# 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 of detection does it provide?   
  For example, malicious network behavior detection, network anomaly detection, user behavior analysis, digital loss prevention, malware transmission.
* What kind(s) of threats does it target?
* What kind(s) of data does it leverage?
* What kind of data and/or human insight does it provide?
* What (if anything) is unique about this technology?
* What (if anything) does the technology provide in terms of a user interface?

## 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? 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 decrypter, SIEM)? What of those are provided in the submission and what are assumed to be present?
* How does the technology integrate into an enterprise defense?
  + Does it monitor a passive network tap?
  + Does it interact with a SIEM?
  + 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?

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

Provide a description of the ways in which 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.

If supervised or semi-supervised, please discuss the strategy for labeled data acquisition, and any tuning that can occur locally (feedback process or on-prem model retraining).

## 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 (DNS, DHCP, etc.), specify those data dependencies with PCAP as the format.

## Alerting/Notification

Provide a description of the ways in which the technology can alert on or notify of a detected malicious event (e.g., device local logging, syslog message). Specifically comment on the technology’s ability to generate network logs of alerts to a SIEM, and all formats supported.

Also, specify ways that a collection of the technology’s aggregated alerts may be exported en masse. One possible AI-ATAC evaluation approach is to run an adversarial campaign, and then post-test export a detection technology’s full set of alerts to measure its detection efficacy during the campaign. Please comment on 1) the technology’s ability to support that process, and 2) its ability to be cleared or reset to a known state (erasing any observations or insights gained from a test run).

## 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
* 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 and initial use support? If so, provide pricing guide.
* Comment on the technology’s ability to generate network logs of alerts to a SIEM, and all formats supported.

# <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 types of network behaviors, specific exploits, APT patterns, or general threats that would showcase the technology’s discriminating capabilities. This will be used to help shape the evaluation.

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? |  |  |
| Does the technology operate at the network level, or operate on data acquired from network devices and/or resources? |  |  |
| Is the technology capable of ingesting a network data stream (passive tap)? |  |  |
| Is the technology capable of generating network alerts to a SIEM via UDP? |  |  |
| 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. |  |  |
| Does the technology operate on-premises with no dependency on cloud or external network connectivity? |  |  |
| Does the technology have a way to snapshot and restore any and all ML models, including models derived through online learning? |  |  |
| Does the technology operate in a 10 Gb/s network with up to 1500 nodes, and with actual data rates up to 3 Gb/s? |  |  |
| Is the technology capable of synchronizing with an NTP server? |  |  |
| Does the technology submission include a license through December 2020? |  |  |
| Does the technology include full and up-to-date documentation for installation and configuration? |  |  |
| Does the technology provide visibility into resource usage (memory, CPU, disk I/O, network I/O) of its components? |  |  |
| Does the technology have the capability to erase all observed events and all other potentially persistent information gleaned from an operational environment? |  |  |