Blue Runbook 1

Document Name	IRTx Blue Run 1	Version	V1
Author	Braedyn Murtagh	Date Created	2023-11-15
Attack Type	Reverse Shell	Last Modified	2023-11-15
Staff Required	1 Analyst	Skills Required	Splunk
Document Description	This run describes how to detect and respond to a potential reverse shell attack.		

Step 1	Task	Complete
Alert Monitoring	Watch the splunk alerts console for incoming alerts. *NOTE: You may have to manually refresh, we advise refreshing at least once every 30 seconds, so as not to miss any alerts.*	
Step 2	Task	Complete
Initial Response	On receiving a “Console Process Started” alert, initiate a remote (Nutanix) session with the affected machine, and begin triage. Check for the suspicious process using tools such as ProcExp and Task Manager, terminate if needed.	
Step 3	Task	Complete
Prevention	Isolate the source of the issue, evaluate logs with splunk to find any potential signs of breach. E.g. *source=”WinEventLog::security” EventCode=4688 “PowerShell”*	
Step 4	Task	Complete
Isolation	If needed, isolate the machine with the vulnerability from the network to prevent further compromise. Ensure to check with client, to ensure minimal loss of service (CIA:3 – A: Availability)	

Blue Runbook 2

Document Name	IRTx Blue Run 2	Version	V1
Author	Braedyn Murtagh	Date Created	2023-11-15
Attack Type	SQL Injection	Last Modified	2023-11-15
Staff Required	1 Analyst	Skills Required	Splunk, SQL
Document Description	This run describes how to detect and mitigate potential SQL Injection Attacks		

Step 1	Task	Complete
Alert Monitoring	Watch the splunk alerts console for incoming alerts. *NOTE: You may have to manually refresh, we advise refreshing at least once every 30 seconds, so as not to miss any alerts.*	
Step 2	Task	Complete
Investigation	On receiving a “Potential SQLi Attempt” alert, review logs in splunk to find any potentially suspicious activity. E.g. *sourcetype=”apache_error” “Unknown column”*	
Step 3	Task	Complete
Evaluation	Determine if there is a significant risk of password breach, based on the logged queries.	
Step 4	Task	Complete
Isolation and/or Mitigation	IF there is a chance that the system has been further compromised, see run 1 for mitigation processes. OTHERWISE, If needed, isolate the machine with the vulnerability from the network to prevent further compromise. Ensure to check with client, to ensure minimal loss of service (CIA:3 – A: Availability)	

Blue Runbook 3

Document Name	IRTx Blue Run 3	Version	V1
Author	Braedyn Murtagh	Date Created	2023-11-15
Attack Type	Malicious File Upload	Last Modified	2023-11-15
Staff Required	1 Analyst	Skills Required	Splunk
Document Description	This run describes how to detect and mitigate potential issues caused by malicious files being uploaded		

Step 1	Task	Complete
Alert Monitoring	Watch the splunk alerts console for incoming alerts. *NOTE: You may have to manually refresh, we advise refreshing at least once every 30 seconds, so as not to miss any alerts.*	
Step 2	Task	Complete
Investigation	On receiving a "Potentially Malicious Upload Access" alert, review logs in splunk to find any potentially suspicious activity. E.g. *sourcetype="combinedaccess" "uploads"* *NOTE: If a "Console process started" alert was also triggered, go directly to run 1 for processing and mitigation.*	
Step 3	Task	Complete
Locate File	Initiate a remote connection (either Nutanix or FTP, where applicable) to the affected machine. Locate and isolate the malicious file. Be sure to remove the malicious file from the uploads folder. Process and analyse the file for traces back to the file's source.	
Step 4	Task	Complete
Mitigation	Temporarily disable uploads until a patch can be devised. Ensure to check with client, to ensure minimal loss of service (CIA:3 – A: Availability)	