PEN TEST PARTNERS

Contact us:
info@pentestpartners.com
+44 (0)20 3095 0500

Security Consultancy

Experience Counts

We have a significant amount of incident response and digital investigation experience.

Our forensics and incident response consultants have Masters level education and SANS Institute training.

They are more than qualified to deliver a broad range of cyber incident investigation and planning services across your entire business.

The threat landscape has never been more challenging. Significant numbers of highly skilled and motivated threat actors present a real danger. They have many potential goals such as penetrating your defences to steal sensitive data, deliver malware into your network or disrupting your business through destructive attacks such as ransomware or data wipers.

As soon as you believe or suspect you have been compromised, a fast and efficient response is needed to understand the depth and impact of the incident on your critical business functions.

Incident Response (IR) Services

We work with you to help mitigate against disruption, brand damage, and data loss, whilst reducing the operational impact to critical business functions.

24/7 we're a phone call away. Security breach hotline: 0203 095 0520

IR Retained Service

Available 24/7 we provide experienced forensic consultants when you need them most.

IR Policy

The foundation of a good response is effective IR policies and processes – we use our experience to assist in reviewing or creating strategies that actually work for your business.

IR Table-Top Exercises

Test and improve your IR response capabilities in 'mock' tabletop real world tabletop exercises.

Advanced Threat Hunting & Compromise Assessments

Take control, define and manage the breach detection gap that is appropriate for your business.

We understand threats and know where to look for them. 44% of threats go undetected by automated security tools. The average time attackers dwell on networks within EMEA is 106 days, and in APAC 172days. These engagements answer the very important question "have we been breached already?"

Training: Incident Response & Digital Forensics

Training your internal staff with our experienced consultants to understand the Incident Response Process. Learn to effectively perform basic collection and forensics triage functions giving you a speed advantage at the outset of a critical cyber incident.

PEN TEST PARTNERS

Incident Response Lifecycle

Planning for incident response is critical to the effective management of a suspected data breach. Within each phase, there are specific areas to address as the incident progresses.

Preparation

Your response plan should aim to be well documented, explaining everyone's roles and responsibilities. The plan must be tested to ensure your employees will perform as expected. The more prepared your employees are, the less likely they'll make critical mistakes.

Identify

Early identification of the nature of the attack is critical to determine if you have been breached, and how. Once the nature of the attack is known, forensic investigation can be used to increase your situational awareness.

Identification processes will answer questions such as when an event occurred, how was it discovered, have any other areas been compromised, will the attack impact operations and has the point of entry of the attack been identified?

Contain

Upon discovery of a breach, you may be tempted to delete and reimage everything to remove the problem. That may not be the best course of action. Instead, contain the breach to minimise the impact.

That way, any compromised data is preserved. Create short-term and long-term containment strategies such as updating and patching systems, reviewing access protocols, changing user and administrative access credentials and harden passwords.

Eradicate

Once the incident is contained, the next step is to identify and eliminate the root cause of the compromise. All malware should be effectively removed, systems hardened and patched, and updates applied.

Recovery & Lesson Learned

Recovery is the process of restoring affected systems and devices back to a clean state.

The aim is to get business operations functioning normally again. At this stage you should also analyse and document the facts of the breach and conduct a critical review of the incident response process.

This will help to strengthen your procedures and enhance your ability to deal with future attacks.

Key Services

- Incident Response Retainer
- Incident Response Policy Assessment & Development
- Incident Response/Digital Forensics Training
- Incident Response Table-Top Exercises
- Advanced Threat Hunting
- Compromise Assessment

Services

Testing

- Penetration Testing – CHECK, CREST & Tiger Scheme
- CREST STAR & CBEST
- Red Teaming / Brand Damage
- Application Testing
- Infrastructure testing
- Mobile App & Device Testing
- Application Code Reviews
- Cloud Testing (AWS, Azure etc.)
- Social Engineering
- API & Web Services testing

Training

- Security Awareness Training
- Phishing Simulation & Training
- Hardware Hacking Workshops
- Developer Coding Training

PTP Tools

- PAPA: Password Auditing Service
- Version Recon: Patch Update Alerting Service

Specialised testing

- Maritime Cyber Security
- Rail Cyber Security
- Automotive Testing
- Aerospace and Satellite
- IoT Security Testing
- Open Banking
- SCADA/ICS Security Testing
- GBEST & TBEST
- Blockchain

Consultancy

- Incident Response
- PCI QSA
- ISO27001
- GDPR Consulting
- Digital Forensics
- Virtual CISO
- General Security Consultancy
- Policy Creation and review

CHECK IT Health Check Service · CREST · TIGERSCHEME · PCI Security Standards Council · CYBER ESSENTIALS · ISO/IEC 27001 · CBEST