End Point Security

Core windows processes are built in windows tools named Task Manager which assist us in understanding the underlying processes inside a windows machine.The Task Manager is a buily in GUI-based windows utility that alllows users to see what is running on the windows system. And it also provides information resource usage,such as how much each process utilizes CPU and memory.

Note:

When a program is not responding,the Task Manager is used to terminate the process.

Sysinternals

The sysinternals contain tools for analyzing and running artifacts in the backend of a windows machine.

Theses tools are over 70 and are categorized in the following:

File and Disk Utilities

Networking Utilities

Process Utilities

Security Utilities

System Information

Miscellaneous.

The most used sysinternals tools for endpoint investigations are

TCPView-Networking Utility tool and **Process Explorer**- Process Utility tool

Endpoint Logging and Monitoring

Endpoint logging enables us to audit significant events across different endpoints,collect and aggregate them for searching capabilities, and better automate the detection of anomalies.

1. Windows Event Logs: Are not text files that can be viewee using text editor.However the raw data can be translated into XML using the windows API.The events in this log files are stored in a proprietary binary format with a **.evt or .evtx extension.** Thus**,**the log files with the .evtx file extension typically reside in **c:\Windows \System32\Winevt\Logs.**
2. **Sysmon**: It is a tool used to monitor and log events on Windows. Sysmon gathers detailed and high-quality logs as well as event tracing that assists in identifying anomalies in your environment. It is often used with SIEM system or other log parsing solutions that aggregate,filter,and visualize events.
3. **OSQuery**: OSquery is an open source tool created by Facebook. Security analysts can query an endpoint using SQL syntax. Run osqueryi on the OSquery interactive console/shell to interact with the tool.
4. **Wazuh**: Wazuh is an open source,fre
ely available and extensive endpoint detection and response (EDR) solution. Endpoint detection and response are tools and applications that monitor devices for an activity that could indicate a threat or security breach.These tools and applications have features that include:
    a. Auditing a device for common vulnerability
    b. Proactively monitoring a device for suspicious activity such as unauthorized logins,brute-force attacks,or previlege escalations
    c. Visualizing complex data and events into neat and trendy graphs
    d. Recording a device’s normal operating behavior to help with detecting anomalies.

Endpoint Log Analysis.

Event Correlation : Identifies significant relationships from multiple log sources such as application logs,endpoint logs and network logs.

For Example a network connection log may exist in various log sources such as sysmon logs (Event ID 3: Network Connection) and Firewall log may provide the source and destination IP,source and destination port,protocol, and the action taken.

Baselining : Refers to the process of what is expected to be normal. With regards to endpoint security monitoring ,it requires a large amount of data-gathering to establish a standard behavior of user activities, network traffic across infrastructure, and processes running on all machines owned by the organization.

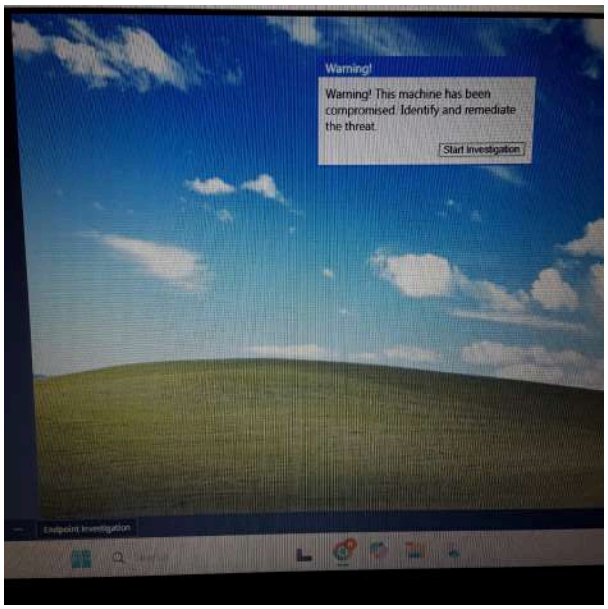
Thus,baseline serves as a reference to determine outliers that could threaten the organization.

Examples:

Baseline	**Unusual Activity**
A single workstation is assigned to each employee.	A user has attempted to authenticate to multiple workstations.

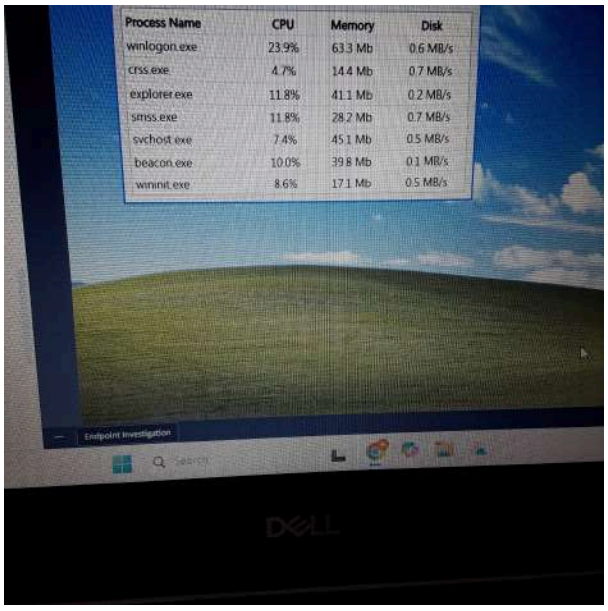
Investigation Activity

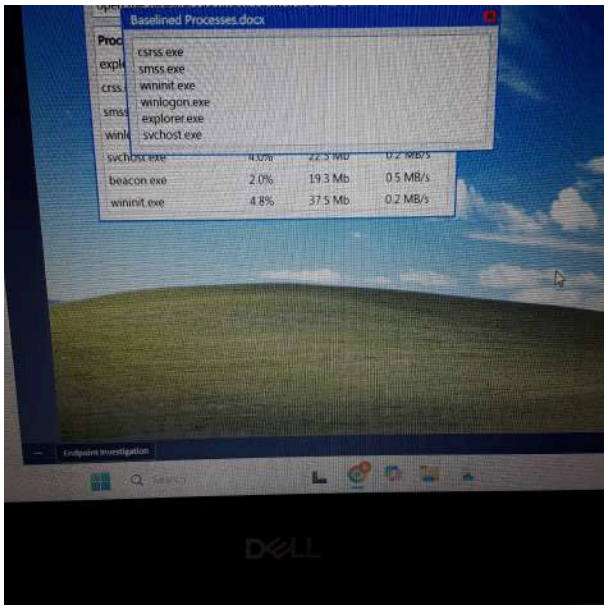
Alert : warning! This machine has been compromised.Identify and remediate the threat.



Identify the abnormal running process.

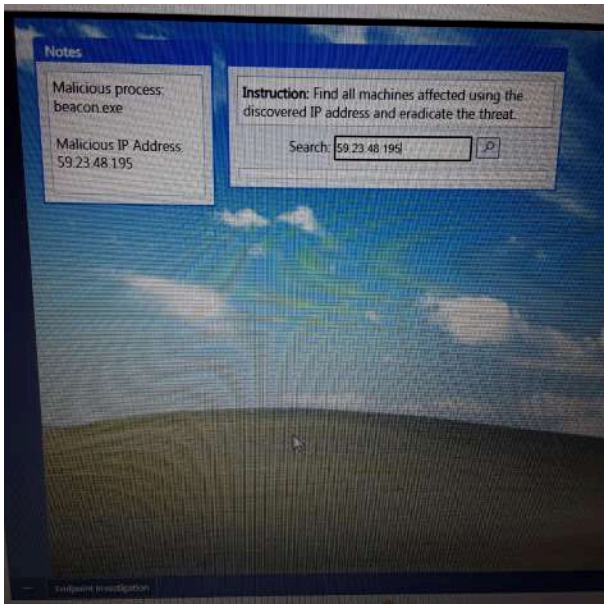
I read read the baseline document created by security team to enable me identify the outlier that may be a threat to the company.

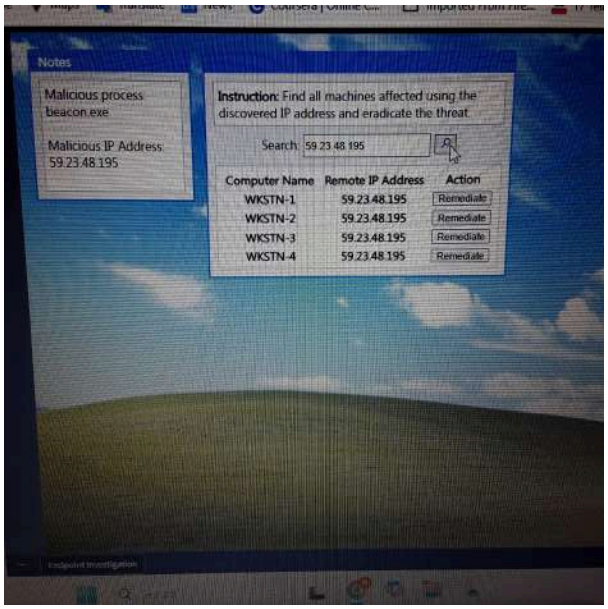




Based on the identified malicious process,I determines the malicious network traffic,by clicking on the process to get the IP address.

To find all machines affected by the malicious IP address and eradicate the threat,I inserted the IP address of the malicious process in search bar.





To eradicate the threat ,I clicked on remediate under action.