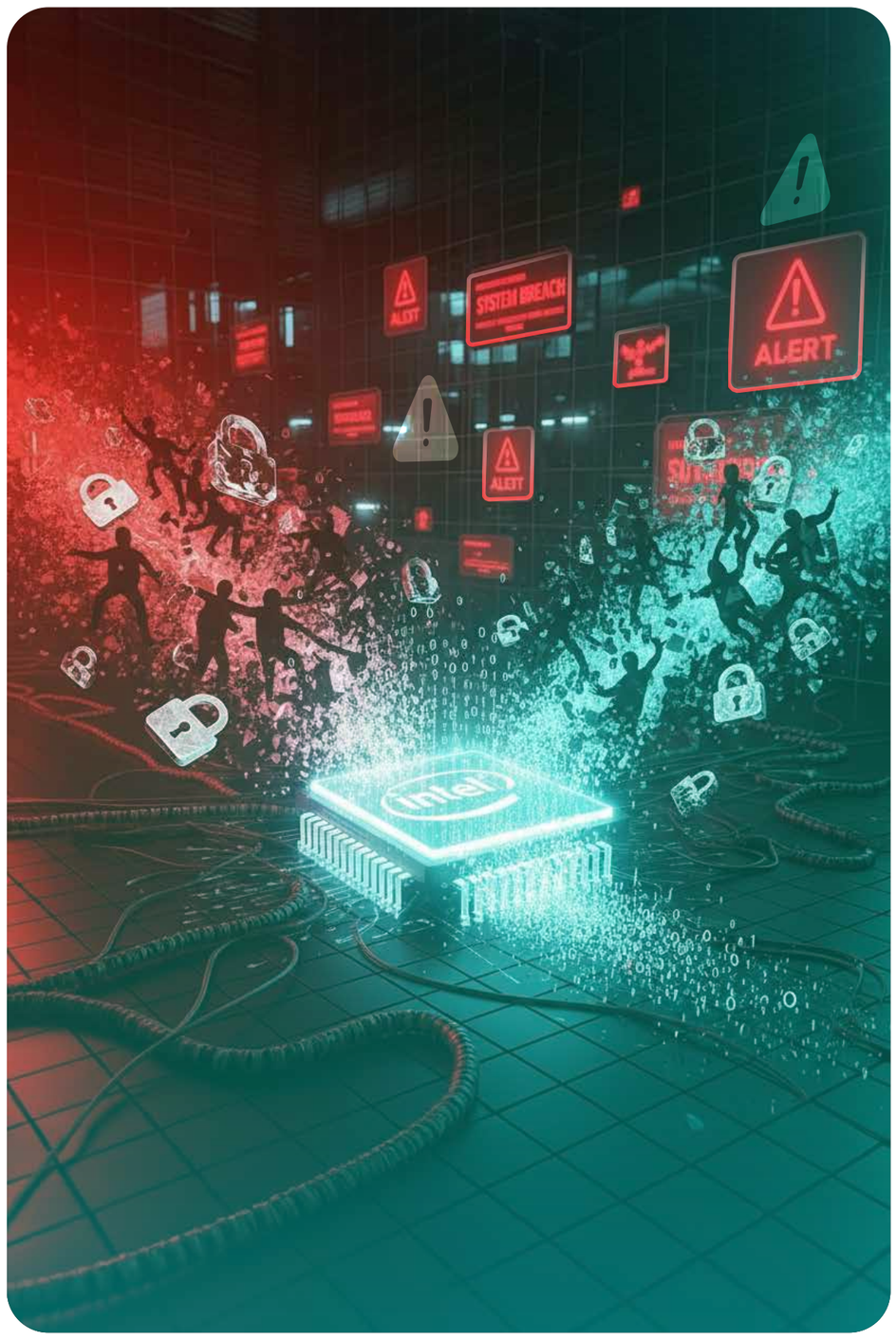
Attack Type : BYOVD Attack

Cause of Issue : Abuse of Signed Drivers

Takeaways : Allowlist drivers, alert on registry changes.

FortiSIEM RCE Exploit Loose Unauth Hackers Commandeer Security Platforms

MSSP platforms vulnerable to CVE-2025-25256 RCE via CLI injection, allowing unauth commands for system takeover and data exposure. This wild exploit risks lateral movement and compromises security infrastructure integrity.



Attack Type : Remote Code Execution

Cause of Issue : Improper Sanitization

Takeaways : Patch SIEM urgently, log input sanitization.

Intel Vulns Leak 270K Employee Records Auth Bypasses Expose All

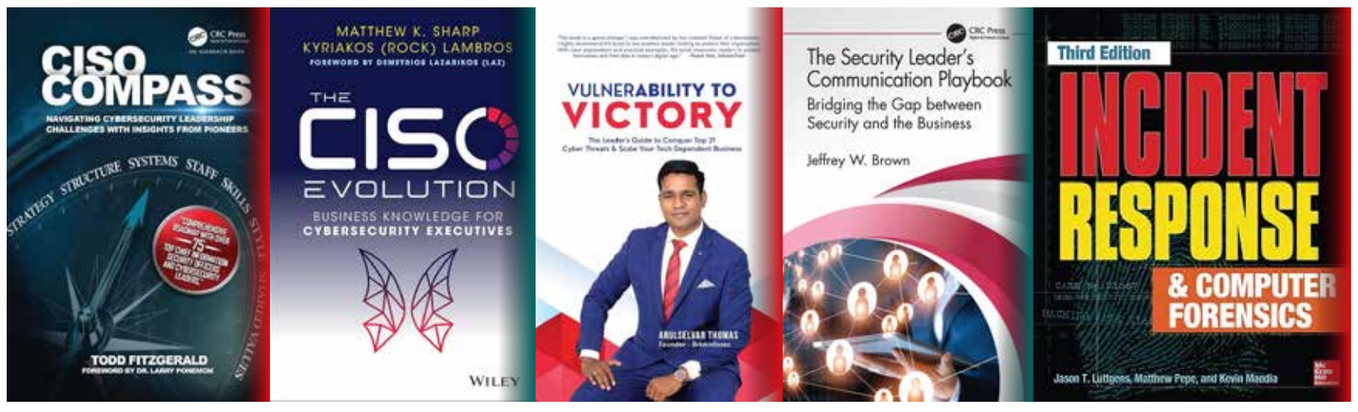
Enterprise IT at Intel exposed via auth bypasses and hardcoded creds in internal sites, leaking 270K employee/supplier details in 1GB JSON files, remediated by February 2025. This privacy disaster enables targeting and underscores dev practice flaws.

Attack Type : Authentication Bypass

Cause of Issue : Weak Auth & Exposure

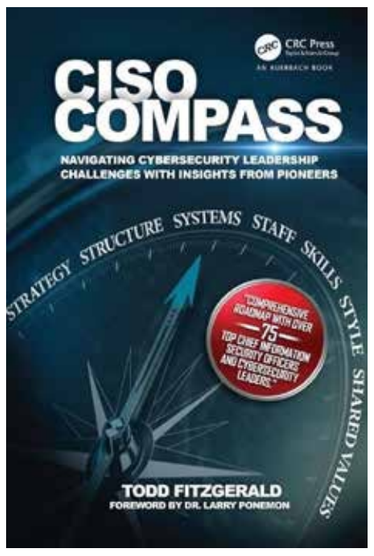
Takeaways : Scan for vulns, eliminate hardcoded credentials.

5 Must Read Books for Every CISO



BriskInfosec

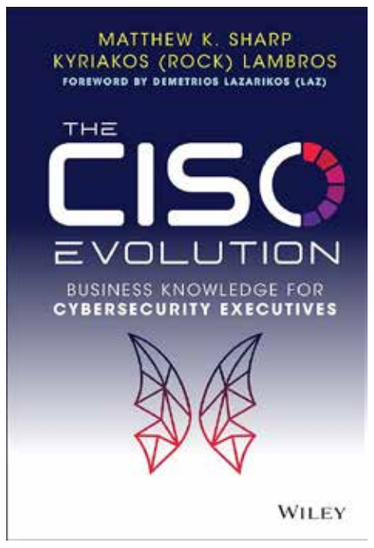
www.briskinfosec.com



CISO Compass : Navigating Cybersecurity Leadership Challenges with Insights from Pioneers

The definitive CISO leadership guide featuring insights from 75+ security executives. Covers strategy, team management, board communication, and compliance using proven frameworks

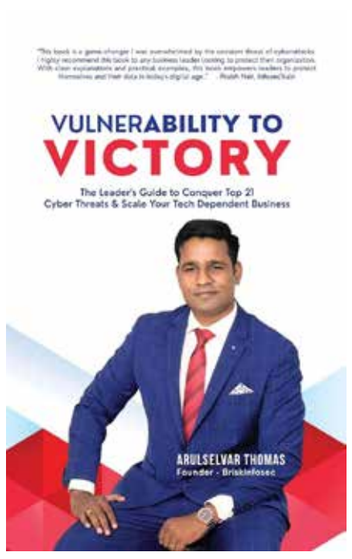
Author : Todd Fitzgerald



The CISO Evolution : Business Knowledge for Cybersecurity Executives

Teaches CISOs how to align security with business priorities, communicate with executives, and secure funding through business-focused approaches.

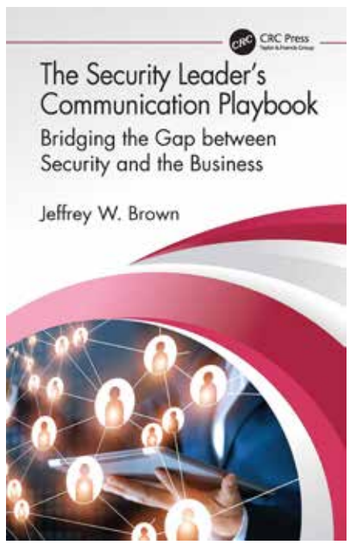
Authors : Matthew K. Sharp, Bill Bonney, Gary Hayslip



Vulnerability to Victory

Transforms cybersecurity thinking from defensive cost center to strategic business enabler. Provides frameworks for turning security challenges into competitive advantages

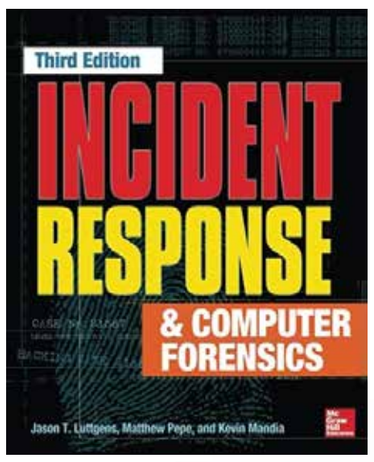
Author: Arulselvar Thomas



The Security Leader's Communication Playbook : Bridging the Gap Between Security and the Business

Essential communication guide for security leaders covering executive presentations, crisis communication, and stakeholder engagement strategies.

Author : Jeffrey W. Brown



Incident Response & Computer Forensics

Gold-standard reference for incident response and forensic analysis by Mandiant founder Kevin Mandia. Covers complete incident lifecycle with real-world case studies.

Authors : Jason Luttgens, Matthew Pepe, Kevin Mandia

Top Critical CVEs of August

CVE-2025-53779

A relative path traversal vulnerability in the Windows Kerberos authentication system (Windows Server 2025) that enables an authenticated attacker to elevate privileges over a network.

Severity : HIGH

Attack Type : Privilege Escalation

CVE-2025-50165

An untrusted pointer dereference in the Microsoft Graphics Component allows an unauthenticated attacker to achieve remote code execution (RCE) over a network.

Severity : CRITICAL

Attack Type : Remote Code Execution

CVE-2025-53787

An information disclosure flaw in Microsoft 365 Copilot BizChat lets attackers exploit improper input neutralization (CWE-77) to access sensitive data via unintended command execution.

Severity : HIGH

Attack Type : Information Leak

CVE-2025-57810

A vulnerability in jsPDF before 3.0.2 allows attackers to exploit unsanitized image data in the addImage method, causing high CPU usage and denial of service. Fixed in 3.0.2.

Severity : HIGH

Attack Type : Denial of service

CVE-2025-57810

A heap-based buffer overflow vulnerability exists in Windows GDI+ (Graphics Device Interface Plus). This flaw enables an unauthenticated, remote attacker to achieve remote code execution (RCE) without any user interaction.

Severity : CRITICAL

Attack Type : Remote Code Execution

BriskInfosec

www.briskinfosec.com

GITEX GLOBAL | 13-17 OCT 2025 DUBAI WORLD TRADE CENTRE

BriskInfosec Exhibiting at GITEX Global 2025

We're thrilled to announce BriskInfosec's participation in GITEX Global 2025, the world's largest technology event where industry leaders gather to shape the future. As AI transforms global economies, cybersecurity grows increasingly vital. BriskInfosec proudly joins this revolutionary platform, demonstrating how security and innovation unite.

What Awaits You at Our Stand

- Discover next-generation security solutions for the AI-driven economy
- Experience AI-powered threat detection with advanced intelligence systems
- Meet cybersecurity experts for personalized security consultations
- Learn about emerging threats and digital landscape security trends

Join the Global Tech Revolution

GITEX Global unites over 6,500 exhibitors and 200,000+ visitors worldwide. This massive convergence of technology enthusiasts, business leaders, and innovators creates unparalleled networking opportunities. We look forward to connecting with industry peers, potential partners, and forward-thinking organizations ready to secure their digital future.

Venue Details

Dubai World Trade Centre
Dates : 13th – 17th October 2025
Stall H23 - C16

“Security is not about building higher walls
It’s about understanding who is already inside”

+91 44 4352 4537 | +91 73059 79769
contact@briskinfosec.com | www.briskinfosec.com