INCIDENT RESPONSE & TRIAGE

KEY BENEFITS & DELIVERABLES

- **24hr response:** A dedicated 24 hr hotline to provide the customer with immediate response
- **Expert guidance:** Analysts experienced and skilled in incident response to provide direction and advice in reacting to the event
- **Specialist assistance:** Real-world penetration testers and security analysts to swiftly and accurately diagnose the compromise and offer remediation recommendations
- **Onsite deployment:** As warranted by the situation, deployment of a security analyst to the client's site to act as a liaison and perform onsite investigations
- **Ongoing reporting:** Constant updating as the investigation unfolds assisting the organisation in the decision-making process of how best to manage the incident
- **Reduced duration and impact:** Our shared sense of urgency minimises the organisation's exposure
- **Retainer based:** Eliminates procurement and approval process delays

KEY SERVICE COMPONENTS

- A 24x7x365 number to call as needed with immediate response
- Analyst response once a breach has been confirmed
- As needed, deployment of a skilled analyst within mutually agreed timeframes
- A methodical and structured approach to identify and investigate incidents such as:-
  - o Network intrusion
  - o Application intrusion or tampering
  - o Insider threat activity
- Malware reverse-engineering to examine what was compromised and how
- Diagnosis of the attack type, scope of the attack and breach impact
- Ongoing updates and reports as the investigation unfolds
- As instructed by the client, triage assistance working with the organisation's IT personnel
- A comprehensive report detailing what was found, including gaps, organised around what was learned about the attack

SERVICE DESCRIPTION

In the context of IT Security, incident response & triage is the formal, organised & structured approach that takes place once a breach of the business's cybersecurity defences has been detected or is suspected to have occured. It is the analysis of what happened or is happening, how it happened, what was affected, who was responsible and what can be done to prevent further occurrences. Combining people, processes and technology, the main goals of SecureData's incident response and triage service is to:

- Determine whether a compromise has occurred
- Limit the damage of a potential compromise
- Reduce recovery time and effort to recover from a security incident
- Decrease the amount of time that an attacker has unlimited access to the network
- Conduct an initial analysis of what occurred or may have occurred in order to enumerate possible response strategies and decide on the best course of action. At the end of this analysis the customer will be formally presented with an initial set of conclusions and a set of possible responses, ordered by preference.

Based on the renowned U.S. Airforce OODA loop methodology (Observe, Orientated, Decide, Act) we swiftly establish the cause and impact of the incident and provide accurate information helping the organisation in deciding how to react to the event.
The phases of the OODA loop are:

- Observe: Collect available information such as: -
  - o Background, suspicions, evidence, etc.;
  - o Network, architecture, layout, code, dependencies etc.;
  - o Logs and records etc.;
  - o Any other artefacts or collateral supporting the investigation.
- Orient: Examine logs and other digital artefacts in order to gauge the likelihood of a breach and identify the source of the intrusion. This is preferably conducted onsite and using 'live' analysis;
- Decide: Determine what the likely previous or next steps an attacker may have taken or will take based on available evidence and a strong understanding of how cyber attacks work.
- Act: Decide on a course of action appropriate for the finding. This could include disabling or fixing systems found to be vulnerable, instrumenting them to gather more evidence on the attacker, or engaging a formal forensic process in preparation for laying charges.

On agreement by the client, we will initiate the deployment of experienced analysts best suited for the investigation. Should remote diagnostics and forensics not be suitable, a member of the response team will be onsite as soon as practically possible to act as the client liaison performing required onsite investigation.

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com