CYBER SECURITY SAM ENGAGEMENT

With a Cyber Security SAM Engagement from Phoenix Software, you get a clear view of what software is deployed to identify areas of potential risk and provide high-level guidance on your cyber security programmes and policies.

With intrinsic reliance on technology in a progressively more connected world, the stakes around cyber security are rising. Organisations have a difficult time mitigating security breaches – whether human or system error or malicious cybercrime – and the average financial impact of each breach is increasing. For a cyber security programme to be effective, it’s necessary to have an understanding of your IT infrastructure and how it connects to organisations such as your financial partners, suppliers, vendors and customers.

CYBER SECURITY SAM ENGAGEMENT

You can’t protect what you don’t know! The Phoenix Cyber Security SAM Engagement focuses on providing a view of the software deployed within your environment to identify areas of potential risk and provide high-level guidance on your cyber security programmes and policies. Working with Phoenix Software, the engagement will help enable proper IT Software Asset Management (SAM) and peace of mind for your organisation. The engagement provides a solid baseline that you can use as a foundation for a more in-depth organisational security assessment.
THE CHALLENGES

Modern IT environments can be complex, increasing cyber security risk due to:

• Older software and patches that are no longer supported
• Unknowingly downloading malware via non-genuine digital downloads or online purchases from unknown vendors
• Removable media such as flash drives used to install inappropriate software
• Unauthorised personal devices connecting to the corporate network
• Terminated vendors or employees that continue to have access to IT systems

THE OPPORTUNITIES

• Implementing cyber security best practices and procedures will help you:
  • Securely manage software assets and promote proper cyber security practices
  • Build a resilient and adaptive IT infrastructure that can respond to threats quickly
  • Ensure that you have a secure IT infrastructure that provides an effective defence against attacks
  • Minimise data loss, fraud from theft and employee downtime, resulting in decreased costs and increased efficiencies

WHAT TO EXPECT FROM A SAM ENGAGEMENT

Every engagement will be slightly varied depending on your infrastructure, needs and goals. At a high level, an engagement can be broken down into four phases - Planning, Data Collection, Data Analysis and Final Presentation.

• Planning - the planning phase consists of gathering information from you on your infrastructure background and identifying plans and goals of the engagement, setting up appointments and arranging access to begin data collection and analysis

• Data Collection – the data collection phase includes the discovery and inventory of software assets, followed by the mapping of inventory data, usage and licence entitlements. Questionnaires and interviews with key stakeholders may be employed to ensure all relevant data and information is collected to provide a full and accurate analysis

• Data Analysis – the data analysis phase includes the review and validation of all collected usage, licence entitlement, deployment and other data. An analysis of your current cyber security state versus your long-term strategy and goals will also be performed. During this phase, results will include an assessment of your organisation’s potential vulnerabilities and overall cyber security maturity and provide recommendations on how you can minimise your cyber security risk

• Final Recommendations – at the conclusion of the SAM Engagement, we will present our results, recommendations and next steps in an overview presentation along with a set of detailed reports
DATA COLLECTION AND ANALYSIS

The goal when interpreting your inventory data is to detect what assets need to be protected and pinpoint areas that pose risks, including connections to external systems such as your banking partner, supply chain vendors and customers. Through Clarity, Phoenix will identify areas for improvement and develop a set of recommendations and processes to help your organisation optimise its software investments and stay compliant. The data collection and analysis will include the categories defined below.

ASSET INVENTORY
As a starting point, we define the scope of the machines to be inventoried, identify the extra steps needed to gather data from devices and networks that may not be easily accessible, and prepare environments for scanning and data collection. Once the inventory is complete, we will work with you to conduct a cyber security assessment.

DATA INTERPRETATION AND TECHNICAL REQUIREMENTS
Analysing the results from the inventory data collection involves identifying and documenting all product deployments, usage and licence entitlements. We will consolidate data collected from different inventory tools and map the data to critical information that supports you in making informed decisions. For example, mapping deployment data to product support lifecycles will provide you insights into when software needs to be upgraded. We will also analyse how software and network access is currently monitored.

DEPLOYMENT CONSIDERATIONS
We will then identify any potential changes that need to be implemented to decrease your cyber security risk. This may include installing security updates regularly, keeping antivirus software active and up-to-date using the most recent versions of software and starting to monitor and manage personal device use at work.

LICENSING CONSIDERATIONS
We will help you assess whether you are properly licensed and using genuine software for your current deployment and usage state, and recommend the optimal licensing options for your future goals based on the information gathered during data collection.

POLICY IMPROVEMENTS
Another important aspect of any cyber security programme is to be proactive in avoiding the risks associated with cyber threats by establishing policies around software piracy, malware, information theft, imposter fraud, and other forms of cyber crime. Phoenix Software will assist you in defining and implementing policies and processes to manage an ongoing cyber security programme.

READY TO LEARN MORE?
Being able to trust in your own data is vital and having a clear and complete view of your software licences and deployments across your organisation’s network, enables you to identify high-risk areas, conduct an in-depth security assessment and respond quickly to cyber security threats.

To learn more about our Cyber Security SAM Engagement contact a member of the Phoenix Team on 01904 562200 or email clarity@phoenixs.co.uk