

Technique: <i>basics</i>	■ Pros	Subtypes
	■ Cons	
A) Statistical-based: <i>stochastic behaviour</i>	<ul style="list-style-type: none"> ■ Prior knowledge about normal activity not required. Accurate notification of malicious activities. ■ Susceptible to be trained by attackers. Difficult setting for parameters and metrics. Unrealistic quasi-stationary process assumption. 	A.1) Univariate models (<i>independent Gaussian random variables</i>) A.2) Multivariate models (<i>correlations among several metrics</i>) A.3) Time series (<i>interval timers, counters and some other time-related metrics</i>)
B) Knowledge-based: <i>availability of prior knowledge/data</i>	<ul style="list-style-type: none"> ■ Robustness. Flexibility and scalability. ■ Difficult and time-consuming availability for high-quality knowledge/data. 	B.1) Finite state machines (<i>states and transitions</i>) B.2) Description languages (<i>N-grams, UML, ...</i>) B.3) Expert systems (<i>rules-based classification</i>)
C) Machine learning-based: <i>categorization of patterns</i>	<ul style="list-style-type: none"> ■ Flexibility and adaptability. Capture of interdependencies. ■ High dependency on the assumption about the behaviour accepted for the system. High resource consuming. 	C.1) Bayesian networks (<i>probabilistic relationships among variables</i>) C.2) Markov models (<i>stochastic Markov theory</i>) C.3) Neural networks (<i>human brain foundations</i>) C.4) Fuzzy logic (<i>approximation and uncertainty</i>) C.5) Genetic algorithms (<i>evolutionary biology inspired</i>) C.6) Clustering and outlier detection (<i>data grouping</i>)