ADARMA
TOGETHER WE'VE GOT THIS

CRITICAL NATIONAL INFRASTRUCTURE THREAT LANDSCAPE REPORT

Q4 2024

Contents

Purpose

Adarma's Q4 Critical National Infrastructure (CNI) Threat Landscape Report provides a thorough analysis of significant cyber threats, threat actors, and incidents impacting CNI sectors in Q3 2024.

This report, developed by Adarma's Threat Intelligence Team using internal and external sources data, highlights critical insights relevant to CNI, including data from our partner, Recorded Future. While primarily covering the period from July 1 to September 30, 2024, relevant incidents from outside this timeframe are included where applicable.

New or Updated

Adversaries Tracked

New or Updated

Malware Strains Tracked

This figure shows the number of adversaries and malware strains tracked by the Adarma Threat Intelligence Team in Q3 2024.

Insights from Adarma

Where CNI systems once operated in isolation, today's infrastructure increasingly relies on interconnected networks spanning geographical boundaries and industries.

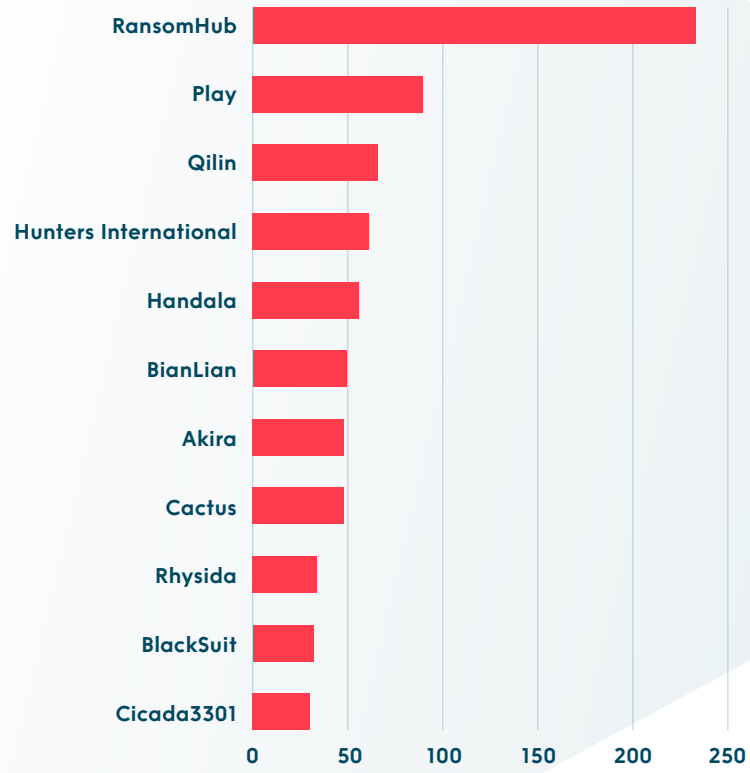
This interconnectedness heightens exposure to cyber threats, attracting a variety of adversaries, from profit-driven cybercriminals to state-sponsored groups aiming for disruption. Rising geopolitical tensions have intensified this risk, as demonstrated by the increased targeting of Ukraine's CNI by Russian threat actors following Russia's invasion of Ukraine.

Ransomware remains the dominant threat, with Q3 activity led by RansomHub, a successful ransomware-as-a-service (RaaS) model, attracting affiliates from LockBit and ALPHV. Other ransomware groups like BianLian and Rhysida have adapted their tactics, exploiting cloud resources like Microsoft Azure tools to mask data exfiltration. Pro-Palestinian hacktivist group Handala intensified their threat by operating a ransomware extortion site, targeting Israeli sectors, including aerospace, defence, and healthcare. Reports of Highly Evasive Adaptive Threat (HEAT) campaigns have also increased, with these advanced techniques allowing attackers extended access to critical systems without detection.

State-sponsored threats and hacktivist activity are also evolving, with groups increasingly blending hacktivism, cybercrime, and espionage. In Q3, state-linked groups such as Andariel and Cadet Blizzard conducted targeted attacks on CNI entities. At the same time, advisories from the Cybersecurity and Infrastructure Security Agency (CISA) and the UK's National Cyber Security Centre (NCSC) highlighted ongoing risks from nation-state campaigns. The UK introduced the Cyber Security and Resilience Bill to mitigate these threats, aiming to strengthen CNI protection through mandatory ransomware reporting and expanding CNI designation to data centres, a critical infrastructure component.

Based on intelligence gathered throughout Q3 2024, the ransomware groups highlighted in the figure shown here, have been the most active on their respective leak sites, targeting various technologies and industry sectors worldwide.

Ransomeware



Key Observed Threats in Q3 2024:

- **EDR-Killing Tools**: In Q3, Endpoint Detection and Response (EDR) tools used to monitor and mitigate endpoint threats were frequently targeted. Groups like FIN7 and RansomHub actively exploited EDR vulnerabilities to disable these defences.
- **Amadey Malware**: Amadey malware was deployed in attacks that compromised credentials within Kiosk Mode, a configuration often used to restrict device functionality to a single application or purpose, typically in public or customer-facing environments.
- **BazaCall Campaign**: The BazaCall campaign used phishing tactics to trick global victims into downloading BazarLoader malware. Once infected, attackers proceeded with data exfiltration and ransomware deployment.

“In response to the ongoing threat from ransomware, the Adarma Threat Intelligence Team has produced several Emerging Threat Hunting packs aimed at helping our customers detect suspicious or malicious activity within their networks. These packs have related to prominent ransomware groups Blacksuit, RansomHub, Qilin and Akira, and have contained several threat hunts based on the group activities and MITRE ATT&CK TTPs.”

Adarma Threat Intelligence Team

Energy, Oil, Gas & Utilities Sectors

Ransomware and hacktivist activities are the primary threats facing the energy, oil, gas, and utilities sectors directly and through supply chain dependencies.

Following earlier hacktivist and Advanced Persistent Threat (APT) attacks on water companies, there has been heightened attention on securing and monitoring Operational Technology (OT) and Industrial Control Systems (ICS) that are connected to the internet.

Publicly disclosed attacks on ICS or Human Machine Interface (HMI) systems have decreased compared to Q1 and Q2 2024, potentially indicating that easier targets have already been compromised or that CNI targets are bolstering their defences. On September 25, 2024, CISA released a bulletin highlighting the risks of exposed OT/ICS systems, warning that threat actors may exploit default credentials, perform brute-force attacks, or apply other low-sophistication methods to access these systems.

Ransomware Activity

This quarter, key ransomware groups targeted the energy, oil, gas, and utilities sectors include RansomHub, PLAY, MEOW, Hunters International, and Qilin. Notable incidents in Q3 included:

JULY

01

July 11

Texas Electric Cooperatives, Inc. (TEC), a non-profit association based in Austin, was hit by the PLAY ransomware group (also known as PlayCrypt). By August 12, TEC notified over a thousand customers of unauthorised access to their network, exposing personally identifiable information (PII) such as names, social security numbers, and driver's licence numbers.

02

July 18

Hayden Power Group, an electrical contractor, suffered a data breach attributed to the Play ransomware group. The attackers reportedly compromised sensitive data, including private and personal confidential information, client documents, budget details, payroll records, accounting files, contracts, tax information, IDs, and financial data.

AUGUST

03

August 21

Oilfield service giant Halliburton disclosed a cyberattack in a filing with the US Securities and Exchange Commission. The company confirmed that the attack led to operational disruptions and data theft. RansomHub was identified as the perpetrator, with an email sent to suppliers indicating the group's involvement. Halliburton continues to experience disruptions, with limited access to portions of their business applications supporting various operations.

Hacktivist Activity

Hacktivist groups, including pro-Russian collectives, have continued targeting energy sector entities in Q3, often employing Distributed Denial-of-Service (DDoS) attacks. In July, the US Department of the Treasury sanctioned two members of the pro-Russian group CARR for attacks on HMIs at water utilities in the US and Poland, part of a broader trend of hacktivists impacting CNI. CARR were responsible for manipulating industrial control system equipment at water supply, hydroelectric, wastewater, and energy facilities in the US and Europe.

Following the arrest of Telegram CEO Pavel Durov by French authorities in August this year, hacktivist groups, primarily led by Russian or Russia-aligned actors, launched DDoS attacks against French targets. One such attack by the Russian Army Cyber Team (RAT) targeted French regional utilities provider Syane, which supplies electricity, gas, and renewable energy services in the Rhône-Alpes region of France. The attack did not appear to cause significant disruption beyond temporary service interruption on Syane's website.

APT Activity

Extensive reporting emerged in Q3 regarding Russia-based hackers compromising a Ukrainian heating utility in January 2024. The attack caused control systems to cool the water running through building pipes. While the incident occurred outside of Q3, it was only reported in July.

In September, the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) released a report detailing an investigation in Ukraine from March 2024. This activity has been attributed to UAC-0002 (also known as Sandworm, APT44). The investigation focused on an attempted destructive attack on nearly 20 Ukrainian energy infrastructure entities, including power, heat, and water supply facilities.

The SSSCIP believes three supply chains were compromised to carry out the attacks, with legitimate specialised software backdooring in one case and service provider accounts from an ICS maintenance and support organisation compromised in another.

In August, Microsoft reported that the Iranian-linked threat actor Peach Sandstorm (also known as APT33, Elfin and Refined Kitten) conducted targeted password-spraying attacks and deployed custom malware against oil and gas companies. Microsoft assesses that these campaigns are intended to gather intelligence for the Iranian government.

Healthcare Sector

The healthcare sector remains a prime target for cyberattacks, not only due to the significant disruptions they can cause to healthcare operations but also because of the highly sensitive patient data at risk of being compromised.

Ransomware Activity

Ransomware has consistently targeted the healthcare sector. The key ransomware groups active in healthcare during this period included RansomHub, Rhysida, Hunters International, Medusa, and Daixin. Notable ransomware incidents in Q3 are as follows:

JULY

AUGUST

01

July 3

Harry Perkins Institute of Medical Research reported a cyber incident affecting servers. The Medusa ransomware group claimed responsibility, publicising 4.6TB of surveillance footage and initially demanding US$500,000 for the data.

02

July 24

American Clinical Solutions, which provides testing for healthcare providers, reported a data breach involving 300,000 patient records, including medical records and insurance information. RansomHub claimed responsibility for the attack on their extortion blog.

03

July 28

Polyco Healthline (UK) was targeted by RansomHub, which publicised the attack to increase ransom pressure.

04

July 29

OneBlood (US) was attacked, impacting blood supplies for over 250 hospitals and initiating blood shortage protocols.

05

August 28

Planned Parenthood (US), a major provider of reproductive health services, disclosed a ransomware attack. RansomHub claimed to have 93GB of sensitive data related to this incident.

Data Breaches

In Q3, the healthcare sector faced significant data breaches, underscoring its ongoing vulnerability to cyber threats that compromise sensitive patient information. A notable incident involved Acadian Ambulance Service, where nearly 2.9 million patient records were compromised. The attack occurred between June 19 and June 21, 2024, but was not disclosed until July 25.

The Daixin Team ransomware group claimed responsibility, alleging the exfiltration of data, including patient names, dates of birth, phone numbers, medical histories, case histories, employment information, symptoms, and suspected drug use. The data was subsequently advertised for sale on the dark web by threat actor Hronikmate.

In August, multiple class-action lawsuits were filed against Acadian Ambulance Service, which began notifying those impacted by the breach in September and offering complimentary credit monitoring and identity theft protection services.

> **"Compromises concerning sensitive patient data can have damaging consequences not only for the healthcare facility but also to the patients if threat actors use it to conduct fraudulent and/or further extortion activity against the individual."**
>
> Adarma Threat Intelligence Team

APT Activity

APT groups associated with Iran, North Korea, and Russia have remained active in the healthcare sector, frequently employing ransomware and cyber-espionage tactics. Each group focuses on different methods and objectives, often aligned with their nation's strategic goals.

In August, Microsoft reported that the Iranian-linked threat actor Peach Sandstorm (also known as APT33, Elfin and Refined Kitten) conducted targeted password-spraying attacks and deployed custom malware against oil and gas companies. Microsoft assesses that these campaigns are intended to gather intelligence for the Iranian government.

Iranian-Aligned Groups

- **MuddyWater (Earth Vetala)**: Since February 2024, MuddyWater has conducted a global phishing campaign deploying BugSleep backdoor malware across various sectors, including healthcare.
- **Pioneer Kitten (Lemon Sandstorm)**: Pioneer Kitten collaborated with ransomware groups like ALPHV (BlackCat) and Ransomhouse, monetising compromised data by selling it on dark web forums.

North Korean-Aligned Groups

- **APT45 (Andariel, Silent Chollima)**: Active in the healthcare sector, APT45 expanded its focus to other CNI sectors in 2024, leveraging ransomware and other advanced techniques.

Russian-Aligned Groups

- **Cadet Blizzard and Ember Bear**: Linked to Russia's GRU Unit 29155, these groups have targeted global CNI, including healthcare, as part of broader cyber-espionage efforts aimed at gathering intelligence and undermining CNI stability.

Chinese-Speaking Groups

- **DragonRank**: This group has deployed BadIIS and PlugX malware in attacks against healthcare web applications, impacting systems across Asia and Europe.

> **"Impair Defences: Disable or Modify Tools was the top TTP investigated last quarter, highlighting that attackers are tampering with tooling in an attempt to evade detection."**
>
> Adarma Threat Intelligence Team

Transport Sector

Due to its critical role in national infrastructure and public services, the transport sector, comprising airlines, public transit systems, and logistics networks, has become a primary target for cybercriminals and hacktivists.

Cyberattacks on transport can cause visible disruption and impact economic stability and public safety. In Q3, a series of high-profile incidents underscored the sector's vulnerability, as threat actors used sophisticated tactics to breach systems and, in some cases, interfere with essential services.

Ransomware Activity

Ransomware remains the most significant threat to the transport sector, as cybercriminal groups target systems essential to operations, aiming to cause disruption or extort ransom payments. In Q3, prominent threat groups, including Akira, RansomHub, Rhysida, Helldown, and KillSec, executed multiple attacks on major transport entities, each incident highlighting different points of vulnerability within the sector's infrastructure.

Notable ransomware incidents included:

AUGUST

01

August 13

The Helldown group breached Italian public transport company ATP Sassari and claimed to have stolen 65GB of sensitive data, including employee and passenger information. This incident underscores the high stakes of data security in passenger-facing operations.

02

August 20

The Akira ransomware group breached the Transit Authority of Northern Kentucky's systems, affecting infrastructure supporting 107 buses serving 6,500 passengers daily. This attack revealed vulnerabilities in regional public transit and the potential for service disruptions.

03

August 24

The Rhysida ransomware group launched an attack that disrupted the Seattle-Tacoma International Airport and Port of Seattle's phone systems, email, and website. Critical systems had to be isolated, and staff conducted dock walks to maintain continuity, highlighting the complexities of security in interconnected transport systems.

04

August 25

Malaysian public transport operator Prasarana Malaysia Berhad was compromised by RansomHub, who claimed to have stolen 316GB of data. Although daily operations were unaffected, the breach underscored the ongoing risk of data theft in large transport networks.

Hacktivist Activity

Hacktivist groups, including pro-Russian collectives and their allies, have been increasingly active against transport sector entities, targeting websites and infrastructure with DDoS attacks:

- **NoName057(16)**: This prominent pro-Russian group targeted the transport infrastructure of NATO-aligned countries in Q3 2024. Notable incidents include DDoS attacks on the Jerusalem high-speed tram network websites, the Tel Aviv light rail, and Austrian Innsbrucker Verkehrsbetriebe, which manages public transport in Innsbruck.
- **Cund El Aksa**: A Turkish hacktivist group aligned with religious-political goals breached Ekomobil, an app used by Kocaeli residents for public transport access. During the attack, the group sent threatening anti-Israel notifications to application users and manipulated display screens on bus card readers to show warnings about suicide bombings. This caused a suspension of bus services in Kocaeli, a city of over 2 million people.

Data Breaches

On September 2, 2024, Transport for London (TfL) announced that it had been targeted in an ongoing cybersecurity breach. TfL is the local government body responsible for most of London's transport network, including the London Underground, Docklands Light Railway, buses, taxis, trams, and river services. There are indications that this attack could be linked to the loosely organised threat actor group Scattered Spider.

The cyberattack and efforts to remediate it affected live travel information services, prevented passengers from viewing their journey history online, and required staff to verify their identities, often in person, to regain access to locked accounts.

On September 20, 2024, around 5,000 TfL customers received letters notifying them that their data, which may have included bank account numbers and sort codes, had potentially been compromised. The affected individuals were Oyster users who had applied for refunds from TfL in the past.

> **"Data staged was the top technique investigated last quarter, indicating attackers actively prepare data before exfiltrating. This emphasises the need for proper data handling detection rules."**
>
> Adarma Threat Intelligence Team

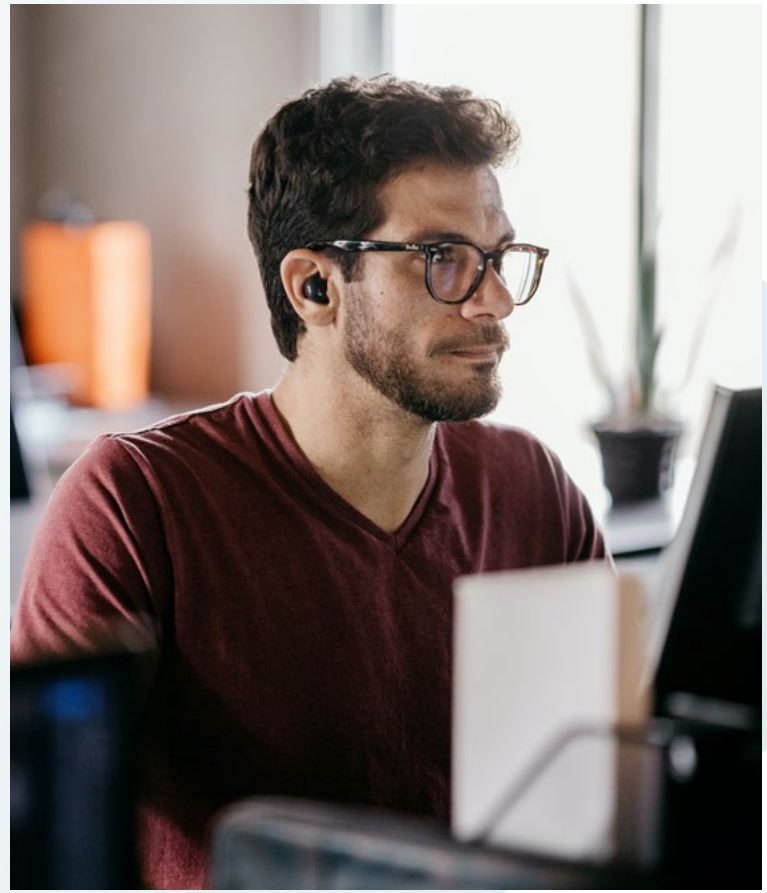
Phishing Campaigns

In September 2024, reports of a targeted phishing campaign against the North American transport and logistics sector emerged. This campaign used .URL attachments to install information stealers and remote access trojans on victim systems. Although the campaign did not lead directly to ransomware, it may have connections to espionage and data theft activities.

APT Activity

During this period, Western intelligence agencies released a briefing linking attacks on transport infrastructure to Russian military Unit 29155 (Cadet Blizzard/Ember Bear), known for conducting espionage and sabotage operations across NATO member states. These findings highlight the persistent risk state-aligned threat actors pose to transport infrastructure.

On September 25, the public Wi-Fi authorisation portal pages at 19 UK railway stations were replaced with content discussing terrorism, far-right politics, and anti-Islam rhetoric. Stations affected included London Euston, Manchester Piccadilly, Liverpool Lime Street, Birmingham New Street, Edinburgh Waverley, and Glasgow Central. Network Rail stated that British Transport Police were investigating the incident and that a third-party company, Telent, provided the Wi-Fi services. However, to date, no group has claimed responsibility for this attack.



Defence Sector

The defence sector remains a primary target for state-sponsored actors, especially amid ongoing military conflicts involving Israel and Ukraine.

As these conflicts persist, Iranian and Russian groups are likely to continue targeting Israel and Ukraine, respectively. Throughout Q3 2024, Russian, Chinese, and Iranian state-aligned groups conducted notable cyberattacks on the US and other Western defence entities, focusing on espionage and data exfiltration.

Hacktivist DDoS activity from pro-Russian groups, particularly NoName057(16), persisted this quarter, though at a reduced intensity compared to previous quarters. Should Ukraine receive approval to use lethal aid for strikes within Russian borders, these groups would likely shift focus toward DDoS attacks on the manufacturers of those weapon systems.

A significant rise in defence-related data advertised for sale on dark web forums like XSS and BreachForums has also been observed. Listed items include PII, email addresses, source code, Virtual Private Network (VPN) access, Secure Shell (SSH) root access, and domain administrator credentials.

Ransomware Activity

Ransomware remains a prevalent threat to the defence sector, targeting both contractors and critical supply chains. While overall ransomware activity in Q3 saw a slight reduction compared to previous periods, notable incidents highlighted the ongoing risk to defence-related entities. Key ransomware groups active in Q3 included RansomHub, Rhysida, and Akira. Significant incidents in Q3 include:

AUGUST

01

18 August

Ransomhouse listed VOP CZ, an aerospace and defence company based in the Czech Republic, on their leak site. The group claimed to have accessed the company's data but did not disclose the volume of compromised information.

SEPTEMBER

02

11 September

Meow ransomware claimed to have accessed organisational data from the Israeli Defence Force (IDF). The compromised information reportedly included personal details of IDF personnel, such as names, dates of birth, and military-related documentation.

Nation-State Activity: Russia 

The Computer Emergency Response Team of Ukraine (CERT-UA) reported a new wave of phishing attacks targeting the Ukrainian government and defence organisations. These attacks were attributed to UAC-0020 (also known as Vermin), a group believed to be connected to the security forces of the Luhansk People's Republic (LPR). The LPR is a region in Ukraine's Luhansk Oblast that was declared independent by Russian-backed paramilitaries in 2014 and later annexed by Russia in 2022.

During the campaign, attackers used a lure involving photos of alleged prisoners of war from the Kursk region. Recipients were prompted to click on a link that led to a ZIP archive, which then deployed SPECTR spyware.

On September 5, 2024, the FBI, CISA, NSA, and their international partners released a joint cybersecurity advisory. The advisory detailed the activities of the Russian GRU 161st Specialist Training Centre (Unit 29155), which has been conducting operations aimed at espionage, sabotage, and reputational harm against global targets since at least 2020.

The group is believed to consist of junior active-duty GRU officers and relies on non-GRU actors, such as cyber criminals. It operates separately from other well-known GRU groups, such as Unit 26165 (Fancy Bear) and Unit 74455 (Sandworm).

Nation-State Activity: Iran 

On 28 August 2024, the FBI, CISA, and DC3 issued a joint advisory on Iran-based threat actor Pioneer Kitten. The group operates two activity streams: one supporting Iran's government, targeting defence networks in the US, Israel, Azerbaijan, and the UAE to steal sensitive data; the other focused on high-volume intrusions in sectors like finance, healthcare, and education. These intrusions are monetised via dark web sales or collaborations with ransomware groups such as ALPHV (BlackCat), Ransomhouse, and NoEscape. Their ransomware activities are likely unsanctioned by Iran and conducted for personal profit.

Nation-State Activity:
China

On 16 July 2024, Recorded Future's Insikt Group released findings on the Chinese state-linked group TAG-100, suspected of a global espionage campaign impacting organisations in ten countries across Africa, Asia, the Americas, and Oceania. TAG-100 primarily exploits internet-facing systems like Citrix NetScaler, F5 BIG-IP, and Microsoft Exchange, using open-source backdoors Pentagana and SpartRAT for post-exploitation. While they mostly target government entities, defence organisations are also likely at risk due to their government connections.

How Adarma Can Help

At Adarma, we understand the challenges of keeping your organisation safe from cyber threats. That's why our threat specialists are here to help! With our expertise and dedication, we can guide you in securing your systems against both current and emerging dangers.

We offer services in the following areas:

Threat Intelligence Platform Management

Adarma's Threat Intelligence Team can set up, configure, and maintain a threat intelligence platform tailored to your business needs. This platform enables the storage of reports, incident details, and indicators of compromise (IOCs) while integrating intelligence feeds into your Security Information and Event Management (SIEM), EDR, firewall, web proxy, or phishing protection solutions. The platform streamlines investigations and prioritises detection efforts by creating associations between threat actor groups, malware types, and related IOCs.

Security Threat Modelling

Our threat specialists conduct security threat modelling that meets industry standards. We can assess threats for applications, platforms, or entire organisations, helping our customers identify potential vulnerabilities and risks that could affect their systems and solutions.

Quarterly Threat Briefings

Our Threat Intelligence Team provides quarterly threat briefings to support your long-term strategic planning. These briefings focus on trends based on industry sector, geographical location, and other customer-specific considerations, providing senior stakeholders with the insights they need for effective planning, budgeting, and risk management.

Monthly Operational Briefings

We provide monthly operational threat briefings to deliver actionable intelligence that informs short-term tactical decision-making and resource allocation. Our Threat Intelligence Team monitors data sources, threat feeds, dark web tools, and information-sharing platforms to deliver detailed breakdowns of your business's current and emerging security threats.

Threat Hunting Expertise

Adarma's Threat Intelligence Team comprises specialists and analysts experienced in threat hunting across SIEM and EDR platforms. We conduct custom behavioural threat hunts tailored to your organisation's unique security concerns. These hunts uncover previously undetected malicious activity, logging issues, and compliance problems and offer recommendations to enhance your security posture.

In conjunction with Adarma's security consultants, the Threat Intelligence Team assist in building and running cybersecurity crisis tabletop simulations based on current threats as seen in the wild, providing your stakeholders with real-world preparedness.

Get in touch

If you would like to speak to an Adarma consultant about any issue or approaches raised in this report, please contact us at **hello@adarma.com**.

ADARMA

TOGETHER WE'VE GOT THIS

hello@adarma.com

www.adarma.com