JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

# Server and Host Events

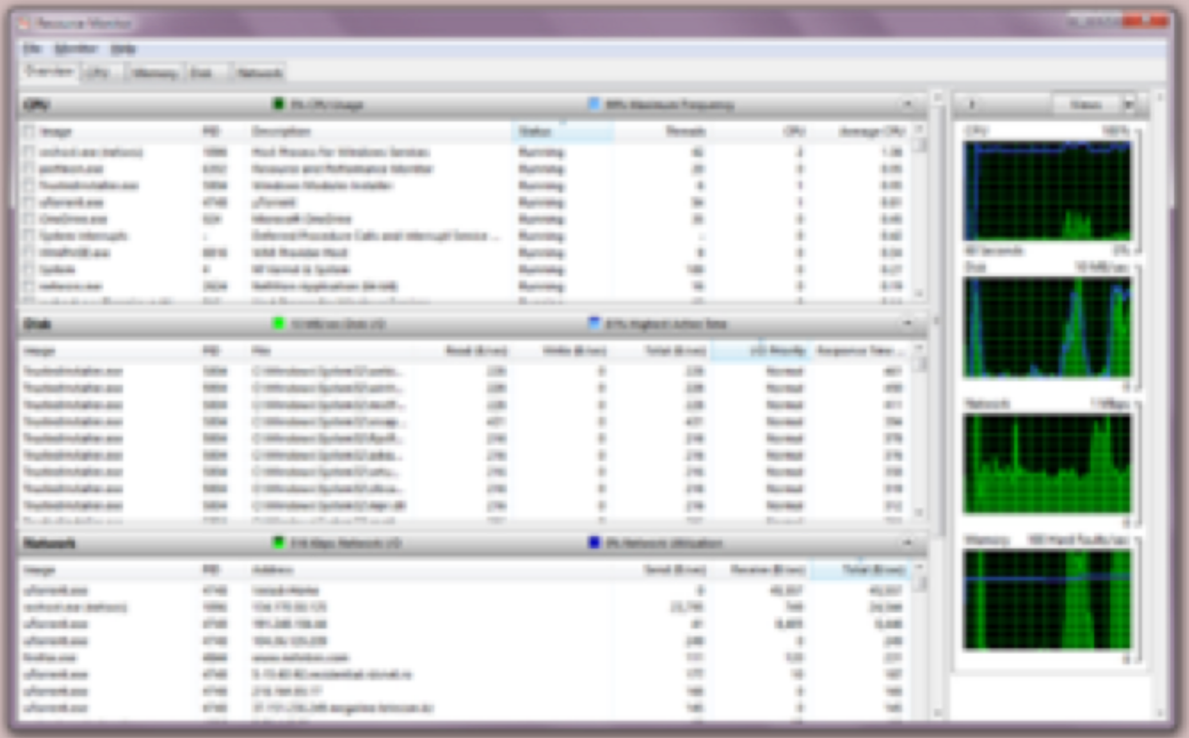
CYBER INCIDENT RESPONSE

# System Monitoring

- Processor (CPU), Memory, and Drives
- CPU attacks usually occur as DoS
- Memory is monitored by the OS based on given thresholds
  - Memory leaks occur when programs don’t release memory after being terminated
  - Eventually, all memory can be used up
  - System restarted to release the memory

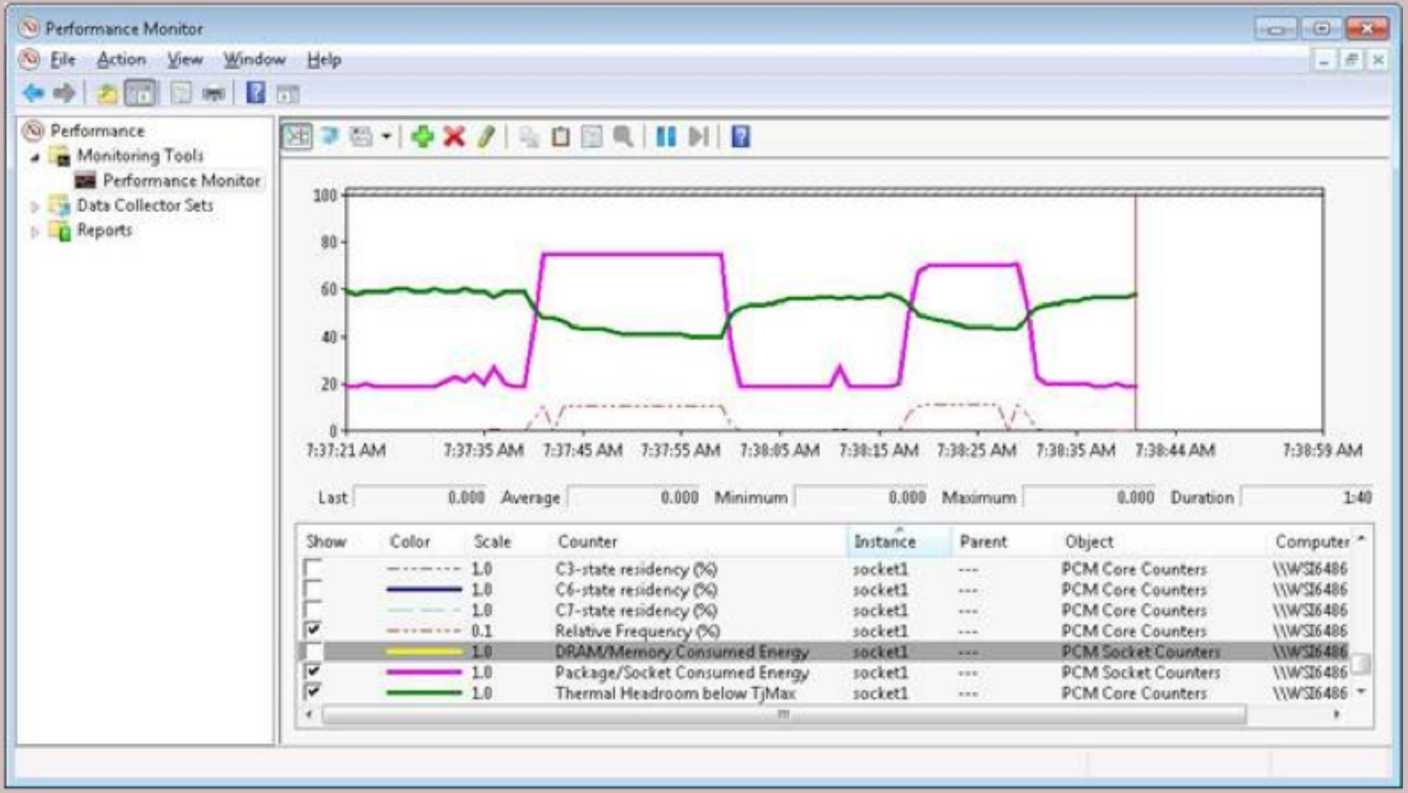
# System Monitoring Tools: Windows

- Resource Monitor (or resmon)
  - Built-in Windows tool for monitoring
  - CPU, Memory, Disk, and Network Utilization



# System Monitoring Tools: Windows

- Performance Monitor (or perfmon)
  - Built-in Windows tool for monitoring
  - Supports collection from remote systems



Last 0.000 Average 0.000 Minimum 0.000 Maximum 0.000 Duration 1:40

| Show | Color | Scale | Counter | Instance | Parent | Object | Computer |
|---|---|---|---|---|---|---|---|
| □ | -·-·-·- | 1.0 | C3-state residency (%) | socket1 | --- | PCM Core Counters | \\WSI6486 |
| □ | ━━━ | 1.0 | C6-state residency (%) | socket1 | --- | PCM Core Counters | \\WSI6486 |
| □ | — — — | 1.0 | C7-state residency (%) | socket1 | --- | PCM Core Counters | \\WSI6486 |
| ☑ | -·-·-·- | 0.1 | Relative Frequency (%) | socket1 | --- | PCM Core Counters | \\WSI6486 |
| □ | ━━━ | 1.0 | DRAM/Memory Consumed Energy | socket1 | --- | PCM Socket Counters | \\WSI6486 |
| ☑ | ━━━ | 1.0 | Package/Socket Consumed Energy | socket1 | --- | PCM Socket Counters | \\WSI6486 |
| ☑ | ━━━ | 1.0 | Thermal Headroom below TjMax | socket1 | --- | PCM Core Counters | \\WSI6486 |

# System Monitoring Tools: Linux

- ps
  - CPU and memory utilization, process info
- top
  - Like ps, but also provides sorting by top usage
- df
  - Report of disk usage
- w
  - Accounts logged on, who ran process

# Malware and Unsupported Software

- Use centralized management tools to conduct installs and inventory
- Antivirus and antimalware tools
- Conduct blacklisting of software/files
- Application whitelisting

# Unauthorized Access, Changes, and Privileges

- Users and permissions are complex with the number of systems in use

- Central Management tools (SIM/SIEM) can correlate logs for analysis
  - Authentication logs
  - User creation logs
  - System logs
  - Application logs
  - Security event logs