

SRI International

Next-generation Intrusion Detection Expert System (NIDES) A Summary¹

**Debra Anderson
Thane Frivold
Alfonso Valdes**

**Computer Science Laboratory
SRI-CSL-95-07, May 1995**

333 Ravenswood Avenue • Menlo Park, CA 94025-3493 • (415) 326-6200 • FAX: (415) 326-5512 • Telex: 334486

¹This report was prepared for the Department of the Navy, Space and Naval Warfare Systems Command, under Contract N00039-92-C-0015

Contents

1	Introduction	1
1.1	Previous Work	2
1.2	Related Work	3
1.2.1	Advisor Project	3
1.2.2	FBI FOIMS-IDES Project	4
1.2.3	Safeguard Project	4
1.2.4	NIDES Training Course	4
1.3	Project Overview	5
2	Software Prototypes	7
2.1	Alpha Release	7
2.2	Alpha-patch Release	8
2.3	Beta Release.	10
2.3.1	Documentation	10
2.3.2	Features	10
2.3.2.1	Optimization of Profile Structure	11
2.3.2.2	Analysis Configuration (Real-time and Batch)	11
2.3.2.3	Status Reporting	13
2.3.2.4	Data Management Facility	13
2.3.2.5	Expanded Rulebase	13
2.4	Beta-update Release	13
2.4.1	Bug Fixes	13
2.4.2	Performance Improvements	15
2.4.3	New Features	16
2.4.3.1	Perl Script	

2.5.1.2	Agend	21
2.5.1.3	Agen	21
2.5.1.4	Arpool	22
2.5.1.5	Statistical Analysis Component	22
2.5.1.6	Rulebased Analysis Component	22
2.5.1.7	Resolver	23
2.5.1.8	Archiver	23
2.5.1.9	Batch Analysis	23
2.5.1.10	User Interface	23
2.5.2	Operation	23
2.5.2.1	Real-time Operation	24
2.5.2.2	Batch Operation	25
3	Future Directions	27
3.1	Technology Transfer and Operational Evaluation	27
3.2	User Support and Training	28
3.2.1	NIDES Maintenance	28
3.2.2	Training	28
3.2.3	Telephone and On-site Support	28
3.2.4	Configuration Management	29
3.3	Security Goals	29
3.4	Network NIDES	31
3.4.1	Data Collection	31
3.4.2	Rulebase	31
3.4.3	Statistical Measures	32
3.5	Intrusion-Detection Testbed	32
3.6	Rulebase Expansion.	33
3.7	Profiling Other Entities	33
3.8	Enhanced Component Independence	34
	Bibliography	35