RBA Readiness Review

A Free Review of Splunk® ES

Overview

Outpost Security is committed to accelerating the Risk Based Alerting journey for Splunk customers. As an initial step on your way to successful implementation of RBA in Splunk ES, we have created a free review of your environment. Upon completion you will receive customized insights to help you move forward and confidence to deliver the exponential gains made possible by RBA.

Review

+ Review current state of data available
+ Review data feeds & field extractions
+ Review current state of data model configurations
+ Review general Splunk configurations & performance

Analyze

+ Analyze key searches and security detections for:
  - Utilization of data
  - Coverage / breadth of visibility
  - Volume and source of historical notables / alerts
+ Analyze Threat Intelligence feeds and their incorporation into detections & notables

Deliverables

+ Detailed report outlining:
  - Positive observations – i.e., areas of strong data presence and utilization
  - Specific opportunities to configure Splunk / populate data models for improved visibility / performance
  - Identification of RBA use cases / detection types that are prime for immediate implementation
  - Examples of expected outcomes / findings from RBA use case implementation recommendations
  - Recommended critical path to execute opportunities and RBA use cases

Requirements

+ Splunk ES
+ Web conference while screen sharing your Splunk environment / data
+ 2 hours with Splunk Admin, engineer, or team member well versed in Splunk navigation and searching
+ Executed NDA per your organization's requirements

OUTPOST SECURITY

SECURITY DATA LEVERAGED

Active Directory, AWS, Barracuda, Blue Coat, Carbon Black, Check Point, Cisco, Crowdstrike, CyberArk, Cylance, Domain Tools, Forcepoint, Fortinet, Google Cloud, Juniper, McAfee, Microsoft Azure, Microsoft Office 365, Microsoft Office 365 email, Microsoft Security, Microsoft Windows, Mindmeld, Okta, Palo Alto, Proofpoint, Recorded Future, SailPoint, Tanium, Threat Stream, Trustar, Workday, Zscaler

DATA MODELS IN SCOPE

Authentication

Email

Endpoint

IDS

Malware

Network Resolution (DNS)

Network Sessions (DHCP/VPN)

Network Traffic

Web