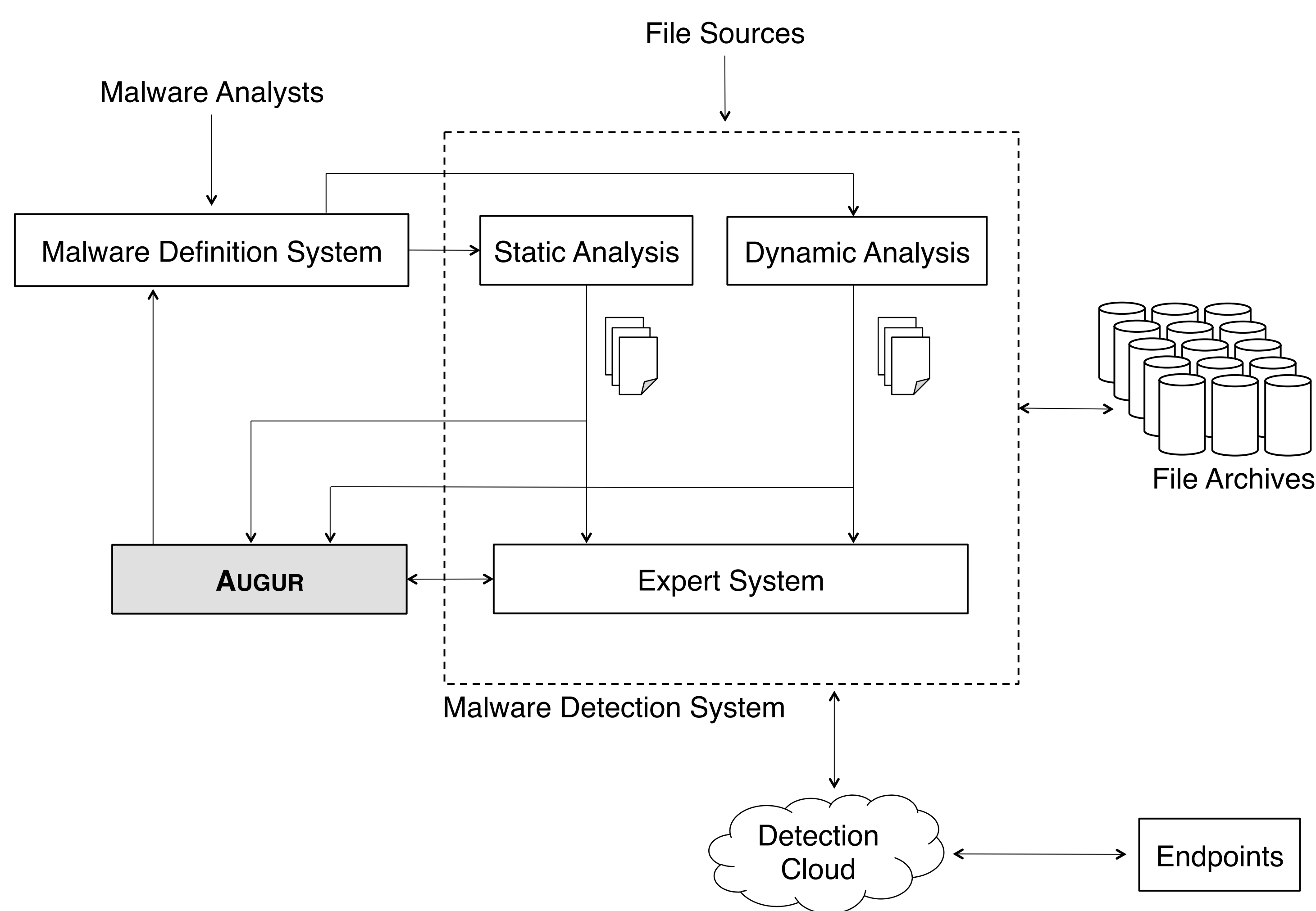
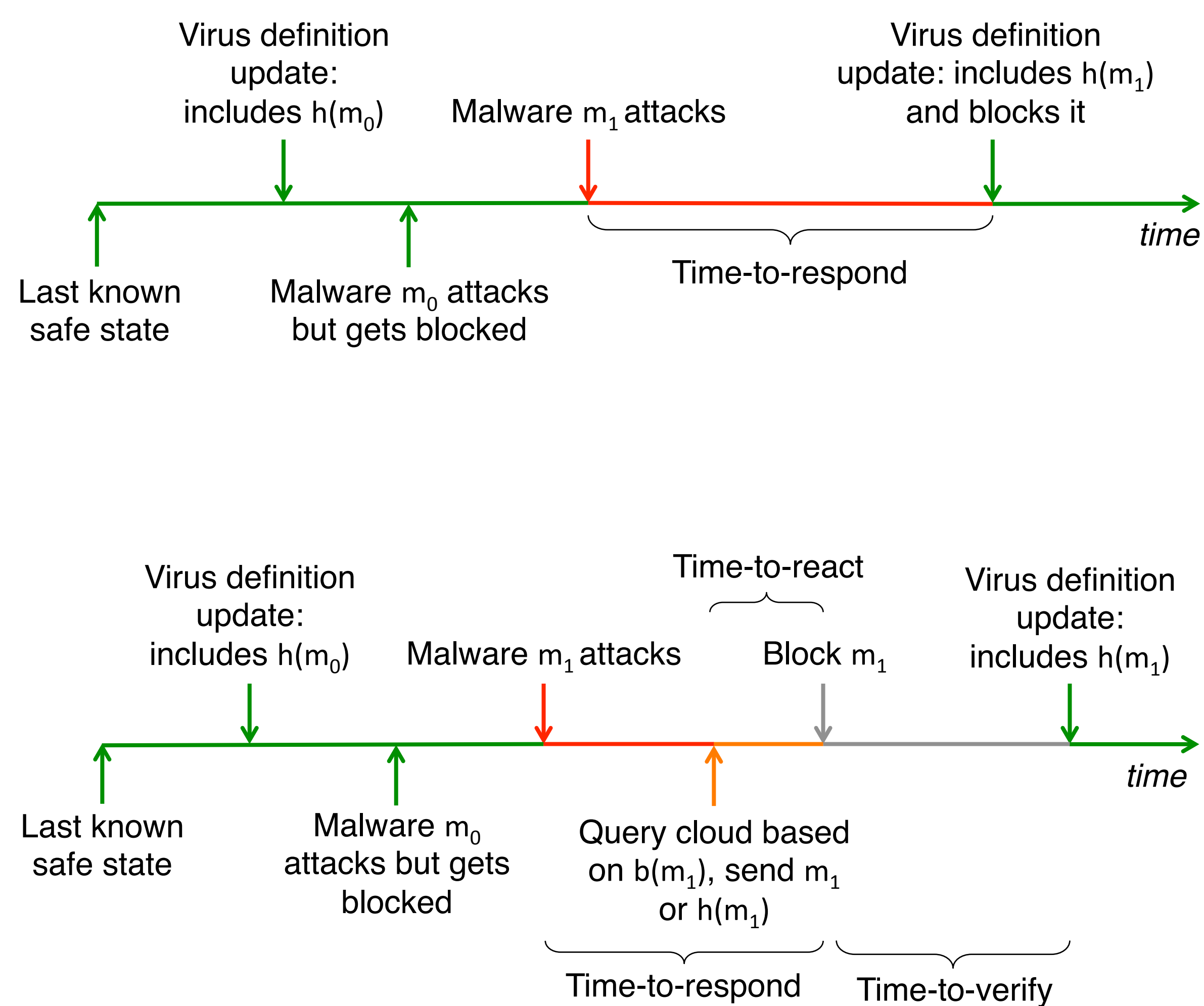


AUGUR: Aiding Malware Detection Using Large Scale Machine Learning

Yazan Boshmaf, Matei Ripeanu, Konstantin Beznosov
University of British Columbia

Kyle Zeeuwen, David Cornell, Dmitry Samosseiko
SophosLabs, Sophos Inc.

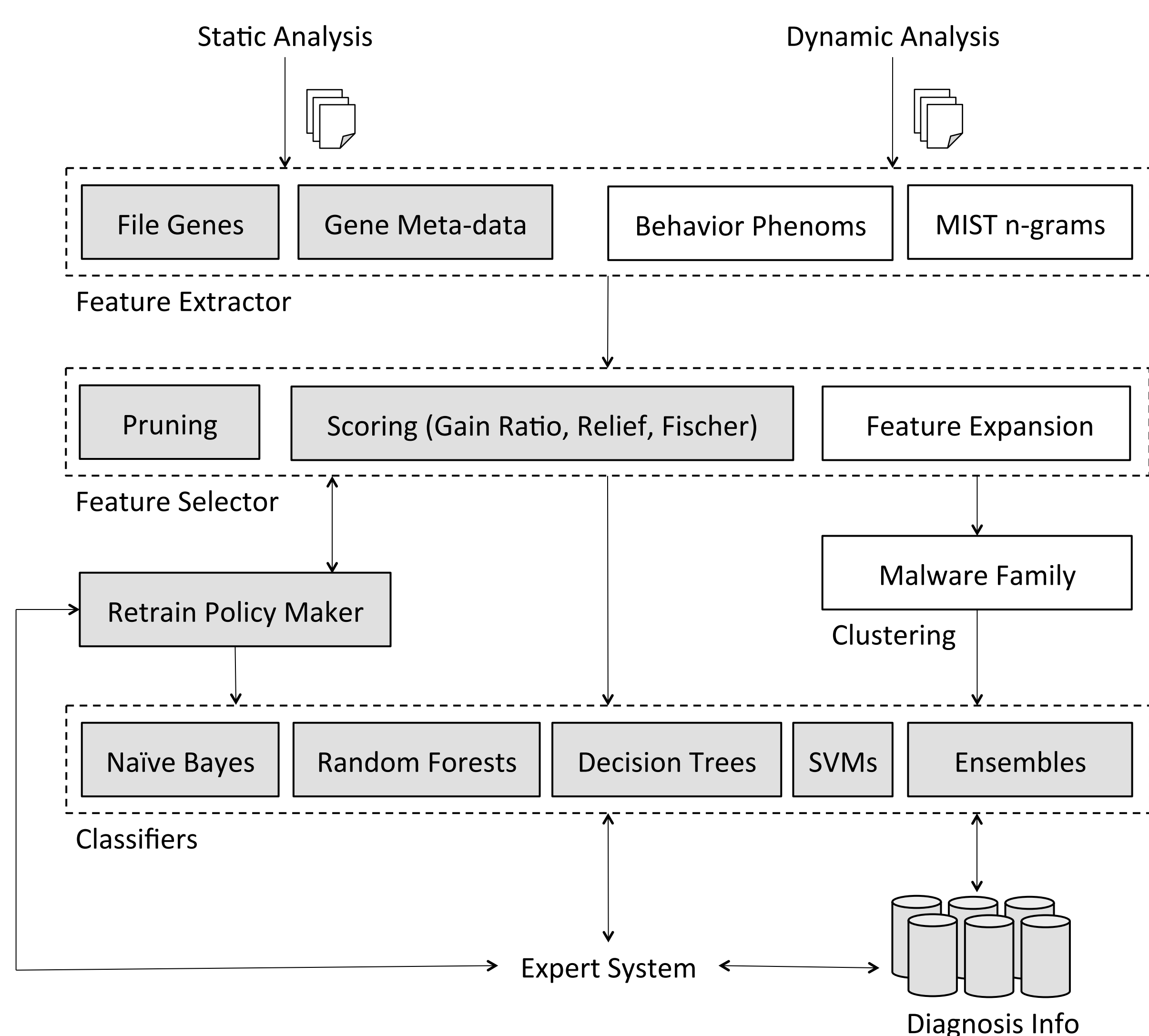


Malware Protection at the Endpoint

Malware Detection at Sophos Inc.

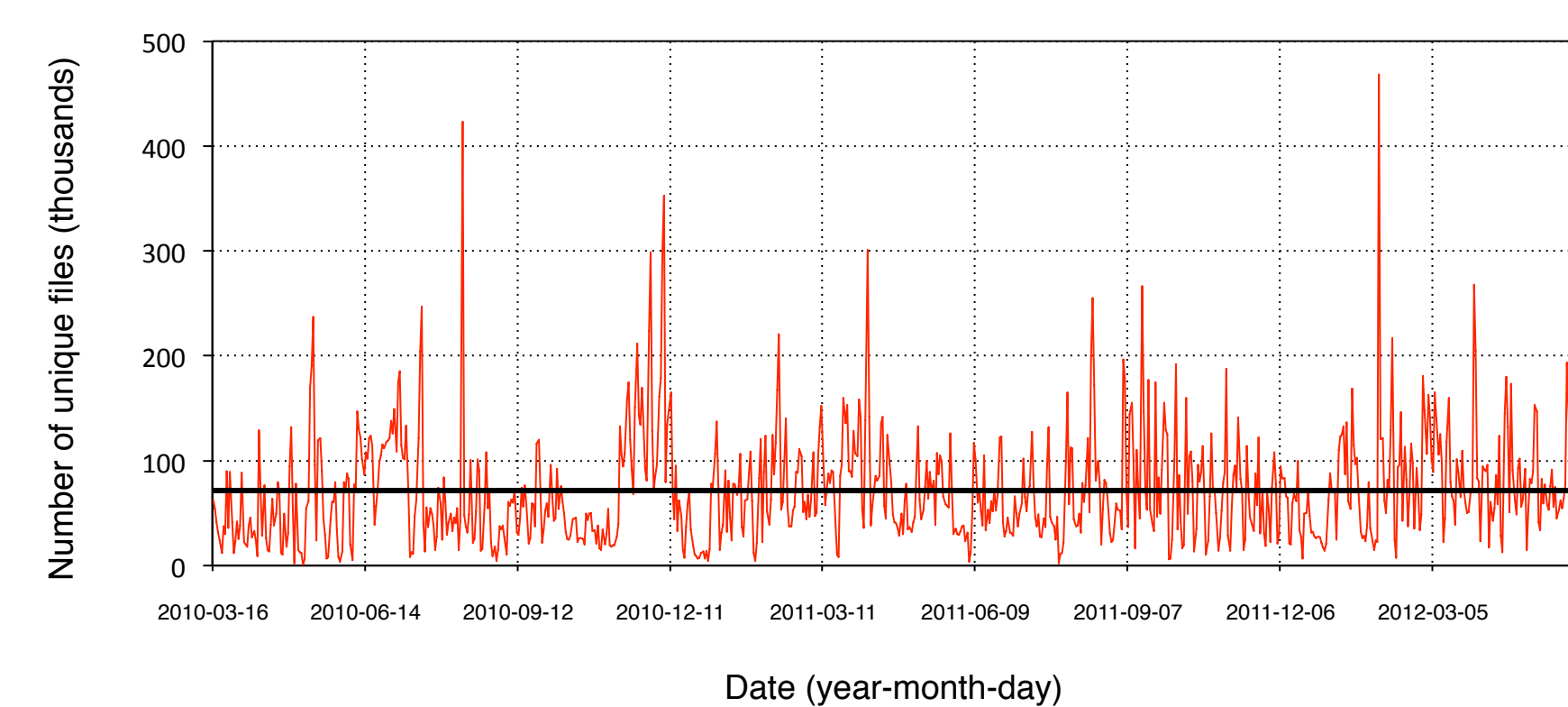
How to make faster reactions to suspicious software?

How to automatically generate effective signatures?

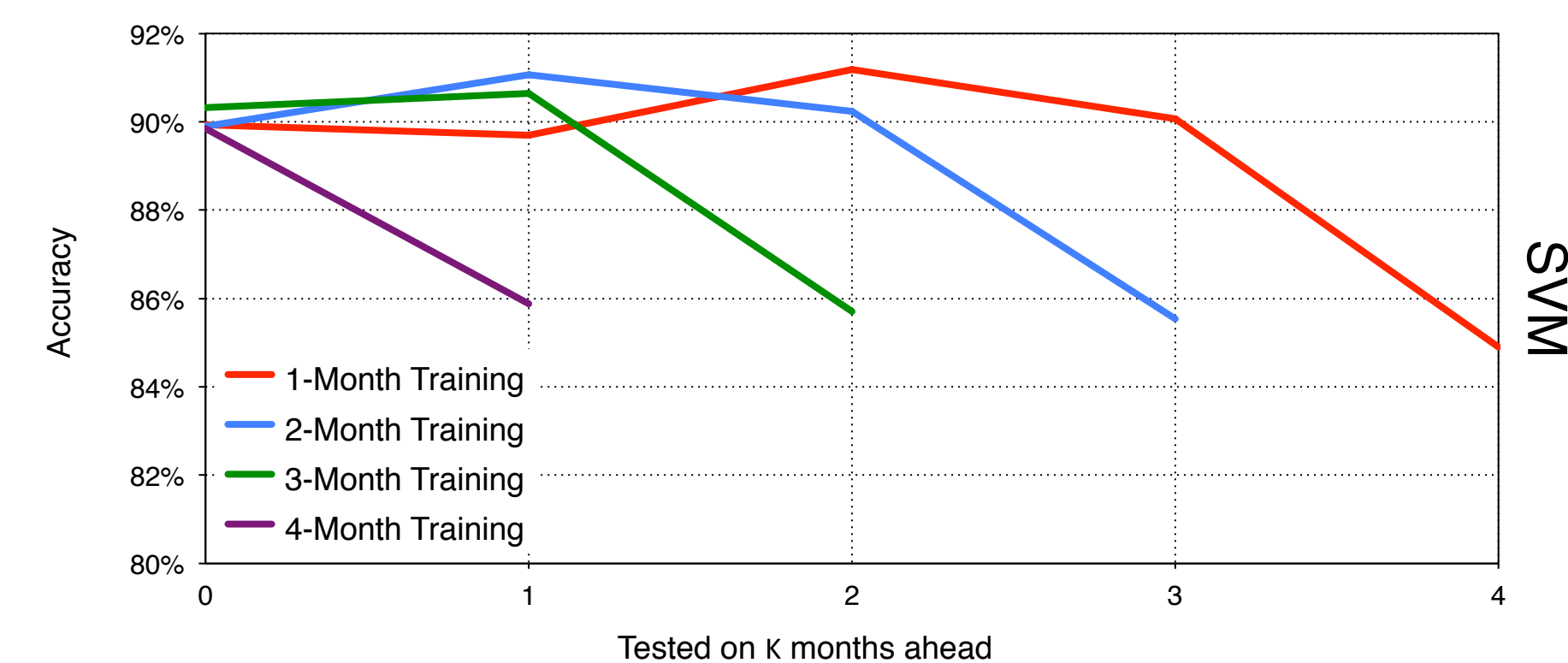


High-Level Design of AUGUR

71.5K new files received on an average day (lower estimate)



Retrain every three months using one-month worth of file samples



Use a sample size of $\geq 5K$ unique files (95% conf.)

