{Fill out the White Paper template, as-is, below. Please do not modify the font size or margins. The response must be six (6) pages or less, plus the Eligibility Checklist. The checklist does not count against the 6 page limit.}

# 0. Contact information for <COMPANY NAME>

**Overall Point-of-Contact:**

Name

Title

Email

Phone number

**Technical Point-of-Contact:**

Name

Title

Email

Phone number

**Alternate Technical Point-of-Contact:**

Name

Title

Email

Phone number

# Introduction to <COMPANY NAME>

Provide a (maximum) 300-word overview of the submitting company.

# Executive Summary of <TECHNOLOGY NAME>

Provide a (maximum) 300-word summary of the technology.

# <TECHNOLOGY NAME> Architecture

## Technology Scope

Provide a description of the scope of the technology:

* What kind(s) of data does it leverage?
* How does the UI increase effectiveness and efficiency of operators in the presentation of data?
* Does it provide threat intelligence and/or integrate with threat intelligence platforms? In particular,
  + Can users access open source or in-house threat intelligence and/or create custom feeds?
  + Does it provide a Secret (classified, SIPRNET) threat intelligence database integration?
* What playbooks are provided?
* How configurable are playbooks & how easily are custom playbooks configured?
* How can playbooks be shared across organizations?
* What collaboration is possible across distinct remote sites?
* Can multiple analysts collaborate on an incident in real-time? Asynchronously via a “hand-off” of all needed data/documentation?
* Can multiple SOCs in different networks work together on incidents via a cloud or on-prem cloud-like capability?
* Is data encrypted on all traffic crated by this SOAR tool? Does it use encryption at rest, i.e., is stored data encrypted?
* What kind of automation is provided, e.g., can all playbooks be automated; are tickets/documentation auto-populated?
* Do you have partnerships or a community of interest that support this solution?
* What (if anything) is unique about this technology?

## Architecture and Integration Points

Provide a description of the architecture and deployment model for the technology, including communication points of integration. Be sure to include:

* What is the form factor for the technology? Software? Hardware? Virtual Machine?
* What are the logical components of the technology and their role? E.g., is there a separate analytic engine and management server?
* What dependency does the technology have on additional network-level capabilities (e.g., a network traffic analyzer, SIEM)? What of those are provided in the submission and what are assumed to be present?
* Does this SOAR tool provide asset information and/or link asset information to logs?
* How does the technology integrate into an enterprise defense? In particular,
  + Does it interact with a SIEM, provide a SIEM, or use some other configuration?
  + Does it operate/communicate on the enterprise network or require an out-of-band network?
  + Is there a performance limit with respect to network data rate or network flow rate?
  + Does the technology easily sync to a provided Network Time Protocol (NTP) service?
  + How does it protect itself from attack?

## Application of Artificial Intelligence/Machine Learning (AI/ML)

Provide a description of how the technology leverages AI/ML. Please specify general approaches (supervised, unsupervised) and conceptual description of how these apply to the data. If the technology uses a hybrid signature-based and AI/ML-based solution, please specify the components that leverage each.

## Data Dependencies and Formats

Provide a description of any and all data dependencies and expected ingestion format for each. Also, please specify whether the data is critical for functionality of the technology or supplemental. For example, if the technology ingests a network data stream but requires network services within that network data stream (e.g., DNS, DHCP), specify those data dependencies with PCAP as the format.

## Playbooks

Provide a description of the preset sequences of actions outlined for an analyst to take in certain situations, if/how these are configurable, and if they are automatable.

## Collaboration via Cloud-like Capability

How can operators work across different SOCs and different networks to collaborate through this SOAR tool? Is a cloud connection necessary or are there “on-prem” abilities or alternate channels to coordinate across networks with instances of this SOAR tool?

## Cost Information

Provide a description of the cost associated with the technology. Specifically,

* Subscription fees for each tool for a 1500 node network, 10Gb/s rate with references to your website rates (initial purchase and annual support, plus any other expected costs or fees)
* Expected HW requirements
* Estimated setup time for SOC operators
* How much time for a SOC Operator to become a “local expert”
* Do you provide any installation, initial use support, or on-going maintenance and technical support? If so, provide pricing guide.

# <TECHNOLOGY NAME> Technology/Resource Requirements

Provide a description of the optimal resources to operate the technology, and any performance expectations or constraints associated with the technology. For example, capacity of network input, memory/disk/CPU requirements, or access via ssh.

# <TECHNOLOGY NAME> Evaluation Approach

Provide a description of the recommended approach to evaluating this technology. This may include ways the core capabilities and the unique capabilities of the tool can be showcased. This may be used to help shape the evaluation.

Does your technology provide enhanced ROI, and if so, how do you measure it? What metrics does your tool gather to show efficiencies and performance?

NOTE: Please do not submit any sensitive or classified information.

# < TECHNOLOGY NAME> Eligibility Checklist

|  |  |  |
| --- | --- | --- |
| **Criterion** | **Response:  Yes/No** | **Submitter Comments** |
| Is the submitter incorporated in the USA or US citizen(s)? |  |  |
| Is the white paper and technology Unclassified? |  |  |
| Are the Demonstration Video AND the Overview Video included, with both under 10 min. each? |  |  |
| Are the software/VM components submitted as configured as possible AND can the submitted technology be installed, set up, and configured in under 16 hours? |  |  |
| If a VM is submitted, is it compatible with VMWare? (If no VM is submitted please mark “n/a”) |  |  |
| Are there subsidiary logs or tools that are needed on the test network for the submitted technology to operate? If so, please itemize and/or explain. |  |  |
| Is the submitted technology capable of allowing customized playbooks to guide junior analysts through high-frequency tasks? |  |  |
| Can all playbooks be automated? |  |  |
| Does the submitted technology have or integrate with ticketing tools AND does it populate tickets during investigations? |  |  |
| Can the submitted technology operate on-premises with no dependency on cloud or external network connectivity? |  |  |
| Can the submitted technology allow collaboration of geographically disparate operators in different networks via a cloud or on-prem capability? |  |  |
| Does the submitted technology operate in a network with up to 10 Gb/s and up to 5000 IPs? |  |  |
| Is the submitted technology capable of synchronizing with an NTP server? |  |  |
| Does the submitted technology include licenses for up to 7 operators on up to 3 networks through December 2021? |  |  |
| Does the submission include an up-to-date setup guide, i.e., documentation for installation and configuration? |  |  |
| Does the submitting entity own the intellectual property of the technology? Note: 3rd party submissions, including licensed re-sellers of the technology, are not eligible. |  |  |

NOTE: Answering NO to any of these questions will likely result in the submitted technology being ineligible.