Assignment: Windows Incident Handling Tools

Assignment Requirements
Responding to incidents in an efficient and repeatable manner depends on having the right tools in place before incidents occur. While there are many types of tools and utilities available for different purposes, some tools support incident handling tasks well. As a security administrator for Ken 7 Windows Limited, you have been given the task of evaluating various software tools for computer security incident response team (CSIRT) use.

You should recommend at least one tool for each of the main CSIRT categories of functional needs. You can select from the list of functional needs given below. For each software tool you should select the most appropriate functional need(s), it best meets.

Review the text sheet titled Tool Summary (provided below). After you identify the functional needs each tool fulfills, describe which tool, or tools, you would recommend for the Ken 7 Windows Limited CSIRT. Explain the reasons for your choice.

Submission Requirements
- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: APA Style

Self-Assessment Checklist
- ✓ I have identified the correct function to secure incidents of Ken 7 Windows Limited.
- ✓ I have explained and given proper reasoning for my choice of tools.

Required Resources (provided below)
- Text Sheet: Case Scenario for Rationale: Importance of Windows Access Control and Authentication
- Text Sheet: Tools Summary
- Worksheet: Match Tools to CSIRT Functional Needs

Case Scenario for Rationale: Importance of Windows Access Control and Authentication

Ken 7 Windows Limited is a manufacturer of Windows for residential and commercial builders. Ken 7 Windows Limited carries a variety of Windows and related products. It supplies builders with all of the tools and supplies to install finished Windows in any type of building.

Ken 7 Windows Limited has just purchased a new enterprise resource planning (ERP) software package to help control costs and increase both quality and customer responsiveness. The ERP software collects and stores information including:

- Raw material costs
- Labor costs
- Materials and labor requirements for products
- Purchasing requirements

Ken 7 Windows Limited has identified six basic roles for users in the new ERP software:

- Administrators—maintain ERP data and system operation.
- Planners—run planning software and generate requirements reports.
- Shop Floor users —enter operational data (receiving, shipping, and product progress during manufacturing).
- Managers—manage department personnel.
- Purchasing users—generate purchasing documents based on planning requirements.
- Accounting users—maintain cost and accounting data.

Access controls limit what users or roles can do with different types of data. For example, consider the following types of data:

- Cost information—raw materials and labor costs, including the cost of finished goods.
- Manufacturing details—cost, amount of labor, and time required to produce finished goods.
- Purchasing requirements—rules for determining when raw materials, components, or supplies should be purchased.

Through access control:

- Cost information can be viewed only by Accounting users.
- Manufacturing details can be viewed only by Shop Floor users.
- Purchasing requirement can be viewed only by Purchasing users.

During the analysis phase of the ERP implementation, Ken 7 Windows Limited raised concerns about users being able to access restricted data.

- Accounting users are able to login to shop floor computers.
- Purchasing users are able to access human resource (HR) applications and data.

The ERP implementation team suggested the following access control measures to protect restricted data.

- Create an organizational unit (OU) in Active Directory for shop floor computers.
- Deploy Group Policy Objects (GPOs) to restrict shop floor users to the shop floor OU.
- Define data access controls in the ERP software to deny access for all non-HR users to restricted data.

Implementation of several access control measures helped Ken 7 Windows Limited to restrict the data access. Hence access control and authentication is important, as it helped Ken 7 Windows Limited in reducing costs and increasing profits.

Tools Summary

- Archer Incident Management:

  http://www.emc.com/security/rsa-archer/rsa-archer-incident-management.htm

  "Archer Incident Management centralizes and streamlines the complete case management lifecycle for cyber and physical incidents and ethics violations. Archer's web-based solution allows you to capture organizational events that may escalate into incidents, evaluate incident criticality, and assign response team members based on business impact and regulatory requirements. You can also consolidate response procedures, manage investigations end-to-end, and report on trends, losses, recovery efforts and related incidents. Powered by the Archer SmartSuite Framework, the Incident Management software solution allows you to effectively handle incidents that occur anywhere you do business from detection through analysis and resolution."

- D3 Incident Reporting:

  http://www.d3security.com/products/incident-reporting

  "The Incident Reporting Software module is at the core of D3's end-to-end integrated security management technology or virtual Security Operations Center (vSOC). The incident reporting application is easy-to-use and fully customizable. The flexible customization options allow incident forms, tasks and analysis reports to be designed to your organizations unique requirements. This greatly reduces unnecessary incident form fields, streamlines adoption of the system by staff and ensures the appropriate information is being collected."

- Application for Incident Response Teams (AIRT):

  http://airt.leune.com/

  "AIRT is a web-based application that has been designed and developed to support the day to day operations of a computer security incident response team. The application supports highly automated processing of incident reports and facilitates coordination of multiple incidents by a security operations center."

- Request Tracker for Incident Response (RTIR):

  http://www.bestpractical.com/index.html

  "RT for Incident Response helps your CERT or CSIRT team to efficiently track computer security incidents big and small. Collaborating with staff from top Incident Response teams, we've built a tool designed to help you manage your entire incident handling workflow. RTIR builds on RT to track Incident Reports, Incidents which tie together those reports and your Investigations into root causes and ideal remediation's. RTIR extends RT with custom data extraction, reporting and workflow tools as well as a user experience centered around the Incident handling process. Best Practical offers a full suite of customization, training, deployment and support services for RTIR. Please contact us for more information."

- BMC Remedy Action Request System:

  http://www.bmc.com/products/product-listing/22735072-106757-2391.html

  "Build powerful business workflow applications for Web, Windows, UNIX, and Linux environments AR System provides a consolidated Service Process Management platform for automating and managing Service Management business processes.
  - Replace outdated manual systems with process automation that speeds the handling of unique processes
  - Out-of-the-box workflow modules commonly used in automating service processes, such as notifications, escalations and approvals
  - Integrate processes with systems across the enterprise
  - Adapt and evolve your processes to continually align with the needs of the business
  - Manage business process performance in real-time
  - Rapidly prototype, deploy, maintain, and iterate service management applications
  - Capture and track critical business data"

Web References: Links to Web references in this document are subject to change without prior notice.

These links were last verified on June 26, 2013.

Match Tools to CSIRT Functional Needs

Responding to incidents in an efficient and repeatable manner depends on having the right tools in place before incidents occur. While there are many types of tools and utilities available for different purposes, some tools support incident handling tasks well. As a security administrator for Ken 7 Windows Limited, you have been given the task of evaluating various software tools for CSIRT use. You should recommend at least one tool for each of the main CSIRT categories of functional needs. You can select from the list of functional needs given below. For each software tool you should select the most appropriate functional need(s), it best meets.

Review the text sheet titled Tool Summary given to you as a handout. After you identify the functional needs each tool fulfills, describe which tool, or tools, you would recommend for the Ken 7 Windows Limited CSIRT. Explain the reasons for your choice.

Select from these CSIRT functional needs:

a. Tracking incidents
b. Reporting on incidents
c. Archiving incidents
d. Communicating incident information
e. Managing an incident's tasks and activities

Software tools (note which CSIRT functional needs each product meets):

1. Archer Incident Management
2. D3 Incident Reporting
3. Application for Incident Response Teams (AIRT)
4. Request Tracker for Incident Response (RTIR)
5. BMC Remedy Action Request System

Which of the tools listed would you recommend for Ken 7 Windows Limited CSIRT? Why?