Security Event:
is an observable change in normal behaviour to I.T. systems, environments, processes, workflow or a person.

Security Incident:
is an event that negatively effects the confidentiality, integrity and/or availability of any Western system.

<table>
<thead>
<tr>
<th>Events</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples</td>
<td>Examples</td>
</tr>
<tr>
<td>- An employee receives a phishing or suspicious email</td>
<td>- The employee replies to the phishing email with confidential information</td>
</tr>
<tr>
<td>- A computer system crashes</td>
<td>- A computer’s event logs indicate unauthorized privilege use</td>
</tr>
<tr>
<td>- An employee reports that their desktop may have a virus</td>
<td>- Multiple viruses are found on the desktop</td>
</tr>
<tr>
<td>- A user reports they can not access a certain service</td>
<td>- Multiple users have reported they can not access a certain service</td>
</tr>
<tr>
<td>- A system administrator believes that a system was breached</td>
<td>- A system administrator has a log entry showing suspicious activity</td>
</tr>
<tr>
<td>- An employee receives a phishing or suspicious email</td>
<td>- An employee opens a phishing or suspicious email and clicks on a link</td>
</tr>
</tbody>
</table>

If at any point in this continuum your are not certain, then treat it as a security incident.

Actions to be taken:
- Take remediation and investigative steps
- Contact the appropriate escalation point and take steps to eliminate any further risk
- Incident responder should notify the Western Incident Response Team and take steps to contain or eliminate any further risk
- Activate the Western Incident Response Plan

Examples:
- An employee receives a phishing or suspicious email
- A computer system crashes
- An employee reports that their desktop may have a virus
- A user reports they can not access a certain service
- A system administrator believes that a system was breached
- An employee receives a phishing or suspicious email
- An employee opens a phishing or suspicious email
- A computer system, after a crash is behaving oddly
- Multiple viruses are found on the desktop
- Multiple users have reported they can not access a certain service
- A system administrator has a log entry showing suspicious activity
- An employee opens a phishing or suspicious email and clicks on a link
- The employee replies to the phishing email with confidential information
- A computer’s event logs indicate unauthorized privilege use
- Virus is a worm and is propagating itself to other desktops
- Incident responder can not login to the service in question
- Correlated data shows many active attempts to compromise the system
- An employee’s desktop receives a pop-up claiming to be Ransomware
- Employee’s account(s) has been breached
- Evidence is found to indicate that access has been used in a manner that violates a Western policy.
- A virus outbreak has been confirmed on multiple systems
- An active DoS attack has been confirmed
- Unauthorized access to a system has been confirmed
- Ransomware has been identified on more than one system

EXAMPLES
- An employee receives a phishing or suspicious email
- A computer system crashes
- An employee reports that their desktop may have a virus
- A user reports they can not access a certain service
- A system administrator believes that a system was breached
- An employee receives a phishing or suspicious email
- An employee opens a phishing or suspicious email
- A computer system, after a crash is behaving oddly
- Multiple viruses are found on the desktop
- Multiple users have reported they can not access a certain service
- A system administrator has a log entry showing suspicious activity
- An employee opens a phishing or suspicious email and clicks on a link
- The employee replies to the phishing email with confidential information
- A computer’s event logs indicate unauthorized privilege use
- Virus is a worm and is propagating itself to other desktops
- Incident responder can not login to the service in question
- Correlated data shows many active attempts to compromise the system
- An employee’s desktop receives a pop-up claiming to be Ransomware
- Employee’s account(s) has been breached
- Evidence is found to indicate that access has been used in a manner that violates a Western policy.
- A virus outbreak has been confirmed on multiple systems
- An active DoS attack has been confirmed
- Unauthorized access to a system has been confirmed
- Ransomware has been identified on more than one system

EXAMPLES
- An employee receives a phishing or suspicious email
- A computer system crashes
- An employee reports that their desktop may have a virus
- A user reports they can not access a certain service
- A system administrator believes that a system was breached
- An employee receives a phishing or suspicious email
- An employee opens a phishing or suspicious email
- A computer system, after a crash is behaving oddly
- Multiple viruses are found on the desktop
- Multiple users have reported they can not access a certain service
- A system administrator has a log entry showing suspicious activity
- An employee opens a phishing or suspicious email and clicks on a link
- The employee replies to the phishing email with confidential information
- A computer’s event logs indicate unauthorized privilege use
- Virus is a worm and is propagating itself to other desktops
- Incident responder can not login to the service in question
- Correlated data shows many active attempts to compromise the system
- An employee’s desktop receives a pop-up claiming to be Ransomware
- Employee’s account(s) has been breached
- Evidence is found to indicate that access has been used in a manner that violates a Western policy.
- A virus outbreak has been confirmed on multiple systems
- An active DoS attack has been confirmed
- Unauthorized access to a system has been confirmed
- Ransomware has been identified on more than one system

EXAMPLES
- An employee receives a phishing or suspicious email
- A computer system crashes
- An employee reports that their desktop may have a virus
- A user reports they can not access a certain service
- A system administrator believes that a system was breached
- An employee receives a phishing or suspicious email
- An employee opens a phishing or suspicious email
- A computer system, after a crash is behaving oddly
- Multiple viruses are found on the desktop
- Multiple users have reported they can not access a certain service
- A system administrator has a log entry showing suspicious activity
- An employee opens a phishing or suspicious email and clicks on a link
- The employee replies to the phishing email with confidential information
- A computer’s event logs indicate unauthorized privilege use
- Virus is a worm and is propagating itself to other desktops
- Incident responder can not login to the service in question
- Correlated data shows many active attempts to compromise the system
- An employee’s desktop receives a pop-up claiming to be Ransomware
- Employee’s account(s) has been breached
- Evidence is found to indicate that access has been used in a manner that violates a Western policy.
- A virus outbreak has been confirmed on multiple systems
- An active DoS attack has been confirmed
- Unauthorized access to a system has been confirmed
- Ransomware has been identified on more than one system

EXAMPLES
- An employee receives a phishing or suspicious email
- A computer system crashes
- An employee reports that their desktop may have a virus
- A user reports they can not access a certain service
- A system administrator believes that a system was breached
- An employee receives a phishing or suspicious email
- An employee opens a phishing or suspicious email
- A computer system, after a crash is behaving oddly
- Multiple viruses are found on the desktop
- Multiple users have reported they can not access a certain service
- A system administrator has a log entry showing suspicious activity
- An employee opens a phishing or suspicious email and clicks on a link
- The employee replies to the phishing email with confidential information
- A computer’s event logs indicate unauthorized privilege use
- Virus is a worm and is propagating itself to other desktops
- Incident responder can not login to the service in question
- Correlated data shows many active attempts to compromise the system
- An employee’s desktop receives a pop-up claiming to be Ransomware
- Employee’s account(s) has been breached
- Evidence is found to indicate that access has been used in a manner that violates a Western policy.
- A virus outbreak has been confirmed on multiple systems
- An active DoS attack has been confirmed
- Unauthorized access to a system has been confirmed
- Ransomware has been identified on more than one system

EXAMPLES
- An employee receives a phishing or suspicious email
- A computer system crashes
- An employee reports that their desktop may have a virus
- A user reports they can not access a certain service
- A system administrator believes that a system was breached
- An employee receives a phishing or suspicious email
- An employee opens a phishing or suspicious email
- A computer system, after a crash is behaving oddly
- Multiple viruses are found on the desktop
- Multiple users have reported they can not access a certain service
- A system administrator has a log entry showing suspicious activity
- An employee opens a phishing or suspicious email and clicks on a link
- The employee replies to the phishing email with confidential information
- A computer’s event logs indicate unauthorized privilege use
- Virus is a worm and is propagating itself to other desktops
- Incident responder can not login to the service in question
- Correlated data shows many active attempts to compromise the system
- An employee’s desktop receives a pop-up claiming to be Ransomware
- Employee’s account(s) has been breached
- Evidence is found to indicate that access has been used in a manner that violates a Western policy.
- A virus outbreak has been confirmed on multiple systems
- An active DoS attack has been confirmed
- Unauthorized access to a system has been confirmed
- Ransomware has been identified on more than one system

EXAMPLES
- An employee receives a phishing or suspicious email
- A computer system crashes
- An employee reports that their desktop may have a virus
- A user reports they can not access a certain service
- A system administrator believe...