SAM for Cybersecurity

This generation of IT environments is being heavily influenced by four key drivers—cloud solutions, mobile devices, social media, and big data—that are driving a transformation within most organizations. At the same time, security risks and evolving threats are growing rapidly. An IDC study estimated that in 2014, enterprises would spend $491 billion because of malware associated with pirated software.

Cybersecurity SAM Engagement

The Microsoft Cybersecurity Software Asset Management (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 cybersecurity programs and policies to help enable proper IT software asset management.

With unprecedented growth and innovation in information technology and a progressively more connected world, the stakes around cybersecurity are rising.

The Cybersecurity SAM Engagement provides analysis regarding the maturity of your organization's cybersecurity program in relation to different models available, such as the Critical Security Controls (CSC) initially published by the Council on Cyber Security or the Microsoft Cybersecurity Maturity Model. But for an overall cybersecurity program to be effective, it is necessary to first have an understanding of your IT infrastructure and how it connects to other organizations such as your financial partner, suppliers, vendors, and customers. Here are some challenges you may be facing and some of the benefits you can gain by working with a Microsoft SAM Partner on a Cybersecurity SAM Engagement.

Challenges

Modern IT environments can be complex, increasing cybersecurity 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.
- Unauthorized personal devices connecting to the corporate network.
- Terminated vendors or employees that continue to have access to IT systems.

Opportunities

Implementing cybersecurity best practices and procedures will help you:

- Securely manage software assets and promote proper cybersecurity 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 defense against attacks.
- Minimize 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 using an inventory tool followed by the mapping of inventory data, usage, and license entitlements. In addition, it includes the collection of data related to the Cybersecurity assessment recommendations. 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, license entitlement, deployment, and other data. An analysis of your current cybersecurity state versus your long term strategy and goals will also be performed. During this phase, results will include an assessment of your company's potential vulnerabilities and overall cybersecurity maturity and provide recommendations on how you can minimize your cybersecurity risk.

Final Recommendations – At the conclusion of the SAM Engagement, your SAM Partner will present their results, recommendations, and next steps in an overview presentation along with a set of detailed reports.

Microsoft

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. Your Microsoft Certified SAM Partner identifies areas for improvement and develops a set of recommendations and processes to help your company optimize its software investments and stay compliant. The data collection and analysis will include the categories defined below.

Asset Inventory
As a starting point, your SAM Partner will work with you to choose the right tools, 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. The inventory tools used should collect a wide range of data points to include any machines that may be running outdated or unsupported software. Once the inventory is complete, your SAM Partner will work with you to conduct the cybersecurity assessment.

Data Interpretation and Technical Requirements
Analyzing the results from the inventory data collection involves identifying and documenting all product deployments, usage, and license entitlements. Your partner 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. Your partner will also analyze how software and network access is currently monitored.

Deployment Considerations
Your partner will then identify any potential changes that need to be implemented to decrease your cybersecurity risk. This may include installing security updates regularly, keeping anti-virus 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
Your partner 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 cybersecurity program 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 cybercrime. Your SAM Partner will assist you in defining and implementing policies and processes to manage an ongoing cybersecurity program.

Engagement Deliverables

Prior to the engagement you should receive a letter of engagement and a full Statement of Work from your partner explaining what to expect during your engagement and for the work being performed. At the conclusion of the engagement, you should receive the following reports.

Executive Overview Report	The executive overview report contains a high level executive summary of the engagement scope, results, recommendations, and next steps.
Established Deployment Position (EDP)	The EDP report provides detail related to all software currently deployed within your IT infrastructure.
Effective License Position (ELP)	The ELP report provides details related to license entitlements which are mapped to deployments and identifies any gaps or underutilization in your organization.
Cybersecurity SAM Assessment Report	This report includes an assessment of your overall cybersecurity maturity and recommendations for minimizing the risks your company faces when combating cyber threats.
License Optimization Report	This report provides recommendations on how to optimize your Microsoft licensing program and structure for your company. The report details the risks, liabilities, and opportunities for your company's current licensing practices and recommendations on how to better manage your licenses to minimize future risk and align with your cybersecurity strategy.
Additional Uses of Data Report	The Additional Uses of Data Report includes recommendation on how to use the data you've already collected for other purposes, such as developing a virtualization roadmap, cloud migration plan, or a SQL Workloads assessment.

What is Software Asset Management

http://www.microsoft.com/en-us/sam/overview.aspx

Microsoft