Securing a work-from-home organization

Scenario: A global pandemic has forced all your employees to switch to working from home. Now, with so many employees working on their home networks instead of the corporate network, you are concerned about data security. Additionally, the alerts you had previously configured, such as those for unusual login times, are firing constantly as people’s work habits have changed. You need to realign your organization’s security policies and practices with these new circumstances. You want to use Splunk software to create new baselines, then use this data to establish new alerts, monitoring, and reporting that fit with a home-based workforce.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- **People**: Security architect, security analyst
- **Technologies**:
  - Splunk Enterprise or Splunk Cloud Platform
  - [Remote Work Insights - Executive Dashboard](#)
- **Data**:
  - VPN data
  - System log data
  - Authentication data

How to use Splunk software for this use case

You can run many searches with Splunk software to safeguard an organization with a remote workforce. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Number of active VPN sessions
- Successful VPN logins over time
- Number of active Zoom meetings
- Number of all Zoom meetings created over time
- Most commonly accessed business applications
- Location of remote workers

Results

As the habits of your organization’s employees continue to evolve, the need to correlate events, rather than looking at
them independently, will become more important because what was suspicious before might not be now. You may want
to look at the use case Creating a timebound picture of network activity and consider developing some of the following:

- New baselines for logons
- New baselines for network traffic
- Updated phishing investigations
- Remote logons to hosts

Any actions you take likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

- Determining whether to have split tunnel or full tunnel VPN
- Establishing two-factor authentication for your VPN
- Updating or enhancing password policies
- Establishing or improving monitoring of your cloud services
- New methods of team collaboration and communication
- Identification of experts for new types of log data

Additional resources

The content in this use case comes from a previously broadcast webinar, one of the thousands of Splunk resources available to help users succeed. These additional Splunk resources might help you understand and implement this specific use case:

- Webinar: Shifting mindsets, modernizing the Security Operations Center
- White Paper: Remote work insights
- Blog: Hunting COVID themed attacks with IOCs
- Blog: Top services to monitor now that everyone is WFH
- Blog: Splunking Cisco WebEx meetings data
- Tech Talk: Getting Slack data into Splunk
- Tech Talk: Getting Zoom data into Splunk