



ZEROFOX[®]

Weekly Intelligence Brief

Classification: TLP:GREEN

October 7, 2024

Scope Note

ZeroFox's Weekly Intelligence Briefing highlights the major developments and trends across the threat landscape, including digital, cyber, and physical threats. ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 PM (EDT) on October 4, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Weekly Intelligence Brief |

 This Week's ZeroFox Intelligence Reports	2
ZeroFox Intelligence Brief: Cyber Threats to the U.S. Elections	2
ZeroFox Intelligence Brief: Physical Threats to the U.S. Elections	2
 Cyber and Dark Web Intelligence Key Findings	4
DoJ Charges 18 in a Deadly Global Counterfeit Drug Operation	4
NCA Unveils LockBit Affiliates and Sanctions 16 Evil Corp Members	4
U.S. Charges Individuals in Cyberattacks Targeting Electoral Campaigns	5
 Exploit and Vulnerability Intelligence Key Findings	7
CVE-2024-0132	8
CVE-2024-41988	9
 Ransomware and Breach Intelligence Key Findings	11
Ransomware Attacks Disrupt Various Sectors	11
Major Breaches and Settlements Across Critical Infrastructure Entities	12
 Physical and Geopolitical Intelligence Key Findings	15
Physical Security Intelligence: Global	15
Physical Security Intelligence: United States	16
 Appendix A: Traffic Light Protocol for Information Dissemination	17
 Appendix B: ZeroFox Intelligence Probability Scale	18

| This Week's ZeroFox Intelligence Reports

ZeroFox Intelligence Brief: Cyber Threats to the U.S. Elections

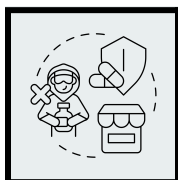
The cyber threats posing risks to the U.S. presidential election to be held on November 5, 2024, illustrate the increasing interconnectivity of the cyber and geopolitical domains. There is substantial variance in the types of threat actors that demonstrate a level of perceived investment in the future U.S. leader, American political stability, or Western nations' ability to maintain their democratic processes. These threat actors are harnessing a more diverse arsenal than ever before—placing increasing strain on security teams to ensure the election remains transparent and trustworthy. Threat actors are using malicious tools to cause disruption or breach networks and steal data, either as a part of an espionage campaign or in pursuit of financially or ideologically motivated objectives. Legitimate tools are also being leveraged, with threat actors using social media platforms and online forums as vehicles to deliver payloads of mis-, dis-, and malinformation (MDM). In the coming weeks, it is very likely that the tempo and potency of cyber activity that actively targets or otherwise exploits the election will increase. While this will likely culminate on November 5, malicious cyber activity will very likely continue for as long as associated elements remain sufficiently topical for use in malicious activities.

ZeroFox Intelligence Brief: Physical Threats to the U.S. Elections

There is an elevated risk of political violence related to the upcoming 2024 U.S. presidential elections. Prior to the assassination attempt on former President Donald Trump at his campaign rally in Butler, PA, the most substantial threats came from those concerned with the integrity of U.S. elections. The overall threats stem from an uptick in politically motivated violence, including physical attacks and death threats that have targeted political candidates, their supporters, government officials, and polling locations since the 2020 election. Passionate opinions related to campaign issues like immigration, wars in Ukraine and Gaza, LGBTQ+ rights, and access to abortion could also lead to violence. The primary risk locations are battleground states and areas where elections were contested in 2020.

| Cyber and Dark Web Intelligence |

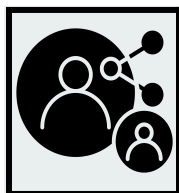
| Cyber and Dark Web Intelligence Key Findings



DoJ Charges 18 in a Deadly Global Counterfeit Drug Operation

What happened: The U.S. Department of Justice (DoJ) has charged 18 individuals involved in a scheme selling counterfeit pills disguised as legitimate pharmaceutical products. The pills, primarily containing fentanyl and methamphetamine, were marketed through numerous fraudulent online pharmacies. Tens of thousands of unsuspecting victims purchased these counterfeit pills, resulting in at least nine fatalities due to narcotics poisoning. Law enforcement agencies seized nine website domains, counterfeit tablets, and substantial quantities of raw narcotics and manufacturing equipment at various pill mills. The drug trafficking operation—which spanned multiple countries, including the United States, the Dominican Republic, and India—had an extensive reach and a large scale of impacts and consequences.

- **What this means:** Unregulated online pharmacies are a major threat to the healthcare industry. Schemes like these lure individuals seeking legitimate medication, taking advantage of their circumstances for monetary gains. Such operations also contribute to broader public health concerns—particularly in the context of the opioid crisis, as the availability of counterfeit drugs online increases the risk of misuse and adverse outcomes. The fake pills, designed to mimic real medications, create a false sense of security among consumers and often prove fatal to some. The impact of such operations extends beyond individual tragedies; they are very likely to cause financial losses, physical harm, and mental health deterioration for the victims. Spreading awareness of the dangers and providing tips on identifying legitimate internet pharmacies are likely to help mitigate the risks associated with online medication purchases and protect individuals from these deadly scams.

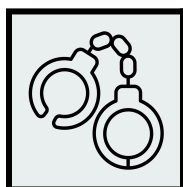


NCA Unveils LockBit Affiliates and Sanctions 16 Evil Corp Members

What happened: The United Kingdom (UK)'s National Crime Agency (NCA) has reactivated the seized "LockBit" darknet site to provide crucial updates on recent developments in its ongoing investigations. Among the revelations, the NCA identified Aleksandr Ryzhenkov as a member of the Russian cybercrime group "Evil Corp" and also as a LockBit affiliate known as "Beverley." Ryzhenkov

is believed to have created over 60 variants of LockBit ransomware and to have attempted to extort at least USD 100 million from various victims. The agency also announced the arrest of a significant actor within the LockBit network, alongside multiple arrests in the UK connected to this cybercrime operation. Britain imposed [sanctions](#) on 16 members of Evil Corp, citing their involvement in operations directed by Russian intelligence against NATO allies.

- **What this means:** The recent sanctions imposed by the NCA are crucial in addressing the ongoing threat posed by Evil Corp, which has been identified as a significant global cyber menace linked to LockBit. These measures, along with recent arrests and server seizures, are vital to disrupting LockBit's operations and prosecuting its core members. The NCA's identification of Aleksandr Ryzhenkov as a member of both Evil Corp and an affiliate of the LockBit network reflects a troubling trend in cybercrime: the increasing sophistication and interconnectedness of threat actor organizations. Ryzhenkov's creation of over 60 variants of LockBit ransomware and his attempts to extort more than USD 100 million indicate a strategic effort to maximize impact while evading detection by targeting a wide range of organizations, from small businesses to large corporations. The NCA's actions are part of a coordinated effort with international partners to focus on key figures within LockBit and Evil Corp. These authorities aim to disrupt criminal activities and mitigate risks to critical infrastructure and national security, as well as expose the groups' ties to state-affiliated cyber espionage.



U.S. Charges Individuals in Cyberattacks Targeting Electoral Campaigns

What happened: The DoJ has unsealed charges against three individuals allegedly linked to the Islamic Revolutionary Guard Corps (IRGC) that are accused of hacking into accounts of current and former U.S. officials to steal campaign material in order to influence the 2024 election. According to the Department of Public Affairs, the activity was part of Iran's continuing efforts to stoke discord, erode confidence in the U.S. electoral process, and unlawfully acquire information relating to current and former U.S. officials that could be used to advance the malign activities of the IRGC—including ongoing efforts to avenge the death of Qasem Soleimani, the former commander of the IRGC – Qods Force (IRGC-QF). The announcement comes days after U.S. authorities [accused](#) Iranian actors of hacking into the accounts of officials associated with former President Donald Trump's campaign and attempting to share exfiltrated information with President Joe Biden's campaign staff.

- **What this means:** The unsealed charges against individuals linked to Iran's IRGC highlight the larger threat foreign interference poses to U.S. elections, particularly by

state-sponsored cyber actors. The alleged hacking, targeting the accounts of U.S. officials to steal campaign materials, demonstrates how Iran likely seeks to sway outcomes and weaken the integrity of the electoral process. Attempting to gather sensitive information that could be used to influence outcomes or damage political figures likely aligns with the IRGC's broader geopolitical objectives, including retaliation for the death of its former commander, Qasem Soleimani. Additionally, as Iran is a key player in the ongoing conflicts in the Middle East, IRGC hackers will likely continue to contribute to efforts aimed at disrupting the U.S. elections or threatening electoral operations by disseminating incendiary dis- or misinformation.

| Exploit and Vulnerability Intelligence |

| Exploit and Vulnerability Intelligence Key Findings

In the past week, ZeroFox has observed vulnerabilities, exploits, and updates disclosed by prominent companies involved in technology, software development, industrial control systems (ICS), and government services. The Cybersecurity & Infrastructure Security Agency (CISA) has added five [vulnerabilities](#) to its known exploited vulnerabilities (KEV) catalog: [CVE-2024-29824](#),

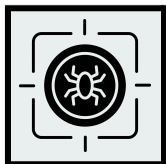
CVE-2023-25280, CVE-2021-4043, CVE-2020-15415, and CVE-2019-0344. In addition to these, CISA has also released [two](#) (CVE-2024-41925 and CVE-2024-45367) ICS advisories. [CVE-2024-0132](#) is a critical vulnerability that affects the NVIDIA Container Toolkit, posing a risk to all artificial intelligence (AI) applications that utilize it for GPU access in cloud or on-premise settings. The Zimbra remote code execution flaw, tracked as [CVE-2024-45519](#), is an SMTP vulnerability exploit script overview. This script checks for vulnerabilities in an SMTP server and, if found, exploits the vulnerability by establishing a reverse shell connection to the machine. [CVE-2024-45489](#) is a vulnerability that enables attackers to exploit Arc's use of Firebase for authentication and database management, allowing them to execute arbitrary code in a target's browser. Tracked as [CVE-2024-34102](#), this critical vulnerability (CVSS score of 9.8) involves improper restrictions on XML external entity references (XXE), which could lead to remote code execution. Security researchers have revealed a serious flaw in CUPS, an open-source printing system based on the Internet Printing Protocol, which could enable an attacker to remotely execute malicious commands by manipulating URLs through a combination of [four](#) vulnerabilities. These include CVE-2024-47176 in "cups-browsed," CVE-2024-47076 in the "libcupsfilters" library, CVE-2024-47175 in the "libppd" library, and CVE-2024-47177 in the "cups-filters" package. [CVE-2024-41988](#) is a critical remote code execution (RCE) bug in the TEM Opera Plus FM Family Transmitter that allows access to an unprotected endpoint, potentially leading to MPFS File System binary image upload without authentication. [CVE-2024-43699](#) is a critical bug in Delta Electronics DIAEnergie is an SQL injection in the script AM_RegReport[.]aspx. An unauthenticated attacker may be able to exploit this issue to retrieve records or cause a denial of service.

**CRITICAL****CVE-2024-0132**

What happened: A critical vulnerability (CVE-2024-0132) in the NVIDIA Container Toolkit poses severe risks to AI applications utilizing GPU resources. The flaw enables container escape attacks, allowing attackers to gain full access to the host system and execute commands. More than 35 percent of cloud environments are at risk. NVIDIA acknowledged the issue and released a fix on September 26.

- **What this means:** The vulnerability has immediate implications for cloud security, especially for organizations leveraging NVIDIA's technology for AI applications. Attackers could exploit systems with an unpatched NVIDIA Container Toolkit to gain unauthorized access and conduct data breaches or ransomware attacks, impacting operational confidentiality and networks.
- **Affected products:**

- NVIDIA Container Toolkit versions 1.16.1 and earlier
- GPU Operator versions 24.6.1 and earlier



CRITICAL

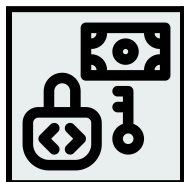
CVE-2024-41988

What happened: TEM Opera Plus FM Family Transmitter allows access to an unprotected endpoint, potentially enabling MPFS File System binary image upload without authentication. This file system serves as the basis for the HTTP2 web server module but is also used by the SNMP module and is available to other applications that require basic read-only storage capabilities. This can be exploited to overwrite the flash program memory that holds the web server's main interfaces and execute arbitrary code.

- **What this means:** The TEM Opera Plus FM Family Transmitter application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.
- **Affected product:**
 - Opera Plus FM Family Transmitter: Version 35.45

Ransomware and Breach Intelligence

Ransomware and Breach Intelligence Key Findings



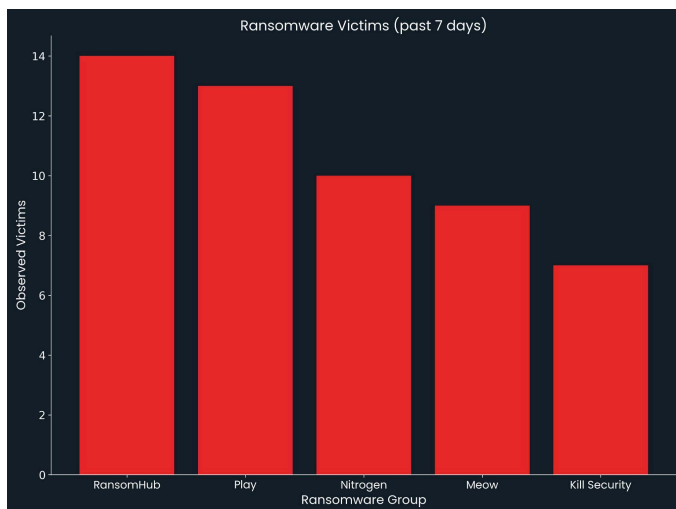
Ransomware Attacks Disrupt Various Sectors

What happened: In the past week, ZeroFox Intelligence has observed over 50 ransomware attacks, with manufacturing being the most targeted sector and North America being the most targeted region.

“RansomHub” emerged as the most active group in the past week. A ransomware attack [hit](#) the University Medical Center (UMC)—a major hospital in Lubbock, Texas—forcing it to divert ambulances and limit emergency services. After spotting unusual network activity, the hospital shut down affected systems and involved a

third party to investigate the incident. A threat actor

called “PaidMemex” has been using a new “MedusaLocker” ransomware variant, BabyLockerKZ, to [infect](#) over 100 organizations per month since 2022. The actor targets diverse industries globally, focusing on small and medium-sized businesses, with attacks peaking in mid-2023 before declining in 2024. Meanwhile, law enforcement continues to [crack down](#) on LockBit, with four more arrests this week—including those of a developer, a bulletproof hosting service administrator, and two individuals associated with LockBit.



Source: ZeroFox Internal Collections

- **What this means:** Details on the impact on UMC’s systems are still unclear, but UMC Health System stated the attack hit “multiple systems,” disrupting its phone system and blocking access to patient portal messages. UMC is crucial for the Lubbock populace because it is the only level-one trauma center within a 400-mile radius. A cyberattack shutting down emergency operations for such a hospital poses a direct risk to the safety and lives of those who need urgent critical care. Hospitals—with repositories of sensitive information and the need to resolve network disruptions as soon as possible—are lucrative targets for financially motivated actors like ransomware groups. Ransomware attacks in healthcare have [risen](#) 67 percent in 2024, with recovery times worsening and costs increasing. Attackers exploit vulnerabilities and compromised credentials, and data theft is prevalent. ZeroFox has detected more than 430 ransomware and digital extortion victims in the

healthcare sector in the past year, close to 70 percent of which are in North America. Meanwhile, PaidMemes' activity reflects a shift in ransomware activity toward smaller organizations, indicating that these firms are becoming prime targets due to their susceptibility and lower cybersecurity budgets. The trend is likely to result in increased financial strain and operational disruptions for these entities, which are less-equipped to handle attacks and ransom payments.



Major Breaches and Settlements Across Critical Infrastructure Entities

What happened: “Kimsuky APT”, linked to the North Korean government, [breached](#) a German defense company that manufactures Iris-T air defense systems. They employed a phishing campaign featuring fake job offers and sophisticated social engineering techniques to break into the company’s systems. The Federal Communications Commission (FCC) announced a multi-million dollar settlement with [T-Mobile](#) due to multiple data breaches that compromised the personal information of millions of users. The Community Clinic of Maui (Hawaii) [experienced](#) a LockBit ransomware attack earlier this year, compromising the sensitive information of over 120,000 individuals that included personal and medical data; there is reportedly no evidence of identity theft. The breached data includes names, Social Security numbers (SSNs), dates of birth, and more. In response, the clinic is implementing enhanced security measures to prevent future incidents. Sellafield Ltd, the company running the Sellafield nuclear site, was [fined](#) GBP 332,500 for persistent cybersecurity shortfalls that left its IT systems vulnerable to unauthorized access and data loss. While no breaches were exploited, internal findings highlighted risks from phishing attacks or malicious insiders that could disrupt operations and delay decommissioning efforts.

- **What this means:** The attack on the German defense company, which is involved in the manufacturing of critical systems like the Iris-T air defense and other missiles and ammunitions, presents significant risks to global security. Such breaches can result in the theft of sensitive military technologies, weakening not only the company but also the defense capabilities of connected nations that rely on these systems. The FCC’s settlement addresses T-Mobile’s repeated failures to safeguard customer data, resulting in multiple breaches affecting millions. The exposure of sensitive information, including names, addresses, and SSNs, significantly increases the risk of identity theft, financial fraud, and privacy violations for customers. The Community Clinic of Maui breach exposes highly sensitive personal and medical information, making over 120,000 individuals vulnerable to identity theft, fraud, and potential misuse of their healthcare data. Such a large-scale

breach can have long-term consequences for the victims, including financial loss, damaged credit, and privacy violations. Cybersecurity shortfalls at a nuclear facility like Sellafield pose significant risks to national security, public safety, and the environment. A successful cyberattack could lead to operational disruptions, damage to facilities, or loss of sensitive data, potentially compromising nuclear safety protocols. Given the hazardous materials and complex processes involved, any cyber vulnerability in such a facility could have severe consequences, including delays in decommissioning and heightened risks of accidents or malicious activities.

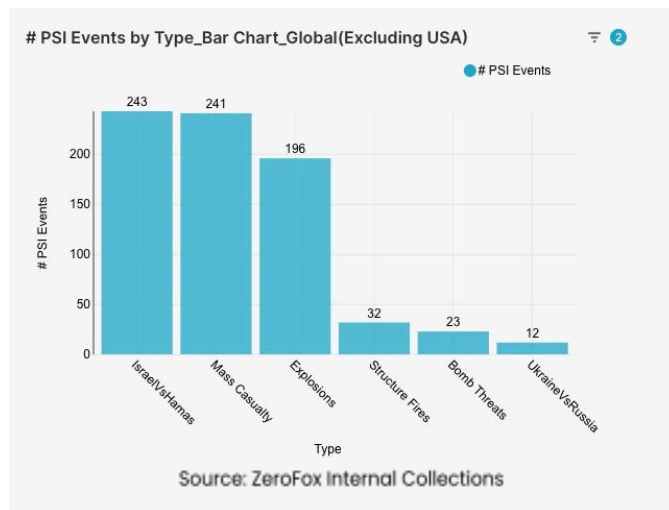
| Physical and Geopolitical Intelligence |

Physical and Geopolitical Intelligence Key Findings

Physical Security Intelligence: Global

What happened: Excluding the United States, there was a 41 percent increase in Mass Casualty incidents this week across the globe, with the top three contributing countries being Lebanon, Israel, and Palestine, in that order; these three countries contributed to almost 72 percent of the total Mass Casualty incidents. General alerts pertaining to the Israel-Hamas conflict increased by 30 percent compared to the previous week, with both Israel and Palestine contributing 38 percent of all Explosion incidents this week. Additionally, there was a 20 percent increase this week over last week of incidents

pertaining to the ongoing Russia-Ukraine war. The top three most alerted subtypes this week were Explosions, Gun Violence, and Structure Fires; Explosions increased by 34 percent, Gun Violence incidents were up by 59 percent, and Structure Fires showed no increase over last week. However, Bomb Threats incidents greatly increased 475 percent over last week.



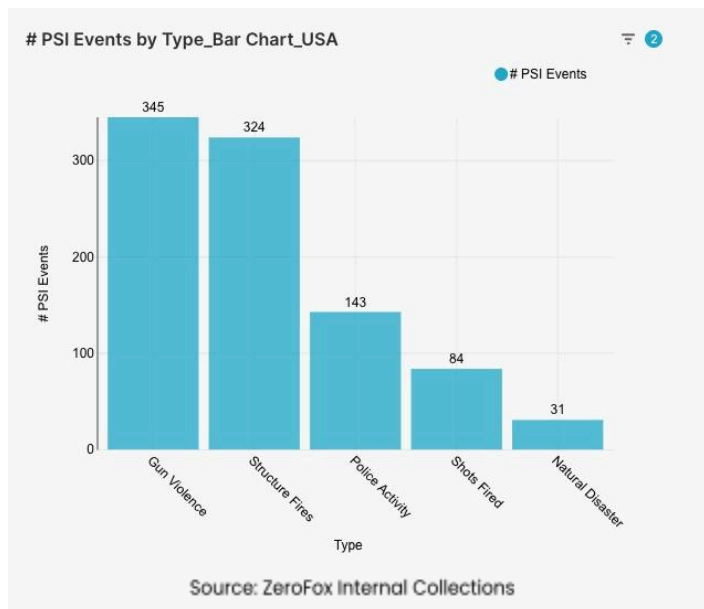
- What this means:** Israel and Hamas-related alerts showed an increase compared to the previous week due to the increasing volatility of the region. The expanded conflict, which [drew in Lebanon](#) in support of Palestine, saw heavy bombardment by Israeli forces this week. On September 27, Israel forces' attacks at the headquarters of Hezbollah in Beirut resulted in the death of leader [Hassan Nasrallah](#), a massive blow to the already dwindling leadership positions of the Hezbollah hierarchy. This week Israel also sent ground troops into southern Lebanon in what was [described](#) as a "limited, localized ground offensive against Hezbollah." This eventually led to Iran, Hezbollah's patron, firing nearly 180 missiles overnight directly into Israeli territory. In contrast to the April missile attacks by Iran, this time the projectiles were able to break through Israeli defenses and hit several targets of vital importance, including a couple of military bases. Additionally, alerts related to the ongoing Russian-Ukraine war showed an increase of 20 percent over the week. Three people were killed in an attack on a [police station](#) in Kryvyi Rih, and [nine people](#) were killed and 12 others injured in an attack on a medical center in Sumy Ukraine.. Bomb Threats saw a massive surge this week, with an increase of 475 percent. Argentina in South America and Philippines in the Southeast clocked in the highest numbers in this category of alerts

Physical Security Intelligence: United States

What happened: In the past week, the most alerted subtypes in the United States were Structure Fires, Police Activity, and Shots Fired. The top two states that had the highest number of Gun Violence incidents were Illinois and California with 69 and 34 alerts, respectively. Together, the two states comprised 31 percent of the total alerts in the category. However, Gun Violence showed no increase compared to the prior week, while School Threats and Active Shooter incidents showed a considerable decline this week compared to last week. Shots Fired

incidents decreased this week compared to the prior week by 7 percent. Structure Fires saw an increase of 24 percent this week compared to the last, with Florida and California contributing to almost 42 percent of the total alerts. Finally, there were 31 alerts related to Natural Disaster compared to 16 last week—an increase of 93 percent.

- **What this means:** In the aftermath of Category 4 Hurricane Helene, death tolls rose to 200. A week afterwards, the destruction left by the hurricane remains with people displaced, no power, limited food, and missing bodies. As the country reels from the devastations of Helene, the National Hurricane Center has confirmed the formation of a Category 4 hurricane named [Kirk](#) and a tropical storm named [Leslie](#). Hurricane Kirk is expected to create large swells on the East Coast and result in local rains but is not expected to make landfall in the United States. The trajectory indicates it is moving to Europe, making landfall in the UK and France by the end of this week. On the other hand, Leslie is a very newly formed tropical storm and is likely to intensify over the next couple of days into a hurricane, closely behind Kirk. This storm is also moving in the direction of the U.S. East Coast. Similarly to last week, California continued to contribute the top two most-alerted subtypes this week. Gun Violence incidents remained the same, while Police Activity-related incidents decreased. Notably, all the major subtypes pertaining to the United States, including School Threats and Active Shooters, showed a large decline in alerts compared to the previous week.



| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%