contextis.com

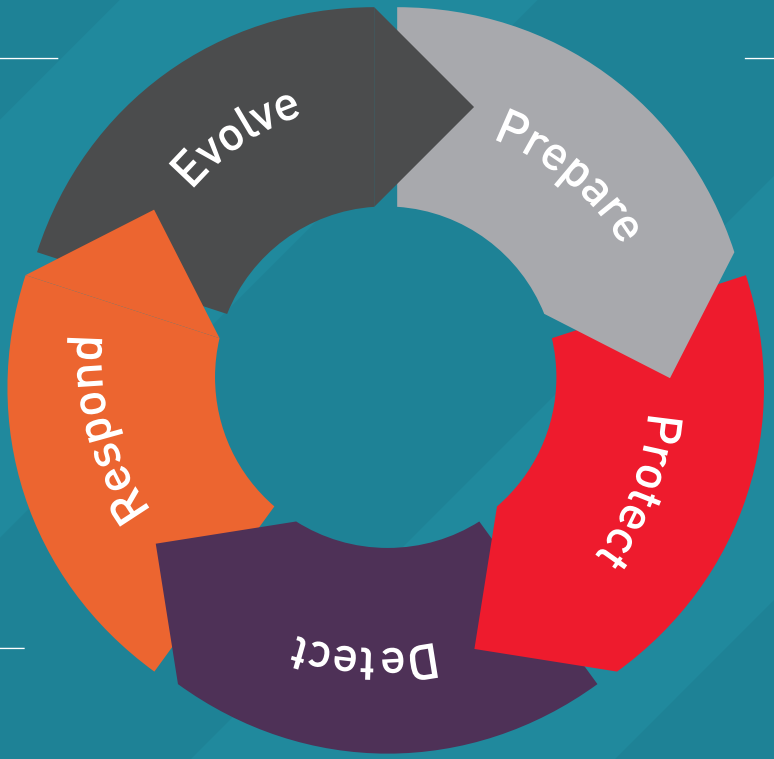
E info@contextis.com
T +1 917 880 3130

Context is a highly-skilled cyber security consultancy that supports organizations to meet their ever evolving information security challenges.

We help clients manage their cyber risk, avoid potential breaches and to deter, detect and respond to the most sophisticated cyber-attacks.

Whether you have a specific cyber security problem, or just want some general help with improving the security posture of your organization, we can help.

- Developing a cyber strategy
- Knowing your threats
- Building cyber resilience
- Implementing changes from lessons learned
- Crisis management
- Incident response
- Supporting your SOC



- Cyber risk management
- Product security testing
- Secure architecture and secure design
- Controls
- Penetration testing and Red teaming
- Build and configuration reviews
- Compromise assessments
- Threat hunting

contextis.com info@contextis.com

Founded in 1998, Context is independently operated with the backing of a multinational corporation. We work with many high profile blue chip companies and government organizations and are recognized as thought leaders in the industry. With offices in the UK, Germany, Australia and USA, we are ideally placed to work with clients worldwide.

Our Accreditations

Context helped to establish CREST (the professional body for regulating professional security testers) and its associated standards. Working with the CREST development team, we helped set the content and standard or their professional exams which are now recognized throughout the industry.

Context is qualified to provide CREST Simulated Target Attack and Response (STAR) services. STAR assessments identify weaknesses that go beyond the technical vulnerabilities typically found in a penetration test, and assess an organization's overall capability to prevent, detect and respond toa compromise.

Context was one of the first adopters of the CBEST scheme which the Bank of England (BoE) developed as a framework to deliver controlled, bespoke, intelligence-led cyber security tests. We are also proud to have been asked to help shape the development of CBEST and devising their accreditation standards.

Context provide a number of the UK's National Cyber Security Centre (NCSC) approved services, including: being a "Green Light" CHECK Service Provider; we are one of a handful of companies approved to provide consulting services for NCSC's Cyber Incident Response (CIR) scheme.

FS 581360

IS 553326

Our People

Our highly skilled workforce is what makes us unique.

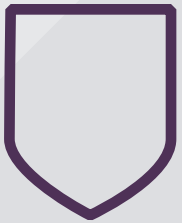
At Context, our employees are hand-picked from a variety of technical and commercial backgrounds and as a result they have a collectively diverse understanding of the industry and the associated security challenges. We actively encourage our employees to expand upon their skillsets by providing an environment that fosters and develops their expertise. In the ever-changing world of security technology, our philosophy is one of perpetual improvement.

Our Services

Cyber Risk Management and Advisory

Context can work with your organization to develop a comprehensive and effective cyber security strategy that covers a full spectrum of services and disciplines. We have worked with organizations both large and small, providing holistic and coherent cyber security solutions that take into account physical, social and technological aspects, in order to increase cyber resilience.

We can help with:
- Cyber strategy and transformation programs
- Cyber risk assessment and compliance
- Security architecture and design
- Threat assessment and threat management



Cyber Defense

With the threat of sophisticated and damaging attacks on the rise, every organization must be prepared to face the challenges of responding to a cyber-incident. Context can assist by helping to ensure your organization is adequately prepared, monitor and identify threats on your system as well as providing timely incident response.

We can help with:
- Threat hunting and compromise assessments
- Network monitoring
- Incident management and readiness reviews
- Incident response
- Security operations (SOC) consultancy

Testing and Assurance

Context provide a range of assurance services that can help to identify gaps and weaknesses in security practices and controls in order to prevent an attack. This is an essential part of any cyber security strategy – for small, medium and large business alike.

We can help with:
- Penetration testing
- Simulated targeted attacks (Red teaming, Blue teaming, Purple teaming)
- Build and configuration reviews
- Source code review and development assurance
- Mobile Device Management (MDM)
- Product security evaluation
- Compliance

Vulnerability Management

Identifying vulnerabilities in internet-facing systems is an important first step for any organization to improve their security posture. However, maintaining the security of publicly facing networks is challenging as network environments are constantly evolving, new services are being offered and new security vulnerabilities are constantly being discovered in existing services.

We can help with:
- Vulnerability scanning
- Monitoring external presence for new applications and services

We can also provide regular and controlled phishing assessments for organizations to measure their exposure to real-world phishing attacks.

Bespoke Research Consultancy

Context has completed bespoke research projects for clients across a wide range of topics and platforms. Previous customers include global technology vendors, corporate and government organizations. The common factors in most projects are our approach and our skill set: we specialize in agile, short to medium-term projects that require a mix of reverse engineering, protocol analysis, vulnerability research and development skills.

We can help with:
— Reverse engineering
— Vulnerability research
— Protocol analysis
— Bespoke development

Training

Effective and advanced training programs give your staff the knowledge and skills to understand and defend against constantly evolving threats and cyber-attacks. Context offer a variety of bespoke technical training courses, user awareness briefings and training, as well simulations and exercises.

Technical training courses:
— Web application hacking
— Mobile hacking and security testing
— Red teaming/ Simulated targeted attacks
— Hacking network infrastructure

Non-technical training include:
— User awareness training
— Corporate training programs on how to prevent phishing
— Table top cyber-attack scenarios
— Incident preparedness and putting cyber incident response plans to the test

Other Bits and Pieces...

Research & Blogs
Research is of huge importance at Context. Analysis of emerging and evolving security threats feeds into the development and refinement of our testing tools and other security services. Much of what we discover in our research is also published on our blog and presented at various events and conferences, enabling us to share our findings and expertise with our clients and with the wider security community. Visit our blog at **contextis.com/blog**

Careers
We are always looking for talented information security professionals to join our team. At Context, you will have the opportunity to work on a range of interesting projects, in a team with a structured training and development plan and a strong focus on technical excellence.

"I love the great working relationship between everyone at Context. You always feel welcome no matter which office you walk into, even if you don't know everyone."

To find out more about a career at Context, please visit our website **contextis.com/careers**

Events
We regularly run workshops and speak at events and conferences. We also run a regular program of our own webinars, training workshops, breakfast briefings and other events throughout the year. Visit **contextis.com/events** to see all upcoming events or subscribe to our newsletter to be kept up to date.

Our Offices

New York
T +1 917 880 3130

London
T +44 (0)20 7537 7515

Basingstoke
T +44 (0)20 7537 7515

Cambridge
T +44 (0)20 7537 7515

Cheltenham
T +44 (0)20 7537 7515

Gloucester
T +44 (0)20 7537 7515

Edinburgh
T +44 (0)131 285 1505

Bad Nauheim
T +49 (0)6032 949 7917

Essen
T +49 (0)201 8777 8550

Melbourne
T +61 1300 565 352

Sydney
T +61 1300 565 352

Suspected Security Breach?

Contact your local office to speak to our cyber incident response team.

response@contextis.com

context