www.portcullis-security.com

UK

Portcullis Computer Security Ltd
Portcullis House
2 Century Court
Tolpits Lane
Watford
WD18 9RS

T. +44 (0)20 8868 0098
E. enquiries@portcullis-security.com
www.portcullis-security.com

USA

Portcullis Inc.
505 Montgomery Street
10th and 11th Floor
San Francisco
California
94111

T. +1 415 874 3101
E. enquiries@portcullis-security.us
www.portcullis-security.us

PORTCULLIS

Incident Management & Response Services

About Portcullis

Test. Respond. Consult. Research. These are our four areas of expertise.

Portcullis is not new to the security market place, with the foundations of our company dating back to the mid-80s. It is fair to say that a lot has changed over the past three decades, but the fundamental principles of why organisations perform information security have remained constant. Private information needs to remain confidential. There is a need to trust the integrity of information. That information needs to be available when it is required. Our areas of expertise deliver this.

Security testing tells our clients exactly where they stand with regards system security. What and how we test continues to change, but the motivations remain the same; our clients have questions, we deliver the answers.

Incidents can and do happen. When there is an issue, Portcullis can be relied upon to have the expertise to respond, manage and restore our client's faith in their own systems. The more that can jointly be done to refine this process ahead of time, the better.

Information security is not just about the tech, so much of the overall security posture is embedded in company culture, policy, process and standards. Working in business terms, our consultants can advise on how to overcome the challenges of today and tomorrow.

In order to keep our clients up to date, and to ensure we remain industry leaders Portcullis has, and always have had, a very strong commitment to research. Research benefits the community, our company and our clients. It costs, but it is worth it.

Across all service areas, our aim is to take the best consultants, understand what the client needs, wrap this skill and knowledge up in efficient processes and then deliver on our promises. Technical expertise alone is not enough; it has to be delivered effectively and for the right reasons.

One of the challenges of information security is the constant change; threats continue to evolve, the use of technology changes and business constantly wants better access to more information. Security cannot stand in the way of this. Portcullis enables our clients to take advantage of new concepts by helping them understand the risks and how to manage them.

You are in safe hands with Portcullis; we know what our clients want both today and tomorrow. The capability to deliver has been proven time and again for decades. We are tried, tested and proven.

PORTCULLIS

Portcullis

Incident Management & Response Services

An effective response is dependent on good processes, timely access to accurate information and good decision making.

Despite best efforts to the contrary, incidents can and do occur. As information security professionals, we work to reduce the likelihood, but the residual risk remains. Through our incident management services, Portcullis helps companies prepare for the worst, provide cyber health checks to clarify the current position and incident response services to those currently handling an incident.

Through our incident management and response services, Portcullis helps companies prepare for the worst, provide cyber health checks to clarify the current position and incident response services to those currently handling an incident.

Incident readiness

If incidents cannot be stopped, they need to be contained, the aspiration being to minimise their impact. An effective response is dependent on good processes, timely access to accurate information and good decision making. Failings in these areas can seriously hinder an organisation's response to an incident and ill-judged, but well intentioned, actions can make things irreparably worse. Portcullis can help organisations build their incident readiness plan, identifying what is required from whom throughout an incident to ensure that evidence is not corrupted, that information is put into the right hands in a timely fashion and that business leaders are equipped to make the right decisions.

A key part of this process is identifying the information that is currently available and deciding whether it would be sufficient during an incident. Better to identify deficiencies now and remediate, rather than find out mid-incident.

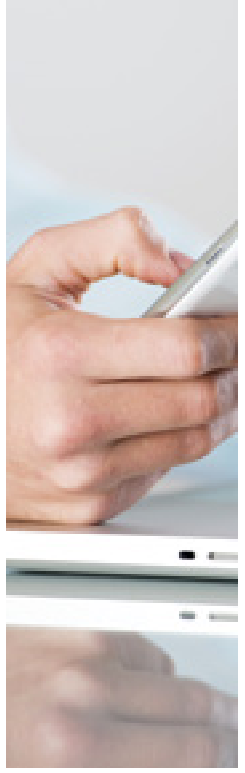
It is easy to have short-term focus on incident readiness, only for that focus to shift and for the plan to gather dust. For any plan to succeed, key personnel need to be familiar with it and ready to execute. Having refined the plan, Portcullis can help organisations replicate an incident and exercise staff and processes to ensure effective delivery, when it really counts. Such exercises can focus on discrete groups of staff, specific types of incident or be completed open-ended, involving everyone that would be involved in a real incident, from the IT technician to the CEO.

With the focus on incidents, there is an obvious crossover to our testing and consultancy work, which can reduce the likelihood of an incident in the first place.

Cyber health checks

Much has been said of the techniques used by modern attack groups and one of the key messages is that they prefer to undertake a prolonged, subtle attack that is notoriously difficult to identify during the normal course of business. Portcullis' cyber health check services are designed to identify such discreet, ongoing attacks which may otherwise go undetected. Essentially, this is an assurance project and is ideal for organisations seeking confirmation that current security measures are proving effective. Much like a penetration test may be commissioned in order to confirm that a given solution continues to meet security expectations. Using a range of techniques, Portcullis will search for 'indicators of compromise'; those minor signs which in isolation mean little but collectively point to a greater problem. If these signs are not present, assumptions can be made regarding the lack of a current breach. If those signs are present, further investigation will occur to confirm an incident, at which stage the engagement crosses over into incident management.

It is also important to remember that many security incidents do not involve an attacker, but instead centre on an organisation's own staff. Portcullis provides health checks that review the activities of staff, not to find that one rogue individual but instead to highlight widespread, cultural practices. Examples include staff using personal devices for note taking, emailing company documents to personal email for offline working, use of cloud-based services for presentations or document sharing, a failure to recognise phishing emails, etc. Depending



on the client and the circumstances that they are worried about, techniques used by Portcullis include technical exercises, log analysis, auditing, surveillance and interview.

Incident response

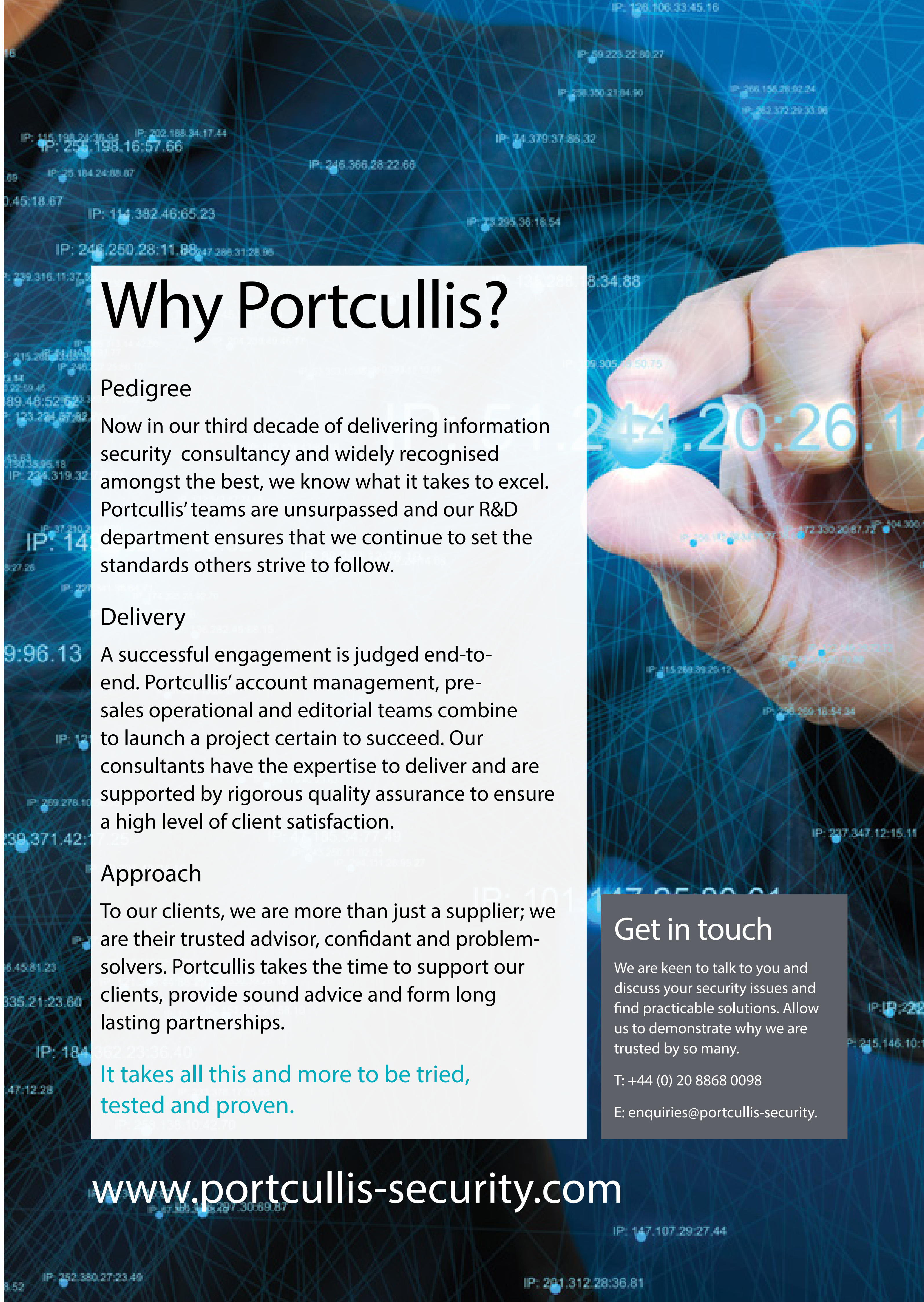
Portcullis has built a strong incident response capability covering both traditional incidents and those commonly referred to as cyber crime, with this capability certified under the CESG endorsed CREST Cyber Security Incident Response scheme. Portcullis' approach is to have a central incident response methodology that takes clients through a journey that confirms that there is an incident, ensures that the incident is contained to prevent further harm, understands what occurred and then resolves the incident fully, so that normal operation can be resumed. Having such a clear methodology is important because incidents by their very nature are unplanned, stressful and often have an air of confusion. Portcullis' methodology brings structure, control and clear direction.

The specific nature of an incident may dictate that different technical skills or approaches are required, but the underlying methodology remains the same, regardless of the type of incident. There is an impression in the media that every incident relates back to a sophisticated international attacker. This may indeed prove to be the case, but is far from a certainty. The singular methodology allows the investigation to scale up to such a serious occurrence, but can also address smaller, less sinister incidents without undue expense.

Portcullis can work on an entirely ad hoc basis, or pre-agree terms and provide a service level agreement for organisations wanting greater confidence in having the right support, when they need it.

Whilst Portcullis can step in and lead an incident, many of our clients have their own teams and do not need that level of support. For these clients, Portcullis is happy to provide specialist resources to perform specific tasks that bridge gaps in the client's own resource. This includes, but is not limited to, malware reverse engineering, forensics on mobile devices, large-scale log analysis and remedial support. Portcullis has access to privileged sources of information regarding the latest threats and attacks. This information allows for investigations to be progressed quicker than may otherwise be the case and makes Portcullis a useful addition to internal client teams who may not have access to such information.

The aim is always to considerhow the security of systems may be undermined in the real world.



Why Portcullis?

Pedigree

Now in our third decade of delivering information security consultancy and widely recognised amongst the best, we know what it takes to excel. Portcullis' teams are unsurpassed and our R&D department ensures that we continue to set the standards others strive to follow.

Delivery

A successful engagement is judged end-to-end. Portcullis' account management, pre-sales operational and editorial teams combine to launch a project certain to succeed. Our consultants have the expertise to deliver and are supported by rigorous quality assurance to ensure a high level of client satisfaction.

Approach

To our clients, we are more than just a supplier; we are their trusted advisor, confidant and problem-solvers. Portcullis takes the time to support our clients, provide sound advice and form long lasting partnerships.

It takes all this and more to be tried, tested and proven.

Get in touch

We are keen to talk to you and discuss your security issues and find practicable solutions. Allow us to demonstrate why we are trusted by so many.

T: +44 (0) 20 8868 0098

E: enquiries@portcullis-security.

www.portcullis-security.com