COLORTOKENS

ColorTokens Threat Advisory

Threat Intelligence Brief #6

August 1 - 15, 2025

ACCESS BRIEF

Threat Intelligence Brief

August 1 - 15, 2025

Executive Summary

Cyber Threat Intelligence (CTI) is critical in understanding and mitigating the evolving threats faced by various industries, like healthcare, finance & manufacturing industry.

- Healthcare organizations are frequent targets for cybercriminals due to the high value of patient data and the critical nature of their services. Ransomware attacks and data breaches can disrupt operations and risk patient safety by shutting down medical devices or hospital networks. CTI in healthcare helps identify threat actors, vulnerabilities in connected medical devices, and the latest attack tactics. By integrating CTI, healthcare providers can proactively strengthen defenses, protect sensitive data, and maintain patient care continuity

- The finance sector faces continuous threats, including ransomware, Distributed Denial of Service (DDoS), and phishing attacks. Cybercriminals often target financial institutions to access valuable data or to extort money. CTI assists financial organizations in identifying emerging threats, such as new phishing tactics or advanced DDoS methods. By leveraging CTI, these organizations can better protect sensitive financial information, comply with regulations, and maintain trust with clients by preventing data breaches and financial losses.

- Effective CTI helps these sectors stay ahead of adversaries by identifying threat actors, tactics, and indicators of compromise (IOCs).



Section 1 - Critical Vulnerability Information

CVE ID	Title	Score	Description	Affected Version	Patch Details	Reference
CVE-2025-54253	Adobe AEM Forms on JEE Miscon figuration leading to Arbitrary Code Execution	10	Critical misconfiguration (CWE-16) in AEM Forms on JEE could allow arbitrary code execution over the network without authentication.	AEM Forms on JEE 6.5.23.0 and earlier	Update to AEM Forms on JEE 6.5.0-0108 per APSB25-82.	https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html
CVE-2025-25256	Fortinet FortiSIEM Unauthenti cated Comm and Injection	9.8	OS command injection in FortiSIEM phMonitor service allows unauthenticated remote code execution; exploit code reported available.	FortiSIEM 7.3.0-7.3.1; 7.2.0-7.2.5; 7.1.0-7.1.7; 7.0.0-7.0.3; 6.7.0-6.7.9; all 6.6, 6.5, 6.4, 6.3, 6.2, 6.1, and 5.4.	Upgrade to Fortinet fixed versions per PSIRT FG-IR-25-152; if unable, restrict access to port 7900 (phMonitor).	https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html
CVE-2025-50165	Windows Graphics Component Remote Code Execution	9.8	RCE via untrusted pointer dereference/uninitialized resources while decoding JPEGs; can trigger via Office/third-party files.	Windows 11 (24H2) and Windows Server 2025 among others (per vendor notes).	Install August 12, 2025 Patch Tuesday cumulative updates. See MSRC CVE page.	https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-august-2025/
CVE-2025-53766	Microsoft GDI+ Remote Code Execution	9.8	Heap-based buffer overflow in Windows GDI+ can lead to RCE over the network; Preview Pane not an attack vector.	Multiple supported Windows releases incl. Windows 10, Windows 11, and Windows Server 2008+ (per vendor notes).	Install August 12, 2025 Patch Tuesday cumulative updates. See MSRC CVE page.	https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-august-2025/
CVE-2025-53778	Windows NTLM Elevation of Privilege	8.8	Improper authentication in NTLM allows low-privileged attackers to elevate privileges over the network without user interaction.	Windows 10, Windows 11, and Windows Server releases incl. 2008, 2012, 2019, 2022, 2025 (per vendor notes).	Install August 12, 2025 Patch Tuesday cumulative updates. See MSRC CVE page.	https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-august-2025/

Critical Vulnerability:

FortiWeb Authentication Bypass Vulnerability Allows Logins as Any Existing User

A critical security vulnerability in Fortinet's FortiWeb web application firewall has been discovered that allows unauthenticated attackers to bypass authentication and impersonate any existing user on affected devices.

The flaw, tracked as CVE-2025-52970 and dubbed "Fort-Majeure" by its discoverer, stems from improper parameter handling in the application's cookie parsing mechanism.
Vulnerability Details and Impact

The vulnerability exploits an out-of-bounds read access issue in FortiWeb's cookie handling code, enabling attackers to force the server to use a predictable, all-zero secret key for session encryption and signing.

Security researcher Aviv Y (@0x_shaq), who discovered and responsibly disclosed the flaw, explained that the authentication bypass occurs through manipulation of the "Era" parameter in session cookies.

The vulnerability exploits an out-of-bounds read access issue in FortiWeb's cookie handling code, enabling attackers to force the server to use a predictable, all-zero secret key for session encryption and signing.

Security researcher Aviv Y (@0x_shaq), who discovered and responsibly disclosed the flaw, explained that the authentication bypass occurs through manipulation of the "Era" parameter in session cookies.

Field	Value
CVE ID	CVE-2025-52970
Published Date	August 12, 2025
IR Number	FG-IR-25-448
Severity	High
CVSS v3.1 Score	7.7
CVSS Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:C
CWE Classification	CWE-233: Improper Handling of Parameters

"This bug represents the kind of silent failure that wasn't meant to happen — where a system built to protect ends up trusting nothing as everything," the researcher noted.

The vulnerability allows attackers with non-public information about both the target device and specific users to craft malicious requests that bypass authentication entirely.

The session cookie mechanism in FortiWeb consists of three components: an Era value, an encrypted payload containing session information, and an authentication hash.

By manipulating the Era parameter to values between 2 and 9, attackers can trigger the out-of-bounds read that forces the system to use compromised encryption keys.

Affected Versions and Severity Assessment

Fortinet has assigned a CVSS v3.1 score of 7.7 (High severity) to this vulnerability. Multiple FortiWeb versions across different release branches are affected:

FortiWeb Version	Affected Releases	Recommended Action
FortiWeb 8.0	Not affected	Not applicable
FortiWeb 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiWeb 7.4	7.4.0 through 7.4.7	Upgrade to 7.4.8 or above
FortiWeb 7.2	7.2.0 through 7.2.10	Upgrade to 7.2.11 or above
FortiWeb 7.0	7.0.0 through 7.0.10	Upgrade to 7.0.11 or above

The researcher demonstrated successful exploitation through REST API endpoints and CLI connections, showing how attackers can impersonate administrative users.

However, the attack has several limitations that reduce its practical impact. Exploitation requires brute-forcing an unknown validation number and necessitates that target users maintain active sessions during the attack window.

Note:

- The details provided about CVE vulnerabilities are based on publicly available sources, security advisories, and threat intelligence feeds. While efforts are made to ensure accuracy, the information may change over time.
- The severity scores (CVSS) and descriptions are for general reference. Organizations must conduct their own risk assessments based on their unique environment, configurations, and security posture.
- While patching and mitigation recommendations are provided, implementation decisions should be made based on an organization's security policies, compatibility testing, and vendor guidance.
- CVEs may be updated with new exploitation techniques or patches over time. Regular monitoring of official sources (e.g., NVD, MITRE, vendor advisories) is recommended.

Section 2 - Reported Cyber Breaches

Title: Sanderling Healthcare Ransomware Breach Under Scrutiny by Levi & Korsinsky, LLP

Impacted Sector: Healthcare

Attack Summary:

Sanderling Healthcare recently disclosed that it suffered a data breach that compromised the sensitive personal and protected health data of individuals. This data breach has led to concerns over the security of sensitive personal and protected health information entrusted to Sanderling Healthcare.

WHAT'S THIS ABOUT?

On July 3, 2025, Sanderling Healthcare experienced a ransomware attack involving the unauthorized disclosure of the company's database system.

Potentially compromised information includes names, dates of birth, contact details, Social Security numbers, driver's license or state ID numbers, medical and health insurance records, and payment data. While Sanderling Healthcare has yet to issue a formal public notice, it may soon begin notifying individuals whose information may have been affected. Those who are informed of the breach could be eligible for compensation.

Data breaches are serious matters that can cause long-term damage. Hackers may use stolen information to commit identity theft, financial fraud, or other crimes. Companies that fail to secure your personal data may be held liable for the resulting harm.

References:

- https://www.marketwatch.com/press-release/sanderling-healthcare-data-breach-under-investigation-by-levi-korsinsky-llp-faef116f
- https://www.classactionlawyers.com/blog/sanderlinghealth

Title: Michigan Medicine sends postcards without envelopes, exposing personal data of 1,015

Impacted Sector: Healthcare

Attack Summary:

Michigan Medicine experienced a data breach on June 27 when postcards intended to recruit people for a research study were mailed without envelopes, exposing personal health information. This incident affected 1,015 individuals.

The postcards, which contained "a limited amount" of health information, were sent by recruiters for a medical study at Michigan Medicine. This design allowed anyone handling the mail to see personal details. Michigan Medicine, the academic medical center of the University of Michigan, reported this incident on August 14. Jeanne Strickland, Michigan Medicine chief compliance officer, expressed regret and stated that the organization immediately investigates such situations.

Investigations revealed that the University of Michigan's Institutional Review Board (IRB), which oversees human subjects in medical research, had mistakenly approved the mailing of these postcards. In response, the IRB is implementing measures to prevent similar incidents, including providing staff-wide education on protecting personal health information.

Affected individuals were notified by mail on August 14. While Michigan Medicine believes the risk of identity theft from this breach is low, they advise those impacted to monitor their medical insurance statements for any fraudulent transactions.

References:

- https://www.hipaajournal.com/data-breach-langdon-company-michigan-medicine/
- https://www.freep.com/story/news/health/2025/08/14/university-of-michigan-medicine-research-study-data-breach-postcards/85655904007/

Title: Colt Telecom attack claimed by WarLock ransomware, data up for sale

Impacted Sector: Telecom

Attack Summary:

UK-based telecommunications company Colt Technology Services is dealing with a cyberattack that has caused a multi-day outage of some of the company's operations, including hosting and porting services, Colt Online, and Voice API platforms.

The British telecommunications and network services provider disclosed that the attack started on August 12 and the disruption continues as its IT staff works around the clock to mitigate its effects.

Founded in 1992 as City of London Telecommunications (COLT) and acquired by Fidelity Investments in 2015, Colt is a major telecommunications service provider operating in 30 countries across Europe, Asia, and North America. The company employs 75,000 km of fiber networks linking 900 data centers.

Services still offline

Initially, the company announced a "technical issue" without confirming a cyber incident. However, the nature of the event was communicated in subsequent status updates.

The attack forced the firm to take specific systems offline as a protective measure, which affected the operations of support services, including Colt Online and the Voice API platform.

Customer communication through online portals is currently unavailable, and clients are advised to contact Colt by email or phone and expect slower-than-usual responses.

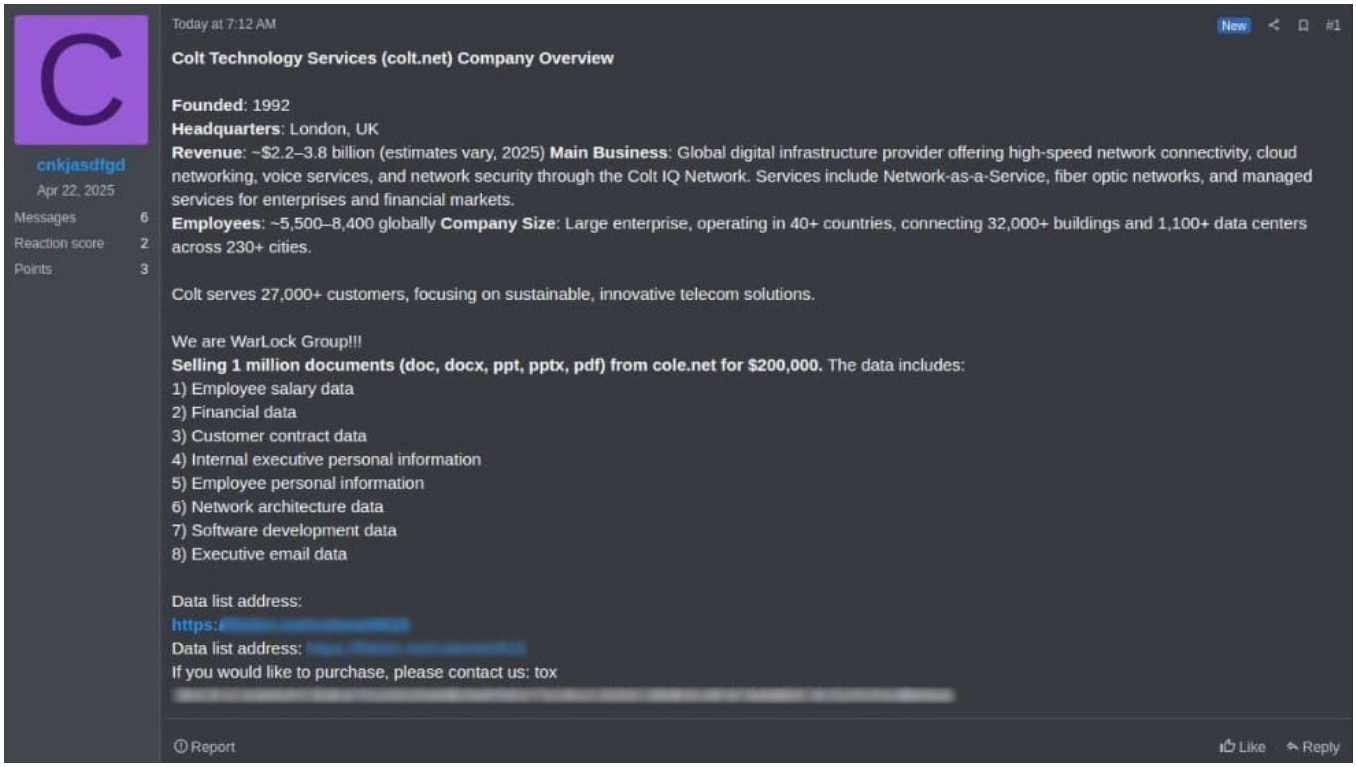
The company underlined that the impacted systems are support services, not the core customer network infrastructure.

As of today, there is no estimation for restoring affected systems and operations.
Colt says it has notified the authorities about the incident without providing any details about the perpetrators or the type of attack.

WarLock claims the attack

A threat actor using the alias 'cnkjasdfgd' and claiming to be a member of the WarLock ransomware gang claimed the attack and offered to sell for $200,000 a batch of one million documents allegedly stolen from Colt.

Several data samples have also been published to prove the validity of the files. According to the threat actor, the stolen files include financial, employee, customer, and executive data, internal emails, and software development information.



Threat actor's post on a hacker forum

Source: KELA

Although the telecommunications company did not disclose the cause of the breach, security researcher Kevin Beaumont says that the hacker likely managed to gain initial access by exploiting a remote code execution vulnerability in Microsoft SharePoint tracked as CVE-2025-53770.

The security issue has been exploited as a zero-day since at least July 18 and is considered critical in severity. Microsoft addressed it in a security update on July 21.
According to Beaumont, the hackers stole a few hundred gigabytes of files with customer data and documentation.

"We're aware of claims regarding the cyber incident. We are currently investigating these claims."

"Our technical team is focused on restoring the internal systems impacted by the cyber incident and is working closely with third-party cyber experts. We are grateful for our customers' understanding as we work towards a resolution to fix the impacted internal systems." - Colt spokesperson

References:

- https://www.bleepingcomputer.com/news/security/colt-telecom-attack-claimed-by-warlock-ransomware-data-up-for-sale/

Title: Bouygues Telecom confirms data breach impacting 6.4 million customers

Impacted Sector: Telecom

Attack Summary:

Bouygues Telecom warns it suffered a data breach after the personal information of 6.4 million customers was exposed in a cyberattack.

The company is one of the largest telecommunication service providers in France, offering mobile, internet, and IPTV services. Bouygues Telecom has 14.5 million mobile subscribers, 9,000 employees, and an annual revenue of €56.8 billion ($66B).

Bouygues Telecom confirmed in a FAQ and a press statement that the attack occurred last Sunday, August 4, 2025.

Although Bouygues Telecom says that there has been no impact observed on customer services or networks, the personal data of 6.4 million customers was compromised.

“Bouygues Telecom was the victim of a cyberattack that allowed unauthorized access to certain personal data from 6.4 million customer account,” reads the translated press statement.

“The situation was resolved as quickly as possible by Bouygues Telecom’s technical teams, and all necessary additional measures have been implemented.”

A previous statement says that internal investigations confirmed that the attack was orchestrated by a ‘known cybercriminal group’ that targeted ‘specific internal resources.’

The firm informed the French National Cybersecurity Agency (ANSSI) and the CNIL (French data protection authority) accordingly, noting that the perpetrator could face up to 5 years of imprisonment and a €150,000 fine for this attack.

According to the FAQ, the following customer information was stolen:

- **Contact details**
- **Contract information**
- **Civil status data**
- **Company details (for business customers)**
- **International Bank Account Numbers (IBANs)**

Importantly, the company said that no credit card numbers or Bouygues Telecom account passwords were compromised.

The company has now blocked the attacker’s access to its network, increased monitoring, and implemented additional security measures.

Customers are being informed of the breach directly via SMS and email, but the situation has exposed them to fraud and phishing risks.

Bouygues Telecom urges its customers not to give away sensitive information like their login credentials to people calling them and mentioning their name and account number to gain their trust.

Although the leaked IBANs are not enough for initial transfers, impacted individuals are still advised to regularly check their debits and contact their bank immediately if they notice suspicious activity.

Just last week, another French telecommunications giant, Orange, disclosed a similar network breach that occurred on July 25, 2025.

Investigations to determine whether customer data was stolen are still ongoing, and the company has not published an update on this.

These incidents targeting European telecom providers echo similar attacks against U.S.-based telcos, attributed to Chinese cyber-espionage agents of the Salt Typhoon hacking group.

References:

- https://www.bleepingcomputer.com/news/security/bouygues-telecom-confirms-data-breach-impacting-64-million-customers/

Title: Google Hacked – Approx 2.5 Million Records of Google Ads Customer Data Leaked

Impacted Sector: Generic

Attack Summary:

Google has disclosed a significant data breach involving one of its corporate Salesforce instances, compromising customer data tied to its Google Ads platform.

Google has not revealed the exact number of people impacted, but according to ShinyHunters, who spoke with Cyber Security News, the breach exposed around 2.5 million records (Approx). Whether some of these entries are duplicates is still unknown.

The incident, detected in June 2025, was perpetrated by a financially motivated threat group tracked as UNC6040, known for its advanced voice phishing (vishing) tactics.

Google notified GBHackers News that the completed email notifications to affected customers on August 8, 2025, following an initial announcement on August 5.

The breached Salesforce instance stored contact information and related notes for small and medium businesses using Google Ads. According to Google's Threat Intelligence Group (GTIG), the stolen data included basic, largely publicly available business information, such as:

- **Business names**
- **Contact details (e.g., email addresses, phone numbers)**
- **Related notes stored in the Salesforce instance**

While Google has stated that the compromised data was limited in scope and primarily publicly accessible, the breach raises concerns due to the potential for this information to be used in subsequent extortion schemes.

The threat actor retrieved the data during a brief window before Google revoked access, though specific details on the volume of affected records were not disclosed.

According to a Cyber Security News report, ShinyHunters demanded 20 Bitcoins (approximately $2.3 million) from Google. However, the threat actor later claimed this was sent "for the lulz" rather than as a serious extortion attempt.

The Attack and Extortion Threats

The breach was executed by ShinyHunters, who also claim collaboration with threat actors associated with Scattered Spider, now referring to themselves collectively as "Sp1d3rHunters."

This group is responsible for gaining initial access to targeted systems, enabling ShinyHunters to conduct data exfiltration from Salesforce environments.

The attackers used a modified version of Salesforce's Data Loader application, authorized through sophisticated voice phishing (vishing) tactics where employees were deceived into approving a malicious connected app.

GTIG notes that the group has evolved its tactics, shifting to custom Python scripts and using Mullvad VPN IPs or TOR to mask their activities.

ShinyHunters has been linked to extortion efforts tracked as UNC6240, contacting victims via emails from addresses like shinycorp@tuta[.]com and shinygroup@tuta[.]com, demanding bitcoin payments within 72 hours.

GTIG warns that the group may escalate by launching a data leak site (DLS) to pressure victims, including those affected by the Google Ads breach.

Extortion attempts often occur months after the initial theft, suggesting collaboration with other actors to monetize stolen data.

The attack highlights UNC6040 refined methods, including the use of compromised accounts from unrelated organizations to register malicious apps and automated data collection via TOR.

GTIG also observed infrastructure overlaps with "The Com," a loosely organized cybercrime collective, indicating potential shared tactics among associated actors targeting cloud platforms like Okta and Microsoft 365.

Google responded promptly, conducting an impact analysis and implementing mitigations to secure the affected Salesforce instance.

References:

- Least Privilege Access: Restrict permissions for tools like Data Loader, particularly the "API Enabled" permission.
- Connected App Management: Implement allowlisting and restrict powerful permissions like "Customize Application" to trusted administrators.
- IP Restrictions: Define trusted IP ranges to block unauthorized access from VPNs or TOR.
- Salesforce Shield: Use transaction security policies and event monitoring to detect suspicious activities, such as large data downloads.
- Multi-Factor Authentication (MFA): Enforce MFA universally and educate users on social engineering tactics to prevent MFA bypass.

References:

- https://gbhackers.com/google-hacked/

Title: Hack at UnitedHealth's tech unit impacted 192.7 million people, US health dept website shows

Impacted Sector: Healthcare

Attack Summary:

As of August 14, Reuters reports that a cyberattack on UnitedHealth Group's technology subsidiary, Change Healthcare, has now been confirmed to have affected approximately 192.7 million individuals, according to the U.S. Department of Health and Human Services' breach database. This marks a notable increase from the company's January estimate of 190 million people affected.

Originally disclosed in February 2024, the incident—now recognized as the largest healthcare-related data breach in U.S. history—was orchestrated by hackers identifying themselves as the "BlackCat" ransomware group, who disrupted nationwide claims processing systems, with broad repercussions for patients and providers.

A UnitedHealth spokesperson confirmed:

"The final total number of individuals impacted by the Change Healthcare cyberattack is approximately 192.7 million," adding that impacts will vary by state.

The compromised data includes health insurance member IDs, patient diagnoses, treatment details, Social Security numbers, and provider billing codes

References:

- https://www.reuters.com/business/hack-unitedhealths-tech-unit-impacted-1927-million-people-us-health-dept-website-2025-08-14/

Section 3 - OT/IoT Security Breaches

Title: OT Disruptions Could Cost $330B Globally

Impacted Sector: OT

Attack Summary:

A new analysis from Dragos and Marsh McLennan models a catastrophic cyber event that disrupts operational technology at global scale. The headline number is stark. Losses could approach 330 billion dollars in a one in 250 year scenario. More than half of that, around 172 billion dollars, would come from business interruption. The estimate folds in supply chain ripple effects and related knock on costs. The report's core message is simple. The direct breach is rarely the most expensive part. The downtime is.

Manufacturing, energy, food logistics and other critical sectors now depend on connected plant. Remote access tools, cloud linked historians and vendor maintenance paths are common. When a production line stops, it is not only throughput that falls. Raw materials spoil, transport slots are missed, service level penalties accrue, and working capital balloons as inventory piles up. Many firms still budget as if OT will behave so long as IT looks healthy. The report argues that this assumption hides the largest exposure on the balance sheet.

Recent disclosures underline the financial stakes. Marks and Spencer booked a 400 million dollar hit after a social engineering attack linked to Scattered Spider disrupted online operations. United Natural Foods said a separate incident tied to the same group would cost at least 350 million dollars in sales. These cases are not identical to an OT plant shutdown, yet they show how fast losses compound when core business systems are offline or constrained. The same dynamic applies in factories and terminals, only with added safety, quality and regulatory risks.

The USD 330 billion figure not as a forecast for the coming year, but as a "tail risk" estimate derived from a decade of breach and claims data, accompanied by an average annual risk of USD 12.7 billion and a one-year aggregated risk of USD 31 billion—serving as crucial planning benchmarks for boards. It underscores that merely investing in perimeter and IT tools doesn't address the core vulnerabilities in OT environments; instead, critical investments should aim to reduce the time to detect, contain, and restore production. Three foundational OT controls are shown to deliver the greatest risk reduction: a fully developed and tested incident response plan tailored for OT operations; defensible network architecture with segmented zones, tightly controlled vendor access, and backup systems; and continuous OT monitoring, including traffic baselines and change detection. Collectively, these measures help minimize downtime, curtail production losses, and mitigate cascading disruptions.

The three controls that move the needle

The report highlights three OT controls that correlate most with risk reduction. They are not exotic. They are fundamentals that too many plants still lack or only partly implement.

- A comprehensive incident response plan for OT. Build and test a plan that includes isolation steps at the line, cell and device level. Include clear call trees, offline copies of network maps, golden images for key servers and engineering workstations, and a path to manual workarounds where safe. Run joint exercises with operations, safety, legal and communications. Measure time to safe shutdown and time to minimum viable production.

- Defensible architecture. Segment trusted zones, restrict east west movement and separate IT from OT with monitored conduits. Treat vendor remote access as a product in its own right. Use jump hosts, time bound approvals, multi factor authentication and per session recording. Apply allow lists for industrial protocols. Protect domain controllers, historians and recipe servers as crown jewels. Keep spares and images for PLCs and HMIs to speed rebuilds.

- Continuous monitoring for OT visibility. Collect logs from switches, firewalls and industrial devices. Deploy passive network detection where active scans could be unsafe. Establish baselines for normal traffic and alert on changes in firmware, configuration or new communications paths. Map dependencies between lines and shared services so responders know which lever to pull first.

- Many organisations still invest the majority of cyber budget in IT. The logic is understandable. IT tooling is familiar, audit friendly and easy to benchmark. OT risk does not fit as neatly into a dashboard. Yet the financial analysis shows that the largest checks get written when production halts. A balanced program aligns spending with potential loss, not with organisational habit.

That means dedicated OT security engineering, a service catalogue for vendor access, and maintenance windows that include cyber hardening alongside mechanical work.

References:

- https://www.thehackacademy.com/feature/the-330-billion-dollar-ot-risk-why-business-interruption-is-the-real-threat/

- OT Disruptions Could Cost $330B Globally | Security Magazine

The Indicators of compromise (IOCs) have been attached in an excel sheet based on the categories for IP, Domain, URL & Hash which are involved in attacks & breaches.

Disclaimer

“Cyber threats are constantly evolving, and the tactics, techniques, and procedures (TTPs) described in this report may change over time. Continuous monitoring and threat intelligence updates are recommended to maintain an effective security posture.”

Feedback

“We welcome your feedback to enhance the accuracy, relevance, and effectiveness of our threat intelligence reports. Please share your insights or recommendations to help us improve future editions and better support your security needs.”

Contact us on “Threat Advisory <threatadvisory@colortokens.com>”

About ColorTokens:

ColorTokens is a leading provider of enterprise microsegmentation and breach containment solutions, dedicated to making organizations “breach ready.” By preventing the lateral spread of ransomware and advanced malware, ColorTokens protects complex network infrastructures through its innovative Xshield™ platform. The platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enabling the enforcement of granular micro-perimeters, swift isolation of critical assets, and effective breach response. Recognized as a Leader in the Forrester Wave™: Microsegmentation Solutions (Q3 2024), ColorTokens delivers proactive security that prevents disruptions and safeguards global enterprises. For more information, visit www.colortokens.com

Copyright 2025 © ColorTokens. All rights reserve