UBA Verification on the Cynet 360 Platform

In addition to a robust set of advanced threat prevention, detection and response features, the Cynet 360 security platform offers customers UBA Verification based on the platform's User & Entity Behavior Analytics capability.

Machine learning and user behavior analytics are utilized to identify anomalous activity. When anomalous behavior is suspected, a mobile verification is sent to the employee / third-party contractor in question, and they reply to verify their identity / activity. If they reply in the negative, an alert is sent by the Cynet platform to the customer's security team via email and via mobile notification.

Examples of anomalous behavior can include:

1. Verification requests at unusual hours – an employee or contractor who usually connects during daytime hours, suddenly connects during nighttime hours.

2. Verifications taking place on workstations / servers which an employee or contractor does not usually access.

3. Running of applications the employee or contractor does not usually use (i.e. SAP, Swift, etc.). This can, for example, be defined on the departmental level (i.e. a non-finance department user opening the SAP application).

4. An employee or contractor in the organization connecting to a critical infrastructure management system to which he has not connected in the past.

Security teams can also create their own dynamic queries which trigger the sending of a mobile verification message in cases of suspected anomalous behavior specific to their systems.

Auto-Remediation of Unauthorized Activity

When unauthorized activity is detected, auto-remediation can be used to kill the process, isolate the machine, block the user and more.