OpSec
Newsletter

COMING SOON: Online Security Training Courses

Classroom-Based NVC-FLP Courses by SPG

NEW: Classroom-based Non-Verbal Communications for Front Line Personnel [NVC-FLP] Courses for Security Personnel operating in various threat-level Environments. Instructed by former SFSG Operators.

An Introduction to Open-Source Intelligence (OSINT) by SPG

A short article on what OSINT is, how it can be used, and by who, to what end? We highly recommend that you learn about OSINT as it can be an invaluable tool in your Security Toolbox, assisting you with valuable resources.

Special Projects Group

IPSA

ARMED FORCES COVENANT

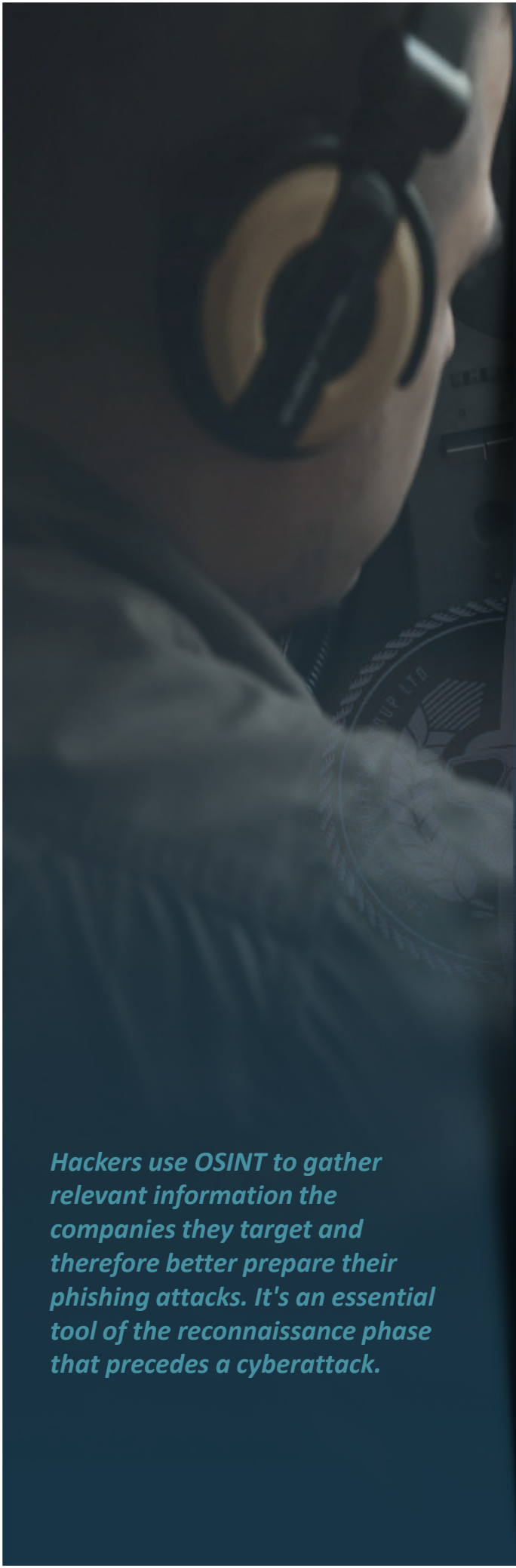# Newsletter Subjects:

Special Projects Group

Article: Open-Source Intelligence (OSINT) – An Introduction

OSINT stands for Open-Source Intelligence. It is the process of collecting, analysing, and utilizing information easily obtained from publicly available sources to gain insights, identify trends, and make informed decisions. OSINT also relies on data that is gathered from a wide range of sources, including (but not limited to):

- **Websites:** Publicly accessible web pages, blogs, forums, news articles, and other online content.

- **Social Media:** Information shared on social media platforms like Facebook, Twitter, LinkedIn, Instagram, and more.

- **Government Publications**: Reports, documents, and data released by government agencies or public institutions.

- **Academic Research**: Findings and data published in academic papers and journals.

- **Public Records**: Information available in official records like court records, property records, business registrations, etc.

- **Media**: News reports and articles from reputable media outlets.

- **Geospatial Data**: Maps, satellite imagery, and geolocation data.

OSINT involves using publicly available information from social media, websites, and news articles to gather information about an individual or organisation. This information can then be used to identify vulnerabilities and plan attacks.

- **Online Forums and Discussion Boards**: User-generated content from public forums and discussion platforms.

- **Dark Web Monitoring** (in some cases): Monitoring publicly accessible parts of the dark web for information relevant to specific investigations.

OSINT is used in various fields and industries, including intelligence gathering, cybersecurity, law enforcement, corporate research, competitive intelligence, journalism, and academia.

It also complements other intelligence disciplines and research methods, and it is often one of the initial steps utilised in the gathering of relevant information about a subject or specific situation.

It is also essential to conduct OSINT ethically and legally, respecting privacy and adhering to the terms and conditions that are set by the sources being accessed.

OSINT practitioners must verify the information they have obtained from multiple sources to ensure it is collaborated, this is to ensure accuracy and avoid relying on unverified or biased data.

OSINT continues to evolve as technology advances, providing a powerful toolset for both individuals as well as organisations seeking valuable insights from publicly available information.

Hackers use OSINT to gather relevant information the companies they target and therefore better prepare their phishing attacks. It's an essential tool of the reconnaissance phase that precedes a cyberattack.

NEW: Non-Verbal Communications for Front Line Personnel [NVC-FLP] Course

Our Non-Verbal Communications for Front Line Personnel (NVC-FLP) course is the ultimate tool for those who face the public daily, delivering vital skills to defuse potential conflicts, mitigate risks, detect danger and improve the overall safety of your environment.

By mastering these techniques, you can safeguard yourself and those you serve from unnecessary risk. The course covers a comprehensive range of topics from threat detection, duress recognition, to understanding cultural differences and micro-expressions. Enhance your ability to build rapport, communicate efficiently, and keep your environment safe.

By understanding the subtle nuances of non-verbal communication, participants can gain insights into how people feel and think. This knowledge gives them the power to create a safer environment for everyone around them. Our course offers an immersive experience with many practical exercises designed to help you apply your learning in real life situations. By equipping personnel with these skills, they can be better prepared to handle challenging and dynamic scenarios.

Our NVC-FLP course is designed to help you improve your awareness and confidence, giving you the tools to assess any situation quickly and accurately. With a range of topics covered including duress detection, cultural differences and emotional leakage, this course will equip personnel with the skills they need to successfully navigate any situation. It's the ideal choice for anyone who works on the front line and wants to be better prepared and safeguarded from potential risks.

Nonverbal communication can have a powerful impact on how others perceive us, particularly in stressful or confrontational situations. Our NVC-FLP course is designed to help participants develop the skills to read nonverbal cues, interpret micro-expressions and respond appropriately.

This will enable them to gain greater insight into what people are feeling and thinking, so that they can better handle any situation. With our immersive training approach, participants will be better equipped to protect themselves and those around them in potentially hazardous scenarios.

Invest in Your Safety - Choose our NVC-FLP Course Today.

To make enquiries regarding our classroom-based training courses, please contact us at enquiries@SpecialProjectsGroup.org and a member of our Training Team will be in touch with you.

The Profitable Edge of Security for Businesses: How a Strong Security Posture Makes Sense

In this era of ever-evolving digital landscapes, businesses confront the constant threat of cyberattacks. Imagine the potential devastation, a whopping average of £2.45 million (GBP) in losses for businesses with fewer than 500 employees.

It's clear as day - fortifying your organisation's cybersecurity strategy not only shields your business, but also presents numerous commercial benefits.

It's not just digital, real-world crime dents UK businesses with billion-pound losses each year. In 2021 alone, the retail industry suffered a stunning £7.2 billion (GBP) deficit due to crime, encompassing theft, fraud, and vandalism.

Several sectors are particularly susceptible to crime:

▪ In hospitality, the threats are theft, robbery, and vandalism.

▪ The construction sector is prone to theft of equipment and materials.

▪ For the transport industry, vehicle and cargo theft are primary concerns.

▪ Financial services constantly battle fraud and cybercrime.

With such daunting impacts of crime, it's baffling how security is often viewed as merely a cost of doing business.

Yet, with soaring security concerns and intense industrial competition, businesses are finding a silver lining.

Consumers are increasingly swayed by a company's cybersecurity posture when deciding where to spend their money.

A recent Accenture survey revealed that a staggering 74% of consumers would abandon a company's services following a data breach.

Implementing solid security measures isn't just about earning customer trust, it's about gaining a competitive advantage.

It signals to potential clients your commitment to safeguarding their data and willingness to invest in cutting-edge security solutions.

But there's more to cybersecurity than protection and competition. It's about seizing opportunities to enhance operational efficiency.

Investments in modern technology like automation and cloud services, can slash costs and streamline processes.

This not only gives you a leg up when vying for contracts, but also assures businesses that their data is in safe hands.

Join us as we delve deeper into the key commercial benefits of a solid cybersecurity posture.

Increasing Customer Trust and Confidence in Your Brand and Protecting your Reputation

When customers entrust their personal information and sensitive data to businesses, they expect that their data will be kept secure. A strong security posture reassures customers that their privacy is respected, and their information is protected.

As a result, customers are more likely to have trust and confidence in your brand and choose your services over competitors with weaker security measures. In the long run, a solid reputation for security can lead to higher customer retention rates and increased brand loyalty.

Companies heavily rely on reputation, and reputations take years to forge but only a few seconds to destroy. Having a strong reputation for security ensures that customers are more likely to remain loyal, and less likely to switch providers. This can result in businesses gaining a competitive advantage as well as increased market share.

Furthermore, having strong security measures can also help mitigate the likelihood of attacks. By investing resources into prevention, companies can protect their data and save money by avoiding costly security breaches. Companies of all sizes need to understand the importance of building a comprehensive security infrastructure to protect their customers and their data from malicious actors.

Having a strong security posture is not only crucial for customer trust and loyalty, but also for the long-term success of any business. Investing in preventative measures now can save businesses money in the long run, as well as keep their customers safe and their reputation intact.

Better Business Opportunities and Contracts

A robust cybersecurity strategy also presents businesses with new business opportunities.

Companies that adopt cutting-edge security technology to protect their customers' data can attract more customers, projects, and contracts.

By showcasing an impressive portfolio of security measures in place, organisations can demonstrate their commitment to securing customer data and prove that they are serious about protecting critical infrastructure.

In addition, organisations with strong security practices can attract more investors and partners who are looking for reliable companies that take data protection seriously.

Having a secure infrastructure and an effective incident response plan in place also makes it easier for organisations to comply with industry regulations such as the GDPR and CCPA which require businesses to keep customer data safe.

Mitigating Financial Implications of Security Threats

Security threats, such as cyber infiltrations, theft, and damage, pose significant fiscal threats to businesses. Direct financial implications of cyber infringements include the costs tied to operational downtime, the loss of confidential data, and the expenditure related to rectifications and enhancements post attack.

Threat Mitigation is the process used to lessen the extent of a problem or attack by isolating or containing a threat until the problem can be remedied.

By prioritising robust security measures, firms can evade these monetary setbacks, ensuring a healthier profit and loss statement.

This allows them to focus on key business goals, such as customer satisfaction and driving expansion, without the constant fear of a lurking security menace.

Moreover, investing in a stringent security system can yield long-term financial advantages.

Organisations that dedicate resources to pre-emptive measures, backed by a solid incident reaction strategy, are better equipped to counter attacks.

This approach lessens the likelihood of expensive interruptions from data infringements, thus guaranteeing uninterrupted business operations.

Mitigating Legal Risks

Data breaches can also expose businesses to legal risks. Following a cyberattack or data breach, organisations may face lawsuits, financial penalties, and regulatory enforcement actions due to the violation of data protection laws.

By maintaining a robust security posture, businesses can significantly reduce their legal risk, allowing them to save money on potential fines and litigation costs.

Legal liabilities can vary by jurisdiction and the nature of the data involved, so it is important that businesses understand their local regulations to ensure they are compliant.
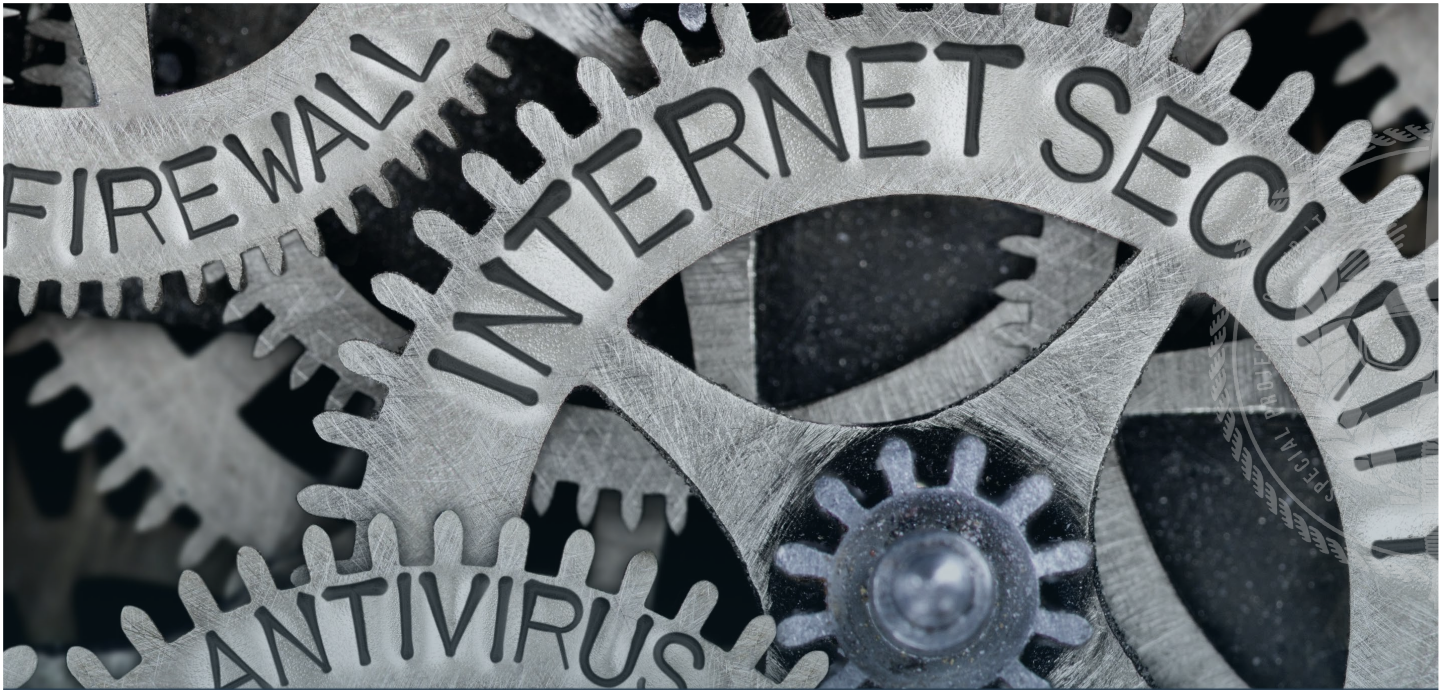
Investing resources into understanding and staying up to date with privacy laws can protect businesses from costly legal repercussions.

Enhancing Business Efficiency

Security measures also play an integral role in enhancing operational efficiency. By investing in modern technology such as automation and cloud services, businesses can streamline processes and reduce costs. This not only gives businesses an edge when competing for contracts but also ensures that their data is safe and protected.

The use of advanced automated security tools can also help organisations to quickly respond to potential threats and spot any anomalies before they become a major problem. This helps organisations to save time and money, as well as reduce the risk of data loss or other security incidents.

Conclusion

Strengthening your organisation's security posture is essential in the modern business landscape, where cyberattacks are becoming more frequent and costly, and physical attacks such as theft and vandalism are on the rise due to economic downturn.

By investing in a strong security posture, organisations can increase customer trust and confidence in their brand, prevent financial losses due to security incidents, and mitigate legal risks.

In doing so, businesses are better positioned to achieve commercial success while also maintaining their commitment to securely handle customer data.

Contact us today to see how your security posture holds up to the level of threat.

SPG Strategic Partnership Programme

Are you interested in becoming a Strategic Partner for Special Projects Group? We are looking to develop strong business relationships with proven, established companies within the Security Sector. We offer excellent commission rates, and partnerships on key projects.

Areas we are looking to collaborate right now are:

- Close Protection Services
- Security Consultancy
- Cyber Security Consultancy
- Insider Threat & Fraud Prevention

Contact us today either through our website, or by emailing us at the following address: enquiries@SpecialProjectsGroup.org .

Special Projects Group Pledges Support to the Armed Forces Covenant (AFC)

During August 2023, Special Projects Group Ltd. made the initial pledge to the Armed Forces Covenant This is a promise by the nation that those who serve or have served in the Armed Forces, and their families, should be treated fairly and should not face disadvantages when seeking to access public or private goods and services in the UK.

The Covenant is a voluntary pledge. Organisations may choose to sign up in order to demonstrate their support for the Armed Forces Community and for the principles of the Covenant. All organisations – public, private or voluntary and small, medium or large – are welcome to sign the Covenant

Special Projects Group Joins the International Professional Security Association (IPSA)

The International Professional Security Association (IPSA) is a membership association for companies working in the security sector, formed over 60 years ago to ensure professionalism in the management of security operations.

IPSA as an established and recognised worldwide professional organisation, provides, in accordance with growing demand.

Coming Soon to SPG: HECPO Training for Private Security Companies

Preparing your Close Protection Teams to achieve a high degree of operational functionality for high-threat environments, focusing on key subject areas that are vital to maintaining an effective protective effort, affording the Client a real sense of personal security and confidence.

When operating within the capacity of high-threat, close protection within hostile, or austere environments, the HECPO [Operator] is expected to function at the highest level of capability and professionalism.

These Operators often work in small teams, fully dependent on one another to ensure an effective protective effort is afforded the Client.

Subjects covered within our HECPO Course include, but are not limited to the following:

- HECPO Team Escort Drills
- Residential Security [High-Threat Environments]
- Site Security Surveys
- Threat & Risk Assessments
- Route Selection & Planning
- Counter-Attack Team [CAT]
- Security Advance Party [SAP] Team
- Venue Security Team [VST]
- Managing the Protective Effort
- Operational Planning & Management

Hostile Environment Close Protection Operator [HECPO] Courses are designed for qualified Close Protection Operators who wish to provide services within high-threat, or austere environments where the use of firearms is highly likely.

SPG to Present at The Security Expo – Olympia London on the 27.09.2023

It's getting closer everyone …

Due to the success of the presentation given by Gary Simpson of Special Projects Group at the recent Security Event in Birmingham on Non-Verbal Communication for the Security Environment, SPG have been asked to deliver a presentation on Non-Verbal Cues at the Security Expo in London (26th to 27th September 2023).

The NVC presentation is being held at the Olympia London on the 27th September 2023 at 1000 hrs, and we hope to provide an interesting and eye-opening presentation.

If anyone is attending this event and wish to meet with us, please feel free to reach out to us by emailing us at the following address enquiries@SpecialProjectsGroup.org and requesting an informal meeting as we would be more than happy to either assist you, or simply to establish a business relationship.

This is an exciting opportunity to network, forge new and long-lasting Strategic Partnerships with Special Projects Group. Why not meet with us on the 27th September after we deliver one of the opening discussions?
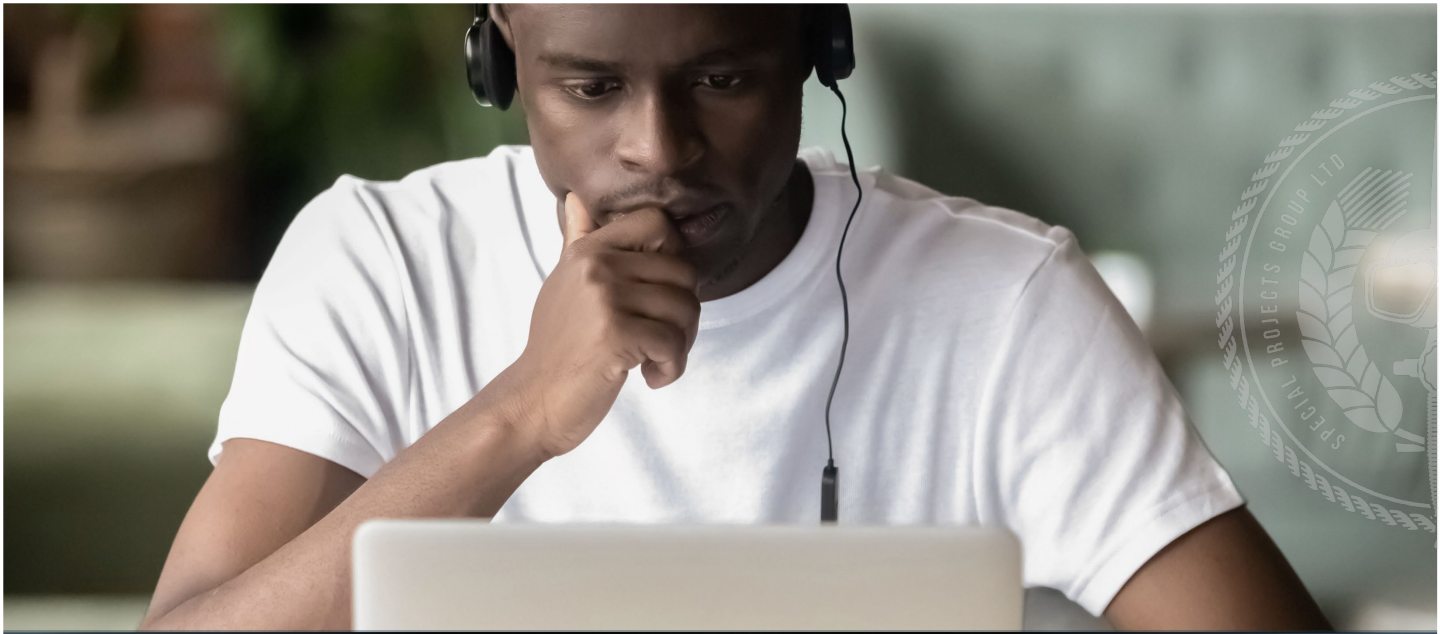
Online Security Training Courses available on the SPG Website

In August 2023, Special Projects Group Ltd. will be forming a Strategic Partnership with the multi-award-winning eLearning company, VIRSEC Ltd. The aim of this partnership is to allow SPG to provide easy and affordable access to customers wishing to grow their skill sets and knowledge in security-related subjects.

Courses that the SPG website will be 'going live' with are as follows:

- Anti-Kidnap& Hostage-taking Awareness Training
- Lone Worker Awareness Training
- Conflict Zone Threat Assessment for NGO's

Other courses will be added to the website over the coming months including the following courses:

- Residential Security Teams – Low to Medium-Threat Environments
- Residential Security Teams – High-Threat Environments

Want to know more, please contact email us: enquiries@SpecialProjectsGroup.org and a member of our team will get right back to you.

Contact Details

To contact Special Projects Group, you can email us at:
enquiries@SpecialProjectsGroup.org and one of our Consultancy Team will respond within 24 hours.

You can also visit our company website at: https://SpecialProjectsGroup.org and use the form available through the contact page on the website.

If you wish to make a WhatsApp call, please use the following number: +44 (0)7584 353 932.

To keep informed about the various Security Consultancy Services and Training Services that we provide, as well as updates, tips, and much more, why not sign up to this FREE Newsletter. Simply go to our website at https://SpecialProjectsGroup.org and sign up.