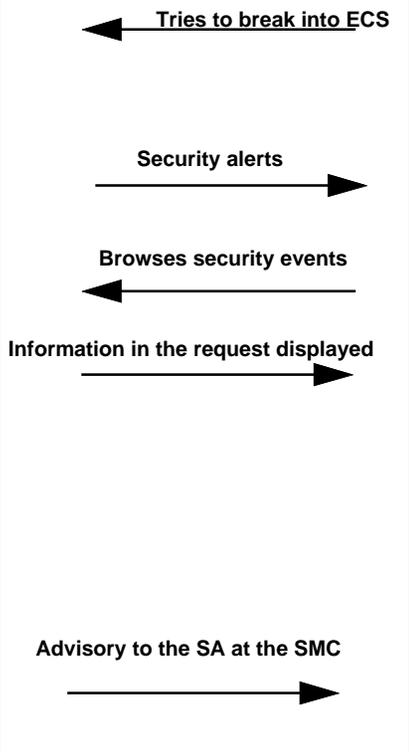


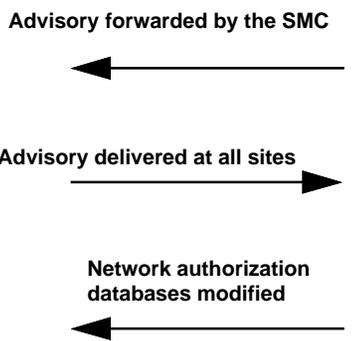
Security Management - Scenario

(Subsystem Involved: MSS)

NOTE: The Security Management Application has been set up to send an alert to the Systems Administrator (SA) upon the occurrence of five login failures from any given source. The subnetwork of a user at an SCF is allowed access to ECS

System	Data Exchanged	Human Actions
<p>2) The Security Management Application detects the security events when the established thresholds have been crossed.</p> <p>4) The Security Management Application displays the requested events</p> <p>7) The Security Analyst at the SMC is advised to follow up with the MIS manager at the SCF campus; and is sent an electronic advisory to direct all ECS sites to explicitly deny all incoming accesses from the host in question</p>	 <p>← Tries to break into ECS</p> <p>Security alerts →</p> <p>← Browses security events</p> <p>Information in the request displayed →</p> <p>Advisory to the SA at the SMC →</p>	<p>1) A “hacker” at the SCF campus (who discovers the hosts at the DAAC) attempts to log in by guessing passwords. The hacker tries a new host after five login failures at a given host.</p> <p>3) As a result, the SA receives multiple security alerts. The SA, during investigation, retrieves security events in the events browser window. The SA discovers that the login attempts on the multiple hosts originated from the same host, which is in the same domain as the SCF</p> <p>5) The SA calls the Security Analyst at the SMC to apprise him of the information, and informs User Services</p> <p>6) The SA at the SMC, after verifying the information, calls NASIRC and CERT to report the incident</p>

Security Management - Scenario (cont.)

System	Data Exchanged	Human Actions
<p>9) Advisory reaches SAs at all ECS sites</p>	<p>Advisory forwarded by the SMC</p>  <p>Advisory delivered at all sites</p> <p>Network authorization databases modified</p>	<p>8) The Security Analyst at the SMC forwards the security advisory to User Services and the SAs at all sites</p> <p>10) Based on this advisory, the SAs at all the sites modify the network security authorization databases to deny all incoming accesses from the host in question</p> <p>11) The Security Analyst reports the event to the MIS manager at the SCF campus who proceeds to have the issue investigated</p>