Federally Recognized
Alaskan Tribal Owned 8(a)

OPERATIONAL SYNERGY

THE KEY TO STRENGTHENING CYBER SECURITY FOR FEDERAL NETWORKS & CRITICAL INFRASTRUCTURE

Splunk-as-a-Service Enterprise Solution Brief
in Response to the Presidential Executive Order

Copper River
Enterprise Services

TABLE OF CONTENTS

RISKY BUSINESS

In meeting mission critical requirements to sustain operational speed, security and performance of today's global enterprise, Federal agencies rely on machine data to gain real-time intelligence into their operations. Thanks to today's technologically advanced landscape, copious amounts of data can now be collected, analyzed & correlated from the enterprise. This data enables agencies to gain important insight that is critical when making strategic business decisions- quickly and effectively.

However, many federal agencies are facing extensive challenges when attempting to gain a comprehensive view of enterprise-wide data. This data is often fragmented between multiple branches, departments and event stakeholders. A lack of real-time, enterprise wide visibility and monitoring not only creates immense risk to the enterprise, it adversely reduces the Mean Time to Detect (MTTD) an attack, and the Mean Time to Respond (MTTR) to incidents.

This solution overview presents a differentiated methodology to attaining a holistic view of enterprise-wide data that Federal agencies require. By applying dynamic and continuous monitoring and detection strategies at an Enterprise level, antiquated and difficult-to-defend IT is removed providing a streamlined and mature security posture for an overall increase in the agency's capabilities. Utilizing an Enterprise Platform approach, Copper River ES and Splunk provide a strategic and tactical way for agencies to build and maintain a truly secure, resilient and modernized IT Operations and Cybersecurity framework.

DATA & SECURITY

IT Operations and Cybersecurity's ever changing technology demands mean agencies are fraught with technology and budget sprawl, tool fatigue and de-centralized or isolated management over their systems. Often, these tools and applications are limited in scope; many functioning independently of each other instead of in an optimal, strategic orchestration of appropriate technologies that scale with the agency. This technology sprawl often creates issues such as:

- Access control vulnerabilities due to the decentralized management of permissions and/or credentials that support the wide spectrum of tools and applications
- Ineffective correlation, presentation, and management of information contained in isolated tools and applications
- Increased risk profile due to lengthy and significant patching and updating of numerous tools, applications and the supporting infrastructure
- Increased demand on already strained budgets for OEM support, licensing, management and support of these disjointed systems
- Inability to gain operational efficiencies such as business & threat intelligence while also meeting log management and auditing requirements

To mitigate these challenges, Copper River Enterprise Services continues to work with agencies to leverage Splunk; no longer as a simple tool, but rather as an Enterprise Platform. Together, we map organizational requirements to an integrated platform of which Splunk is the backbone. With Splunk and

Copper River ES, agencies can begin the process of tool consolidation, automation and establishing a strategic framework where security organically strengthens.

Copper River ES strongly feels that synergy and data sharing amongst departments is crucial to ensuring confidentially, availability, and integrity of the enterprise as a whole. By implementing enterprise log management, agencies significantly improve IT operations; organizations can proactively monitor and fix critical core services before outages occur. This increased information sharing empowers operating divisions within an agency to combine resources for a common goal- thus creating a "Win<->Win" scenario for both IT Operations and Cybersecurity initiatives.

VISIBILITY

Visibility into the entire IT infrastructure is paramount to the success of an agency's mission. Lacking the complete and comprehensive view of enterprise data puts agency's in a reactive state, wasting valuable time and resources when both detecting and responding to cyber threats. Utilizing an Enterprise Platform allows for tools to be consolidated and data to become centralized, increasing the Mean Time to Detect (MTTD) an attack, and the Mean Time to Respond (MTTR) to incidents.

With Splunk deployed at an enterprise level, agencies increase in their ability to monitor and detect insider threats while gaining powerful business intelligence capabilities. Copper River provides agencies near-real time threat analysis of their enterprise through years of experience combined with machine learning capabilities. With your new increased visibility into your existing data, agencies can make better daily business decisions, improve efficiency, and reduce overall costs.

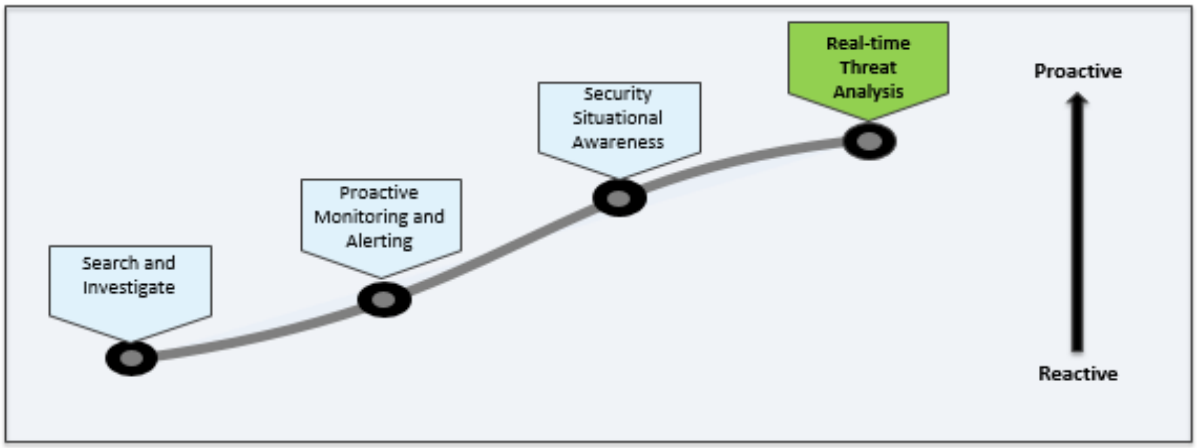

Figure 1 Copper River Enterprise Services moves organizations from reactive to proactive threat detection and analysis

DOING MORE WITH LESS

In the day of decreasing budgets but increasing needs, organizations are all faced with a simple dilemma. How can we do more with less? Splunk as an enterprise platform will provide the roadmap to answering that question. Splunk's ability to integrate with any application allows for a phased, scaled and planned process of eliminating those redundant applications and tools while customizing Splunk to achieve those functions. As those tools and applications are replaced or integrated with Splunk, the costs of supporting and maintaining those tools is eliminated.

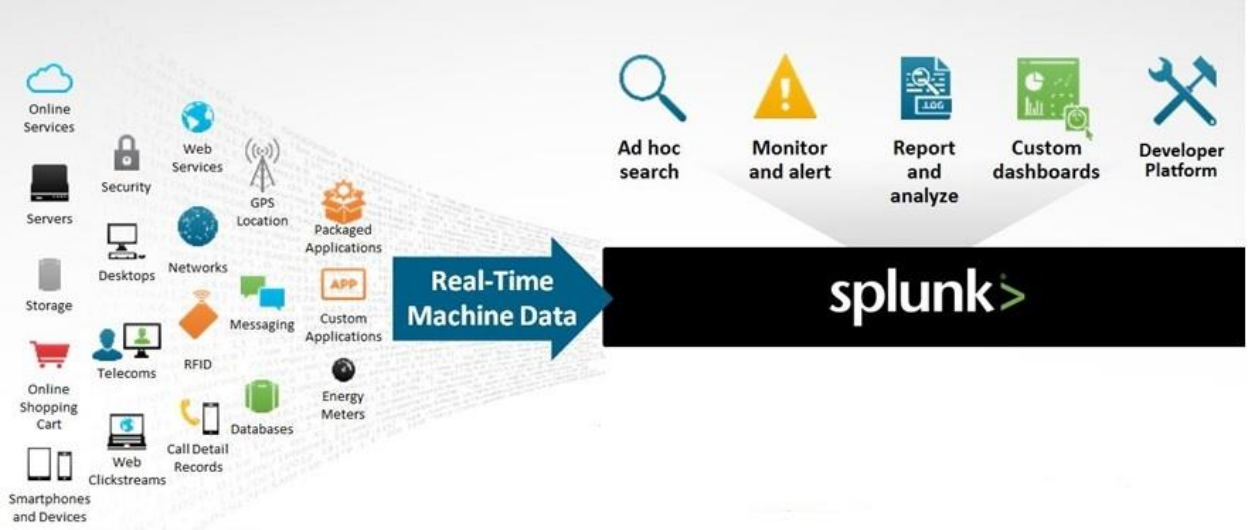

Figure 2 Centralizing machine data; all data is relevant

Eliminating redundant applications and tools is just the beginning of how Splunk can reduce costs while providing a more robust solution. Manpower is also impacted by the deployment of Splunk at an enterprise level. As reoccurring reports and dashboards are established, the time previous spent generating these reports can now be better utilized. With the increased efficiency in responding to, and investigating, incidents the manpower required for these efforts are drastically reduced.

THE TIME IS NOW

On May 11th 2017, President Trump signed an executed order aimed at strengthening the country's cybersecurity capabilities. The order stresses the significance of an effective cybersecurity risk management and mitigation plan, and underscores the importance of building a modern, secure and more resilient IT architecture. Agencies are now under a very aggressive timeline to provide insight on how they plan to improve their cybersecurity architecture while referencing The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institutes of Standards and Technology (NIST).

Copper River Enterprise Services has positioned itself to immediately help. Utilizing our team of highly certified cybersecurity engineers, Copper River ES, in partnership with Splunk, will review your current IT Operations and Cybersecurity policies against NIST Cybersecurity Framework Standard. During this

assessment phase, we will first understand the strategic mission of your organization and agency, look at the enterprise architecture for unmitigated vulnerabilities, antiquated tools and applications, and suggest the best path forward based on your current cybersecurity framework. Based on our findings, the Copper River ES team will provide a report to the agency on how to establish a stronger, NIST Compliant, cybersecurity framework. Our team's assessment of an agency's existing IT Operations and Cybersecurity Critical Infrastructure will include the following:

- Current cybersecurity framework compliance with the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)
- Roadmap for the consolidation of tools & applications that's functionality could be replaced by Splunk
- Business Value Assessment of Splunk as an Enterprise Platform with the agency
- Suggestions on Workforce Development to include training, primary through higher education, suggested certifications and other IT Operation/Cybersecurity related education curricula
- Strategic, operational and budgetary considerations for improving the agency's risk management and elimination of unmitigated vulnerabilities

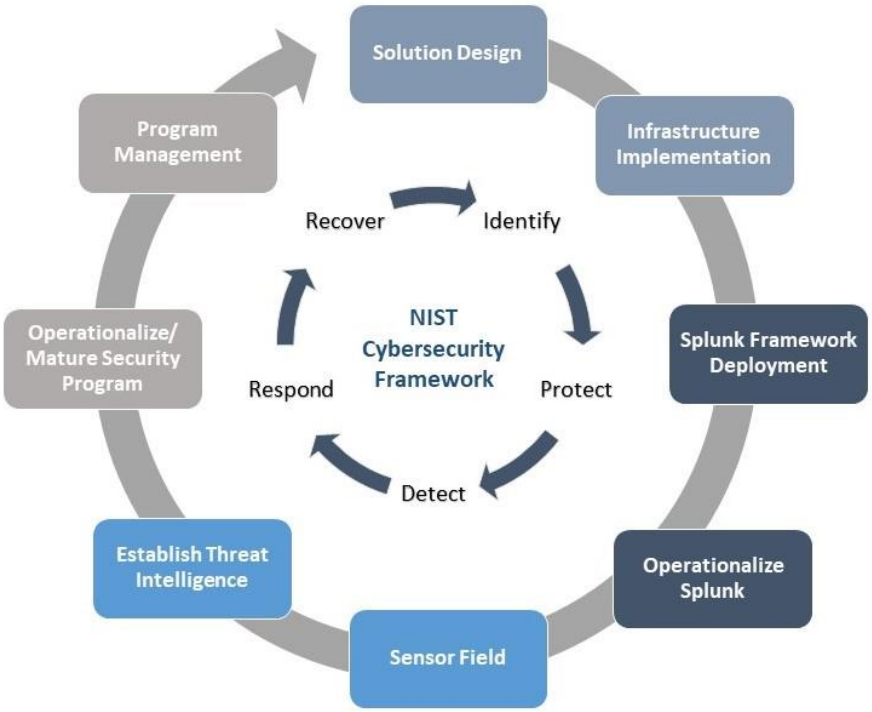

Figure 3: Copper River ES & Splunk Enterprise Platform Approach in relation to the NIST Cybersecurity Framework

We also understand your strict time constraints. Typical procurement processes can often be long and drawn out. As Alaskan Tribal 8(a) Owned, Copper River ES can provide procurement advantages through the Small Business Administration's (SBA) 8(a) Program. Under this program, a sole source contract can be established within a week, with a dollar threshold of $22 million and cannot be protested. This allows

for a scalable and long-term approach to funding a solution aimed at improving the cybersecurity platform of the agency.

HOW TO SOLE SOURCE CONTRACT WITH AN ALASKAN TRIBALLY OWNED 8(A) ENTITY

The process for establishing a direct, sole-source contract with an Alaskan Tribal entity, Native American Tribal entity, or Native Hawaiian Organization is very easy and has been streamlined with the help of the SBA. An acquisition official working with a government program manager would go through the following steps to establish and secure a direct, sole-source contract with an ANC, Alaskan Tribal entity, Native American Tribal entity, or Native Hawaiian Organization. Here is an overview of the six (6) step process:

Figure 4: Six Steps to Sole Source Contract with an Alaskan Tribally Owned 8(a) Entity

This process has been used effectively throughout the federal government to secure solutions in a timely, FAR compliant manner while also assisting government agencies in meeting their small business contracting goals. Meeting small business goals and using the SBA 8(a) program continue to be Administration policy.