PROFESSIONAL SERVICES SOLUTION

Add Indicator to Block List in Splunk

Use Case

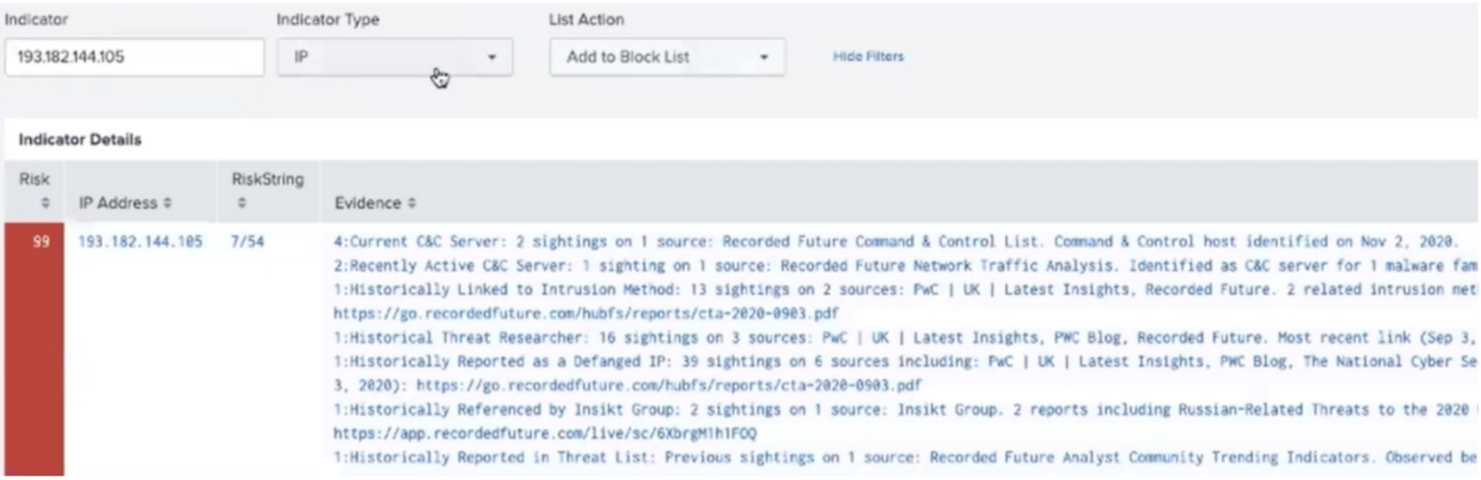
Having the ability to actively block an indicator of compromise found in Splunk is paramount to staying ahead and protecting one's organization. Taking immediate action to block an indicator of compromise can quickly mitigate additional risk. This action will add an indicator to a block list that can be used in conjunction with an organization's firewall. Analysts can use this action to protect the organization quicker, saving time and resources.

Issue

- Unable to quickly block indicators at the firewall
- There is no seamless way to block indicators via ones Splunk workflow
- Currently indicators are added manually via the Recorded Future Platform

Solution

Recorded Future Professional Services offers an enhanced capability, allowing Splunk users the ability to add an IOC to a block list where it can be sent to the organizations firewall for blocking. This list will be stored in the Recorded Future platform. From the Recorded Future platform, a separate file will be created with these indicators, where they can be pulled down into an organization's firewall(s) for proactive blocking.



Indicator: 193.182.144.105

Indicator Type: IP

List Action: Add to Block List

Indicator Details

Risk	IP Address	RiskString	Evidence
99	193.182.144.105	7/54	4:Current C&C Server: 2 sightings on 1 source: Recorded Future Command & Control List. Command & Control host identified on Nov 2, 2020. 2:Recently Active C&C Server: 1 sighting on 1 source: Recorded Future Network Traffic Analysis. Identified as C&C server for 1 malware fam 1:Historically Linked to Intrusion Method: 13 sightings on 2 sources: PwC | UK | Latest Insights, Recorded Future. 2 related intrusion met https://go.recordedfuture.com/hubfs/reports/cta-2020-0903.pdf 1:Historical Threat Researcher: 16 sightings on 3 sources: PwC | UK | Latest Insights, PWC Blog, Recorded Future. Most recent link (Sep 3, 1:Historically Reported as a Defanged IP: 39 sightings on 6 sources including: PwC | UK | Latest Insights, PWC Blog, The National Cyber Se 3, 2020): https://go.recordedfuture.com/hubfs/reports/cta-2020-0903.pdf 1:Historically Referenced by Insikt Group: 2 sightings on 1 source: Insikt Group. 2 reports including Russian-Related Threats to the 2020 https://app.recordedfuture.com/live/sc/6XbrgM1h1FOQ 1:Historically Reported in Threat List: Previous sightings on 1 source: Recorded Future Analyst Community Trending Indicators. Observed be

Technical

From a technical perspective the integration will include and need configured:

- A python script and commands.conf files that are added to the Recorded Future App for Splunk
- Configuration of a dashboard form that will submit the indicator to the block list
- Configuring the firewall(s) to ingest a text file or files of indicators

This service will require the SecOps Module, Splunk Integration, custom integration with a firewall that can ingest indicators via a text file and Two(4) Professional Service Credits for implementation. On-going support covered by Integration or Premium Support.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com @RecordedFuture