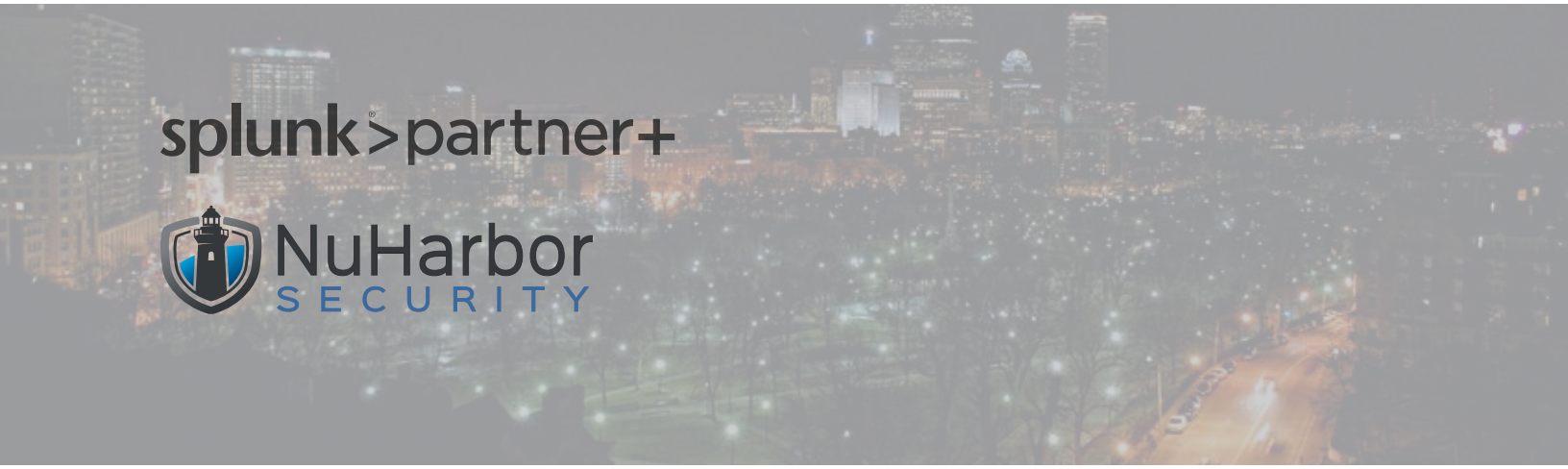

CONTACT US FOR MORE INFO:
sales@nuharborsecurity.com
nuharborsecurity.com
1-800-917-5719

WE'RE SPLUNK SPECIALISTS

NuHarbor Security provides innovative information security services and technology solutions. We are an established Splunk Premier Partner with a deep bench of Splunk accredited professionals. Our dedicated engineers deliver implementation services, ongoing professional services, as well as a comprehensive Splunk Enterprise Security Managed Services Program. With extensive experience in state, local, education, and commercial sectors, NuHarbor is your full-service Splunk partner. We will ensure your Splunk platform scales efficiently for years to come.

SPLUNK ENTERPRISE SECURITY MANAGED SERVICES WITH **NUHARBOR**

CHALLENGE:

You want access to your data, but don't have the resources to consistently monitor logs on a daily or 24/7 basis to ensure your systems' security.

SOLUTION: A TRUE CO-MANAGED SERVICE

HUMAN SECURITY REVIEW

Our engineers search for security anomalies with daily reviews of your Splunk environment. By reviewing alerts and dashboards, we identify potentially malicious activity. Based on review outcomes, our engineers filter false positives, investigate potential threats, and escalate valid security incidents according to your Alert Escalation Communication Plan.

SECURITY RULE TUNING

Based on our engineer's security reviews and client feedback, our team tunes your environment to reduce false positives or increase coverage.

BIWEEKLY STATUS REPORTS

As your trusted data security partner, we are committed to consistent communication. Our team provides a bi-weekly summary report designed for leadership and analyst review. Included is environment health, investigation results, current ticket status, and roadblocks.

NOTABLE EVENT INVESTIGATION

When we escalate a notable event, we also perform first level investigation. Our engineers narrow your search, and reduce your incident resolution time. Rest assured that you will spend precious response time efficiently.

QUARTERLY STATUS MEETING

Your environment is in constant motion which impacts your security posture. To ensure our teams are aligned and pro-active, we provide quarterly meetings to review current security health and future plans that could affect your Splunk environment.

OPTIONAL SERVICE ADD-ONS

24/7/365

Do your compliance or internal directives require 24/7 security monitoring? We have your covered with our affordable 24/7 service.

ADMIN, UPDATES, & CONFIGURATION

Need occasional help with Splunk upgrades, adding new programs, or data ingestion? Interested in customized dashboards and reporting? Our accredited Splunk team can provide additional services as needed.

WHAT WE'RE LOOKING FOR: NOTABLE, **POTENTIALLY MALICIOUS** EVENTS

NOTABLE EVENTS	DATA SOURCES CAN INCLUDE
High Or Critical Priority Host With Malware Detected	Crowdstrike, McAfee AV, Symantec AV
Threat Activity Detected	IPS/IDS , Firewall, Threatfeeds
Unusual Volume of Network Activity	Firewall, Some IPS/IDS Events, Some Load Balancer
Prohibited Service Detected	Windows Event Logs, Linux Logs
Prohibited Process Detected	Windows Event Logs, Linux Logs
High Volume of Traffic from High or Critical Host Observed	Firewall, Some IPS/IDS Events, Some Load Balancer
Anomalous New Service	Crowdstrike, McAfee AV, Symantec AV
Anomalous New Process	Crowdstrike, McAfee AV, Symantec AV
High or Critical Priority Individual Logging into Infected Machine	Windows Event Logs, Linux Logs, Crowdstrike, McAfee AV
Geographically Improbable Access Detected	Authentication Data
Excessive Failed Logins	Windows Event Logs, Linux Logs, Some Firewall
Brute Force Access Behavior Detected	Windows Event Logs, Linux Logs, Some Firewall
Watchlisted Event Observed	All Data for flagged user or host.
Substantial Increase In Intrusion Events	IPS/IDS, Firewall, Some load balancer
Activity from Expired User Identity	LDAP/Active Directory, SSO Platform, Authentication Data

CONTACT **NUHARBOR** FOR PRICING

sales@nuharborsecurity.com
nuharborsecurity.com
1-800-917-5719