

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