**TIP: FOR BEST RESULTS, PICK AN ACTUAL USER IN YOUR ORGANIZATION TO REPLACE JANE AND ATTEMPT TO ANSWER THESE QUESTIONS IN REAL TIME:**

### **SCENARIO**

It is 9:00 AM on a Monday morning and Jane- an employee of the Acme Corporation- is logging into her work computer. As she enters her username and password, she notices that the login process is taking longer than usual. After a few minutes, she is finally able to access her account.

Once logged in, Jane begins to notice some strange activity. She sees that several files have been deleted and that her history file shows files she does not recall recently opening.

### **QUESTIONS**

#### **ADVANCED**

* Does Jane recognize this is a potential security incident? Does she know the process to report the potential incident?
* Who will be engaged to investigate? How long before they are able to begin investigation?
* What questions will they attempt to answer as part of the triage investigation?
* What remediation steps are required and who should be informed and when?

#### **GUIDED**

##### ENGAGEMENT

* Have users been trained to recognize and report potential security incidents?
* Does this training include written instructions informing users who they should engage?
  + Is it an in-house SOC? Outsourced MSSP? Manager?
  + Are they aware and able to correctly follow the process?
* Does your incident response team (or vendor) have an SLA or similar established target for responding to user reported incidents?

##### INVESTIGATION AND TRIAGE

* Scope of impact
  + Do you know which groups Jane is a member of and which servers and services she has access to?
    - Does Jane have any elevated or administrative privileges?
    - Is the authentications to these accounts validated by an SSO solution, a directory server, or does the user also have local system accounts?
  + File activity: What files were impacted?
    - Can you determine which files Jane accessed?
    - Can you see which privileged activities (if any) Jane performed?
      * Can you tell which files were deleted and when?
      * Can you tell which files were opened or accessed?
      * Can you tell if there were files modified?
* Successful auth: Can you identify Jane’s successful authentication activities for the last 30 days?
  + Can you identify the geographic originations for those authentications?
  + Can you identify time of day for those authentications?
  + What is the originating system for these authentications?
    - Are all successful authentications from trusted and controlled systems?
    - Are any successful authentications originating from untrusted systems?
  + Are you able to identify any anomalies or outliers in the data discovered?
  + Are you able to identify interactive logins, remote logins (e.g. - file share & RDP), VPN logins, SSO authentications, SaaS authentications, 3rd party applications (e.g. - AWS, SalesForce), and application logins (e.g. - SQL database)?
  + Does the company use two-factor (2FA) authentication? Was 2FA bypassed for any authentication activity?
  + Can this information be shared with Jane to inquire if she recognizes all of the activity?
* Unsuccessful auth: Can you identify Jane’s unsuccessful authentication activities for the last 30 days?
  + Are any attempts anomalous or unusual?
  + What servers did Jane unsuccessfully attempt to access?
* System analysis:
  + What are the hardware assets Jane uses on a regular basis (e.g. - her workstation)
  + What processes are currently running on Jane’s computer? Are they all trusted? Any unusual? How do you know?
  + When was the last antivirus scan? How current are signatures?
  + Can you detect if any files were moved- particularly to an offsite/external location?

##### REMEDIATION

* Can Jane be forced to change all passwords across all accounts?
* Can heighted or additional monitoring be put in place for Jane’s authentication activity?

##### PROCESS

* Who is responsible to find answers (return data) to the questions listed?
* How long did it take to return these answers?
* Is equal visibility available on-prem and in the cloud for the answers above?
* Does your company consider this a security incident? Who needs to be notified?