System Health Monitoring and Reactive Measures Activation

Alireza Shameli Sendi
Michel Dagenais
Department of Computer and Software Engineering

June 29, 2010
École Polytechnique, Montreal

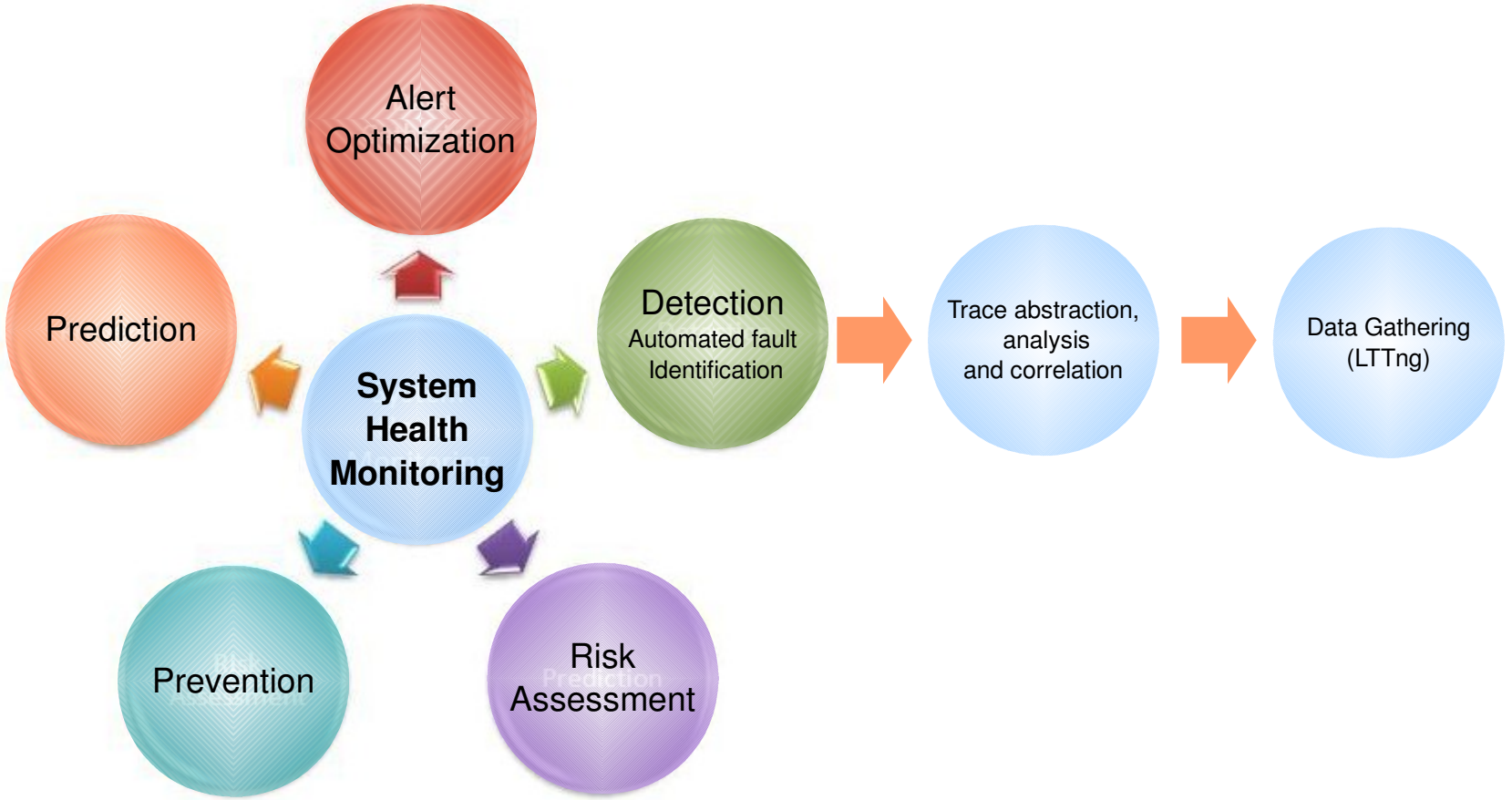
Content

- **Definition, components and architecture**
- **Alert optimization**
- **Prediction**
- **Risk Assessment**
- **Prevention**
- **References**

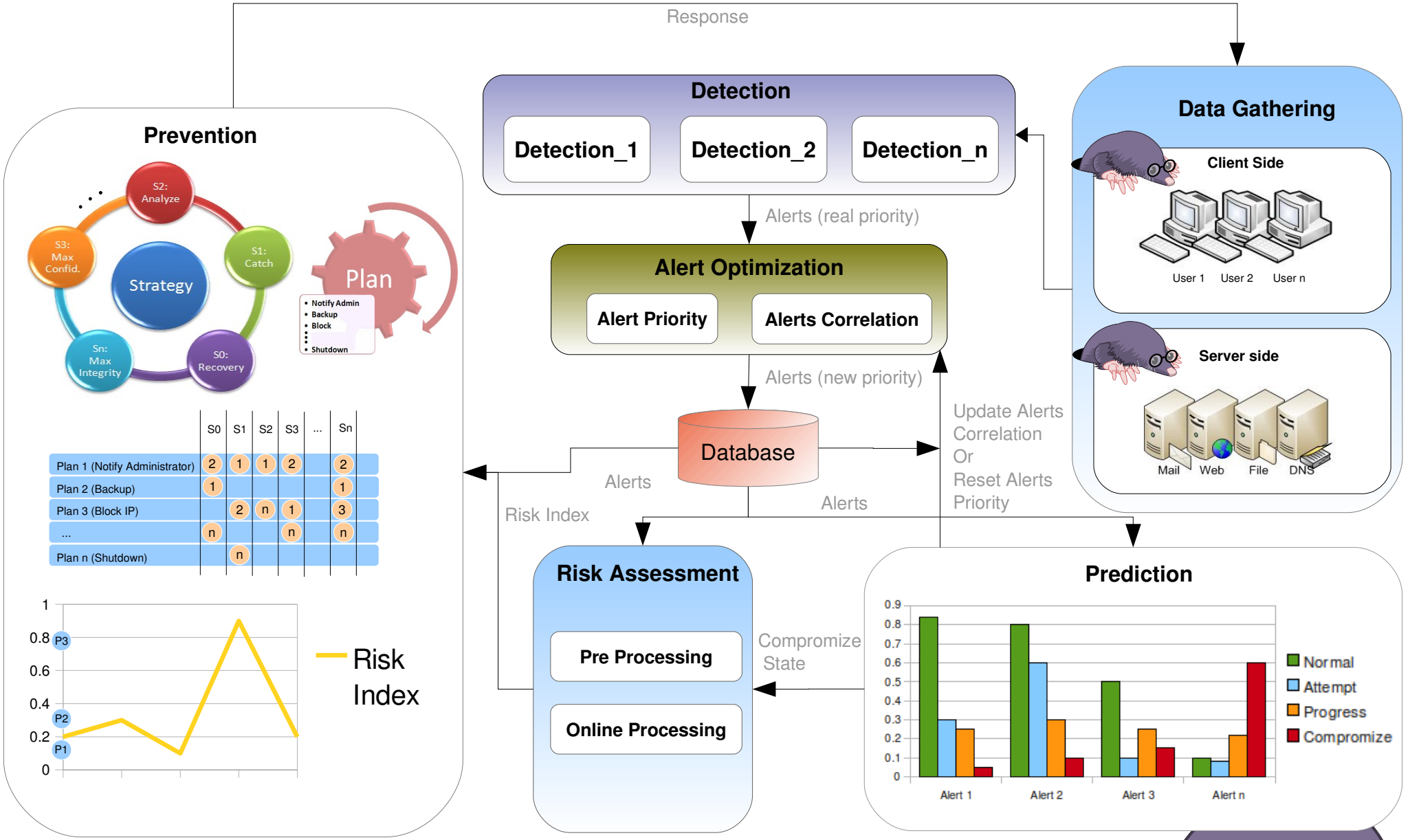
System Health Monitoring and Reactive Measures Activation

SHM continuously monitors the health of a multi-core distributed system so that system anomalies (bad behaviors and attacks) can be detected and handled appropriately

System Health Monitoring Components



System Health Monitoring Architecture



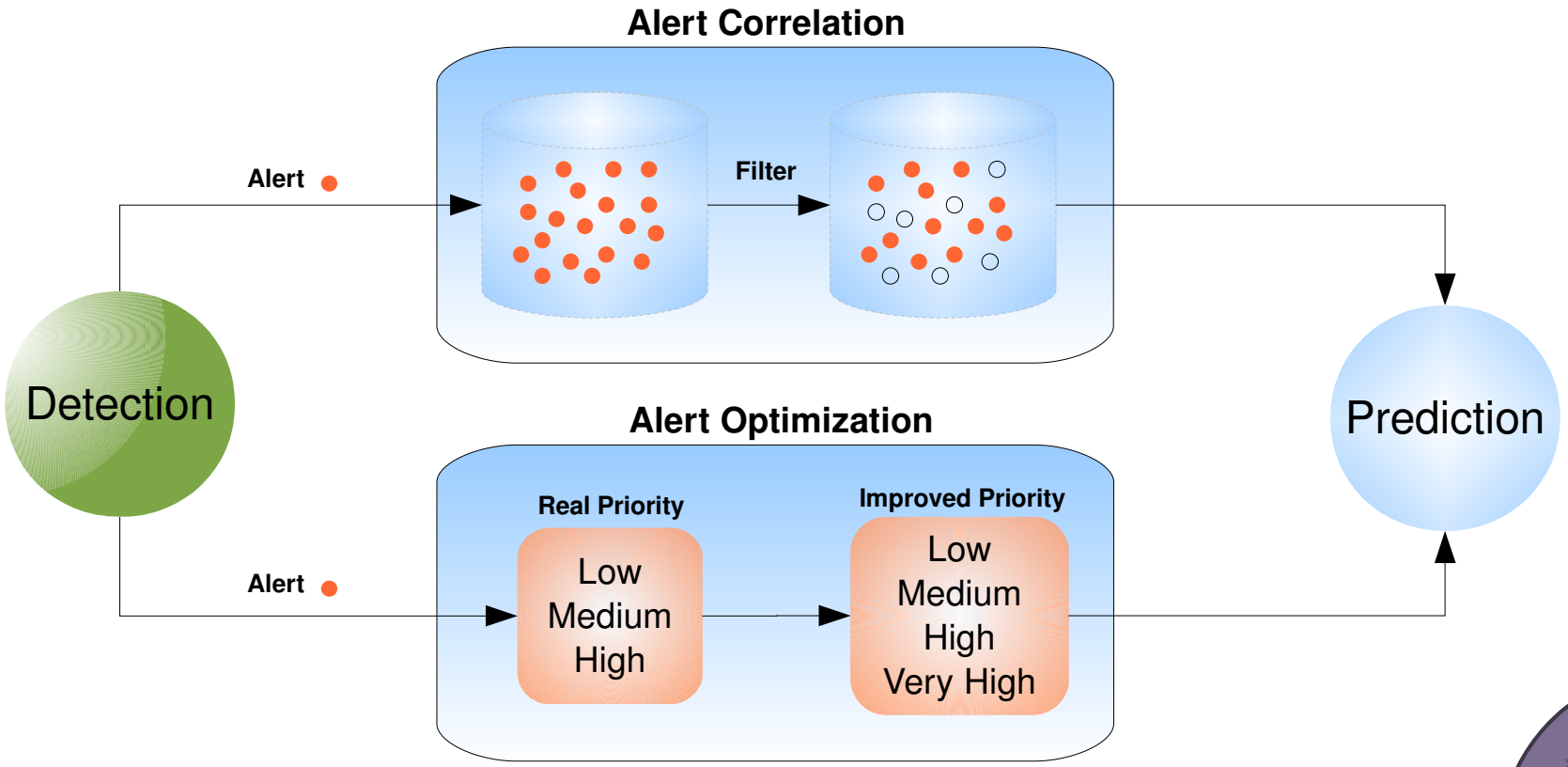
Alert Optimization

Alert Optimization (1)

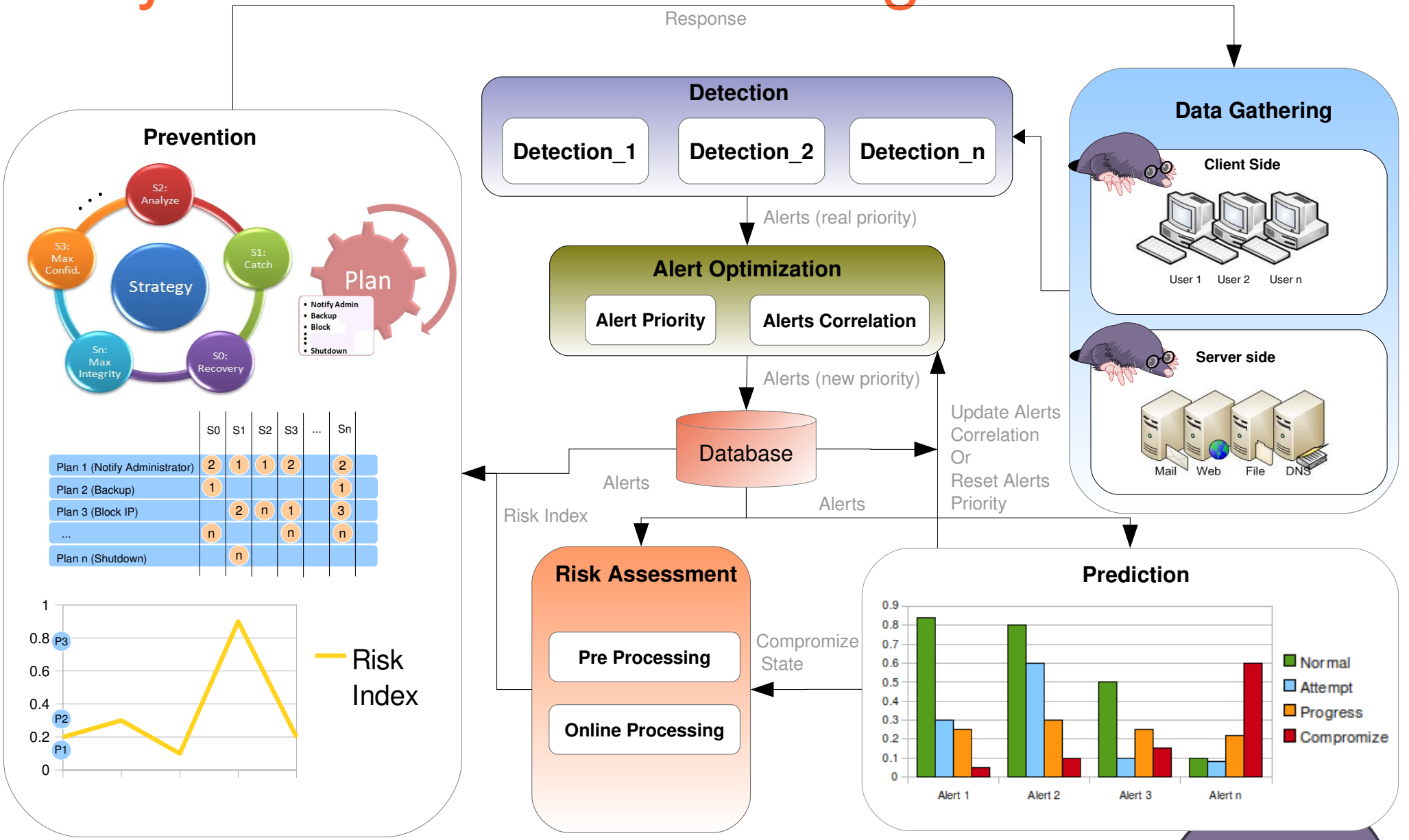
- Alert correlation means to extract true alerts from alerts generated by detection component (filter view)
- In this project, we have taken a different view comparing to the filter view
- Multi steps attack's actions are unknown but may be partially detected by detection component and reported as alerts

Alert Optimization (2)

- Alert optimization component **increases alert priority with correlation concepts**



System Health Monitoring Architecture



Alert Optimization (3)

- Alerts Correlation
  - Alerts correlation shows correlation weights between any two alerts
  - It plays an important role in attack prediction
  - It is defined by expert persons
  - It will be updated by receiving hints from prediction component. It happens whenever the probability of progress state is more than 90%

	Alert 1	**Alert 2**	**Alert 3**	**Alert n**
Alert 1	W11	W12	W13	W1n
Alert 2	W21	W22	W23	W2n
Alert 3	W31	W32	W33	W3n
Alert n	Wn1	Wn2	Wn3	Wnn

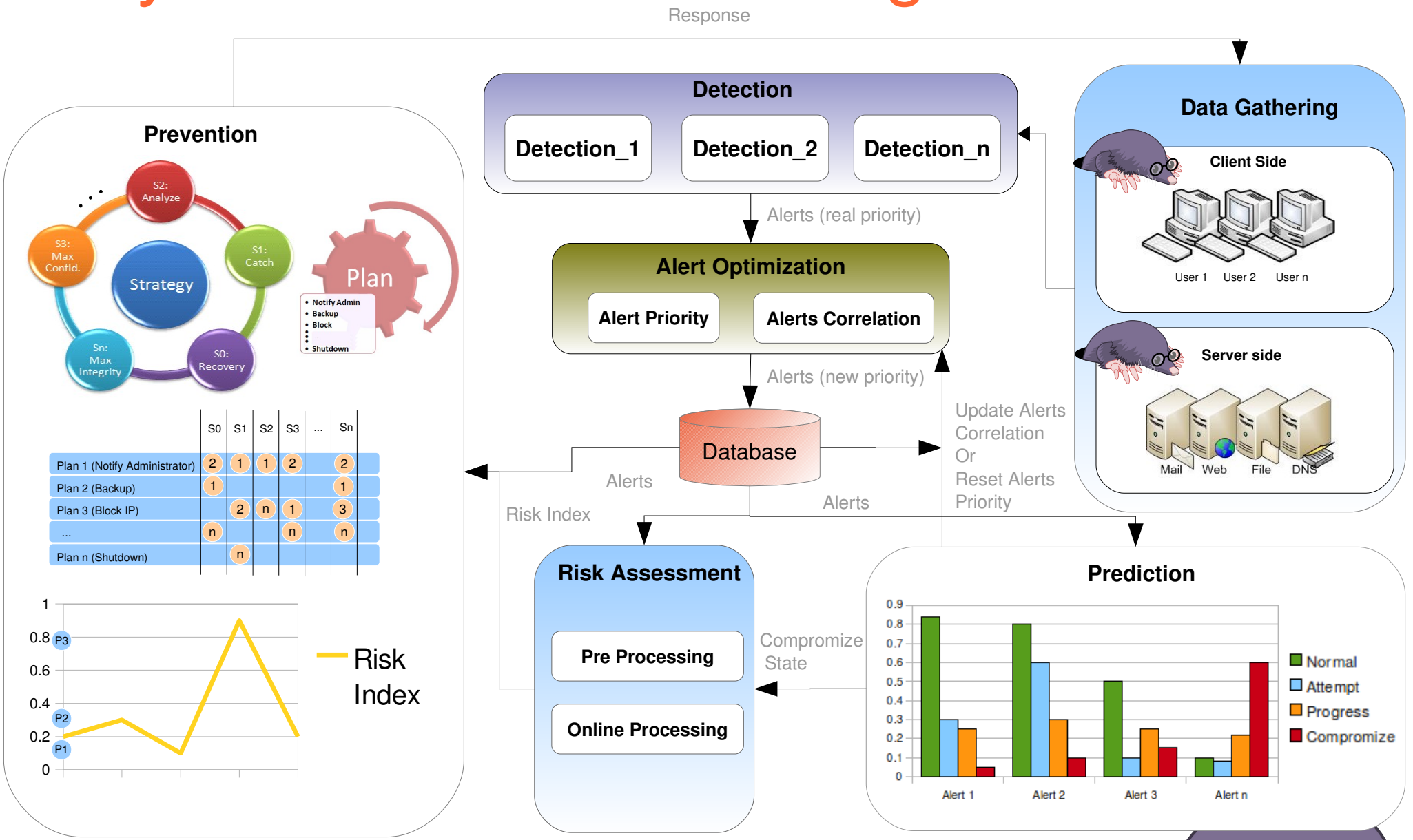
Alert Correlatiom Matrix (ACM)

Alert Optimization (4)

- Alert Priority
  - Alert priority is computed by an exponential formula
  - At the beginning, it is equal to the real priority of alert
  - The equation for each alert is : $f_{\text{priority}} = e^{E*N/(K*A-E*N)}$
    - E (Effect of Alert): It is extracted from the Alert Correlation Matrix and is varied if ACM is updated
    - N (Frequency of each Alert)
    - A (Acceptable number of alert per day)
    - K (Empirical constant): Function has good results with K=200
  - *f* is reset when prediction component sent a message that an intrusion will be happend

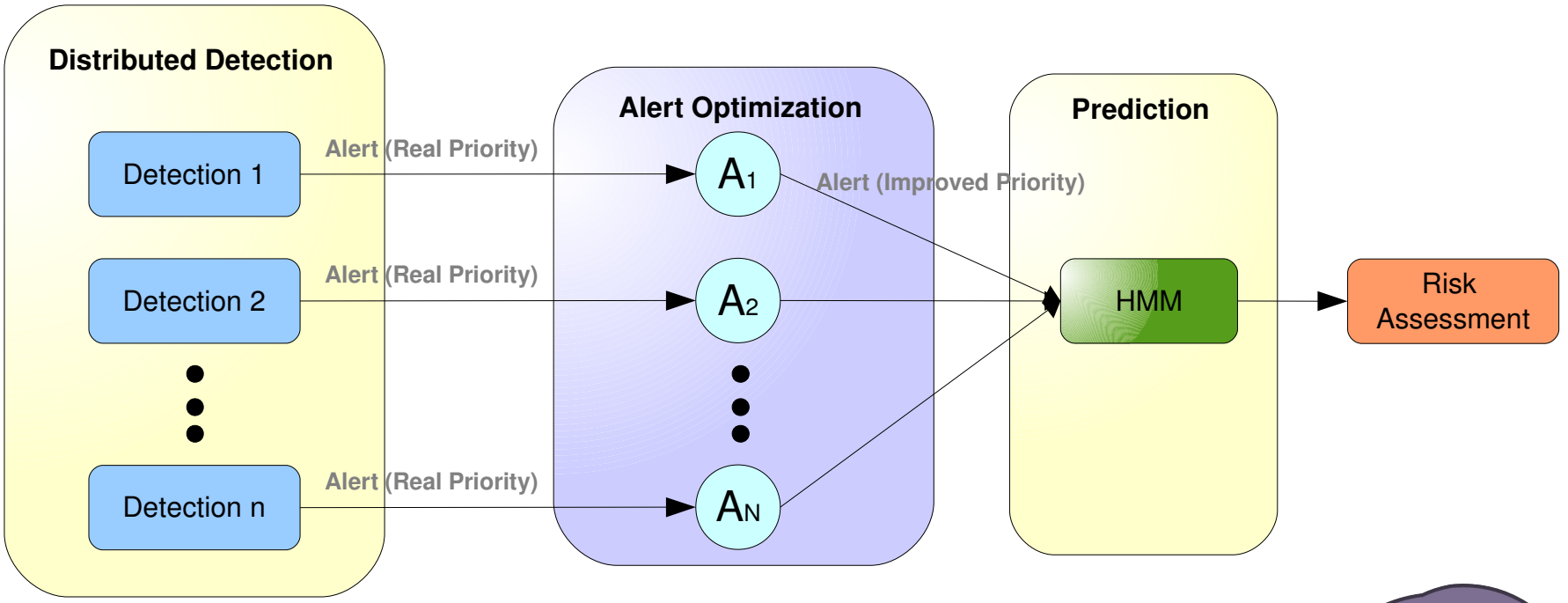
Prediction

System Health Monitoring Architecture

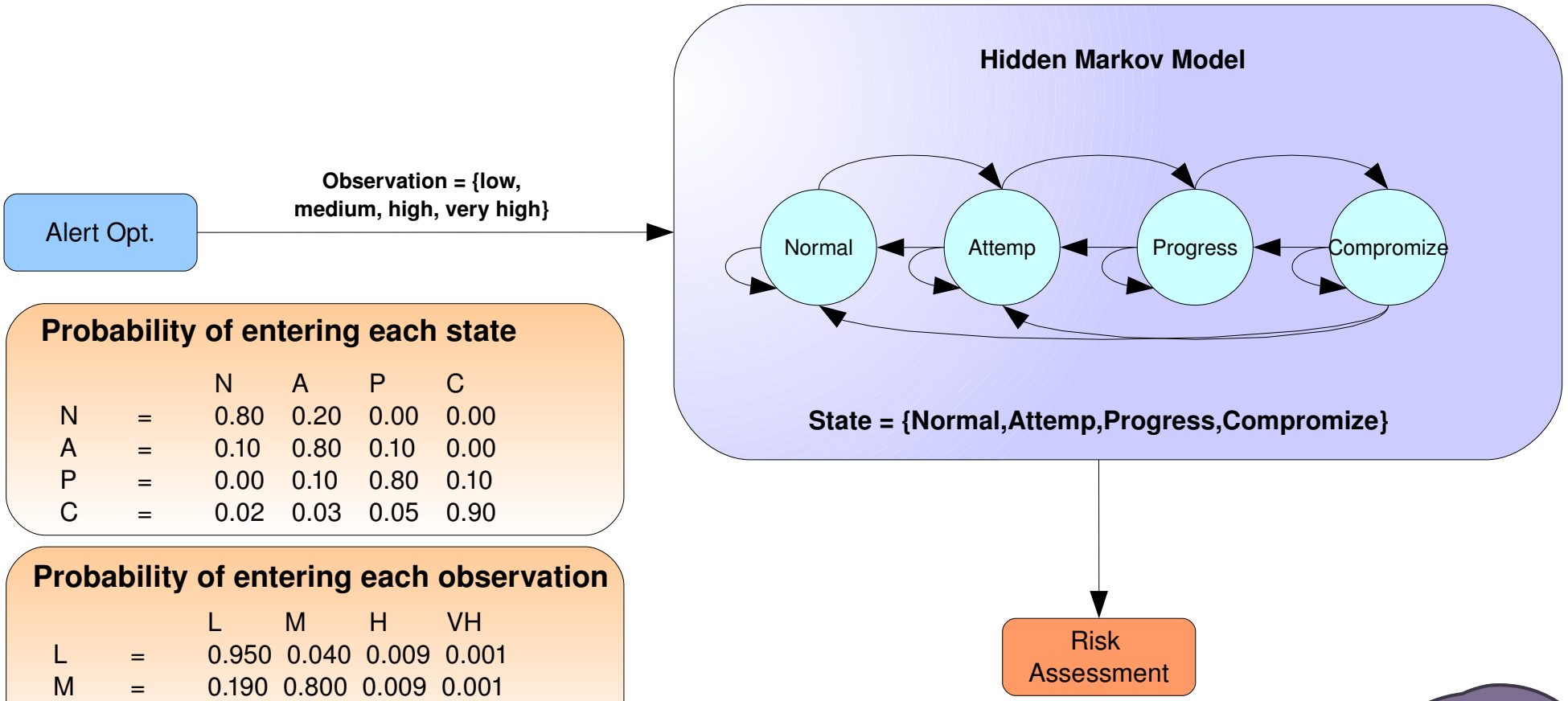


Prediction Structure

- The prediction component will attempt to make a prediction of a possible future problem
- A model is needed to capture the interaction between the attacker and the distributed network



Prediction Algorithms-HMM



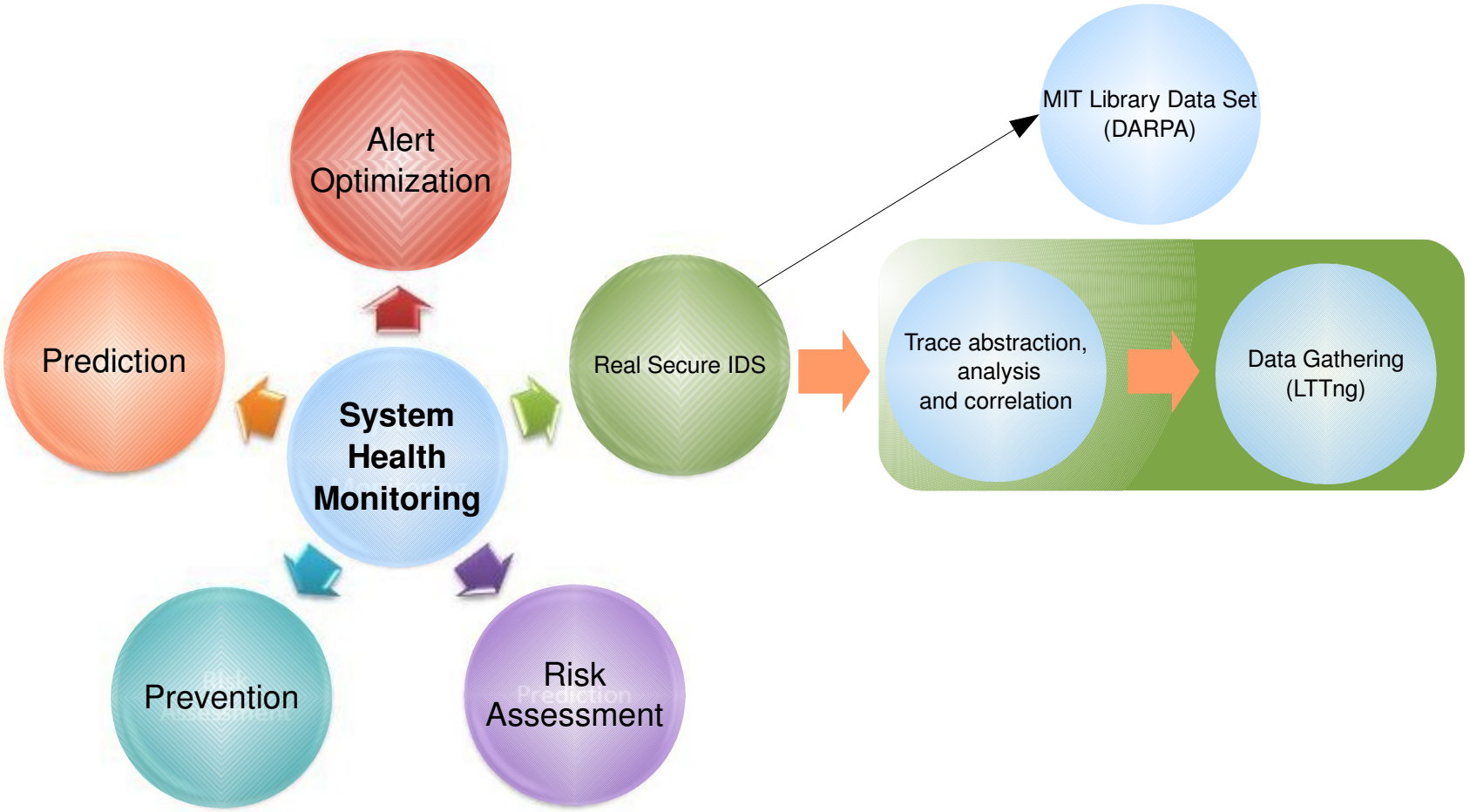
Probability of entering each state

		N	A	P	C
N	=	0.80	0.20	0.00	0.00
A	=	0.10	0.80	0.10	0.00
P	=	0.00	0.10	0.80	0.10
C	=	0.02	0.03	0.05	0.90

Probability of entering each observation

		L	M	H	VH
L	=	0.950	0.040	0.009	0.001
M	=	0.190	0.800	0.009	0.001
H	=	0.010	0.190	0.700	0.100
VH	=	0.010	0.040	0.200	0.750

Prediction Results (1)



Prediction Results (2)

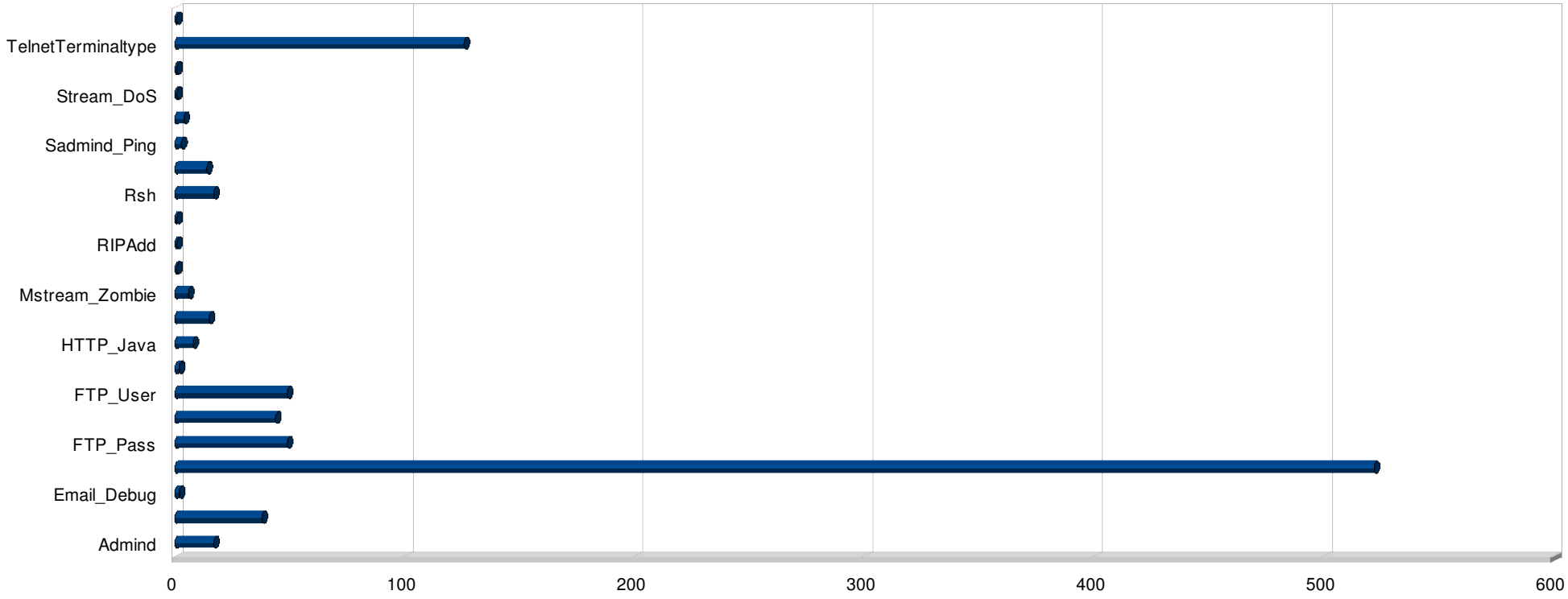
- Lincoln Laboratory 2000 data set (DARPA)
- The data set contains more than 3 hours of intrusion detection data
- The data set contains an attack in 5 phases
- Finally, 3 hosts are attacked and compromised

Prediction Results (3)

Phase	Name	Time	Goal
1	IP sweep	9:45 to 09:52	The attacker sends ICMP echo-requests in this sweep and listens for ICMP echo-replies to determine which hosts are "up"
2	Sadmind Ping	10:08 to 10:18	The hosts discovered in the previous phase are probed to determine which hosts are running the "sadmind" remote administration tool. This tells the attacker which hosts might be vulnerable to the exploit that he/she has
3	Break into	10:33 to 10:34	The attacker then tries to break into the hosts found to be running the sadmind service in the previous phase. Breakins via the sadmind vulnerability
4	Installation	10:50	Installation of the trojan mstream DDoS software on three hosts
5	Launch	11:27	Launching the DDoS

Prediction Results (4)

- RealSecure generates 922 alerts based on DDOS1.0

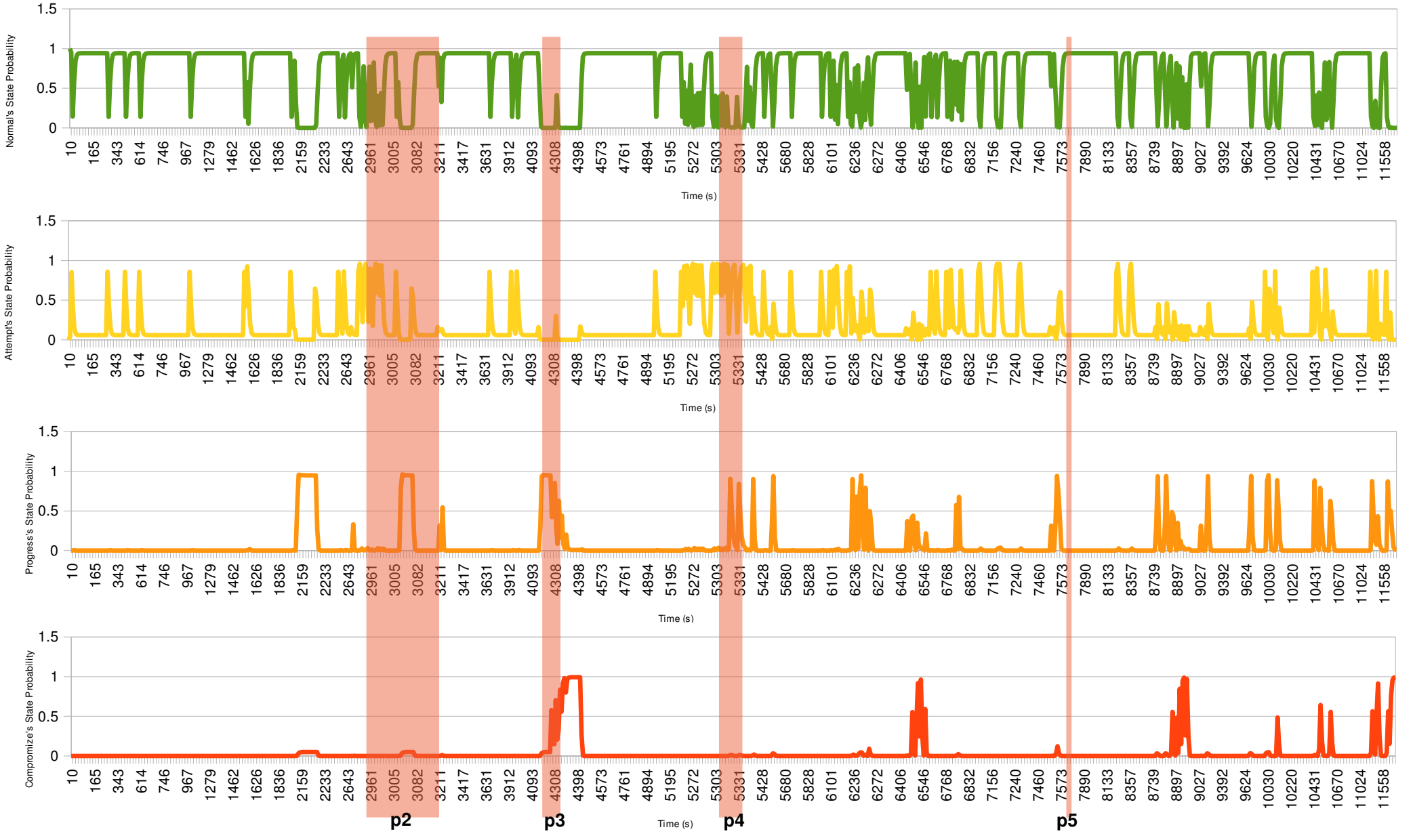


Prediction Results (5)

- RealSecure generates this alerts for each phases

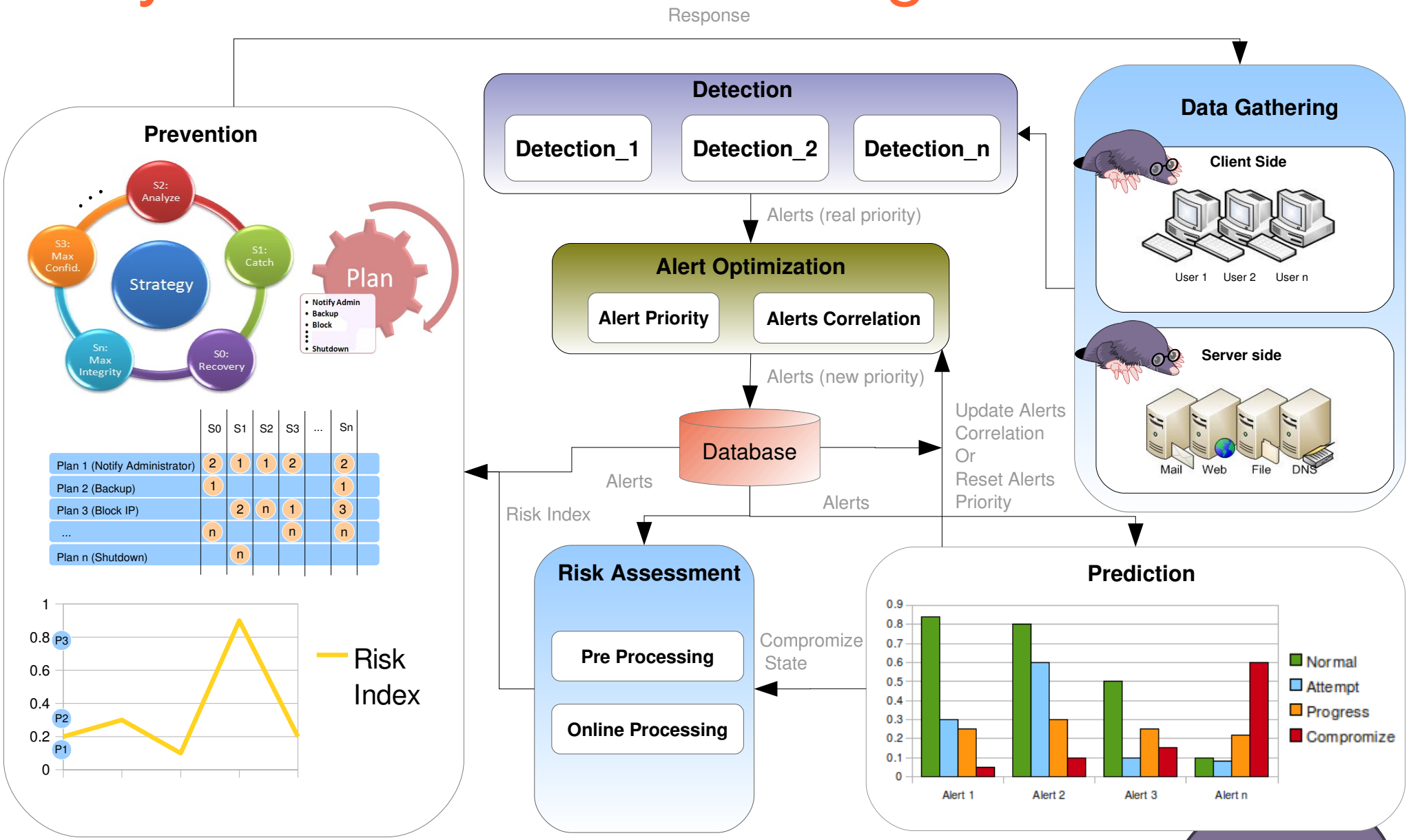
Phase	Name	Alerts
1	IP sweep	No alert is generated for this phase
2	Sadmind Ping	Sadmind_ping
3	Break into	Sadmind_Amslverify_Overflow, Admind
4	Installation	Rsh, MStream_Zombie
5	Launch	Stream_DOS

Prediction Results (7)



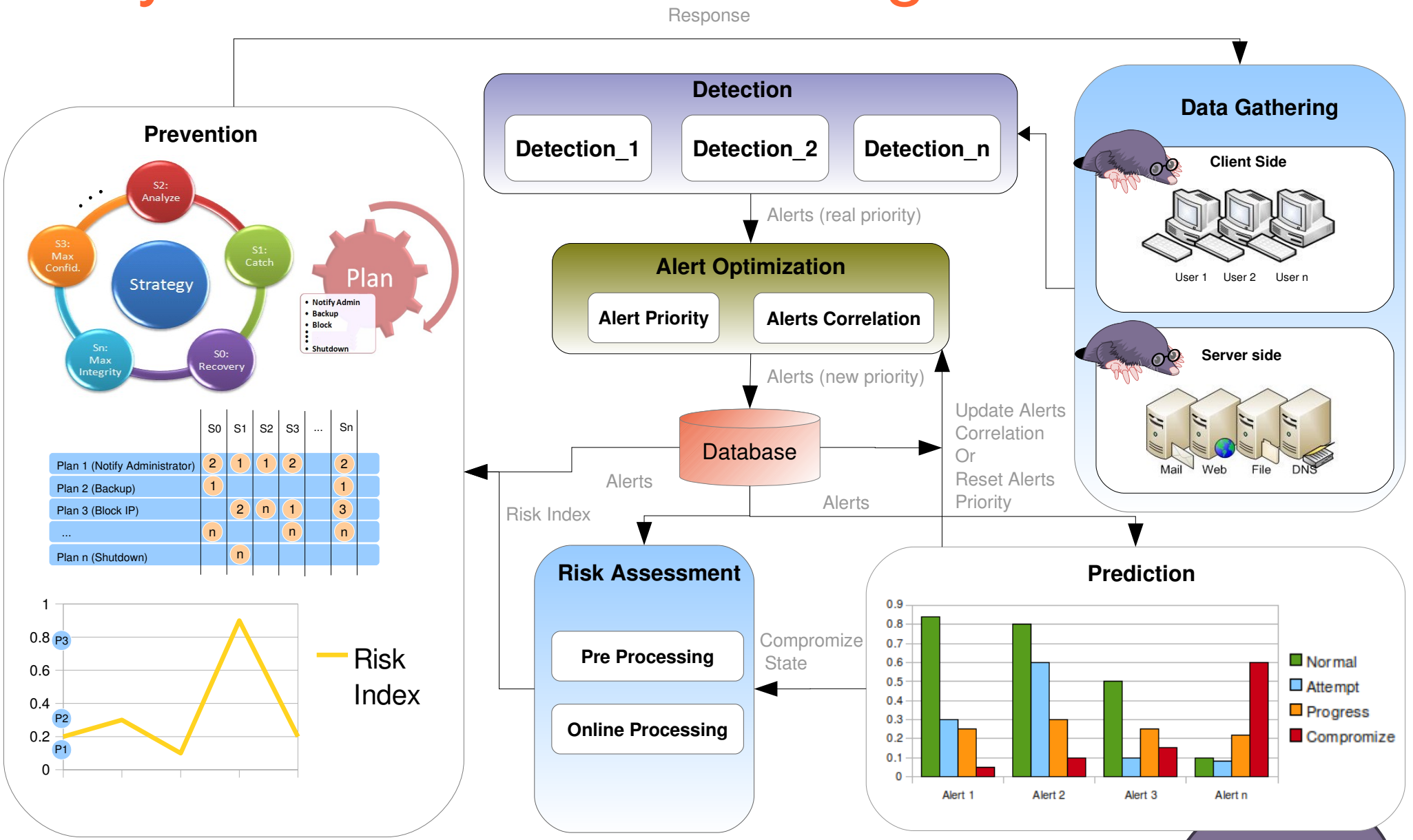
Risk Assessment

System Health Monitoring Architecture



Prevention

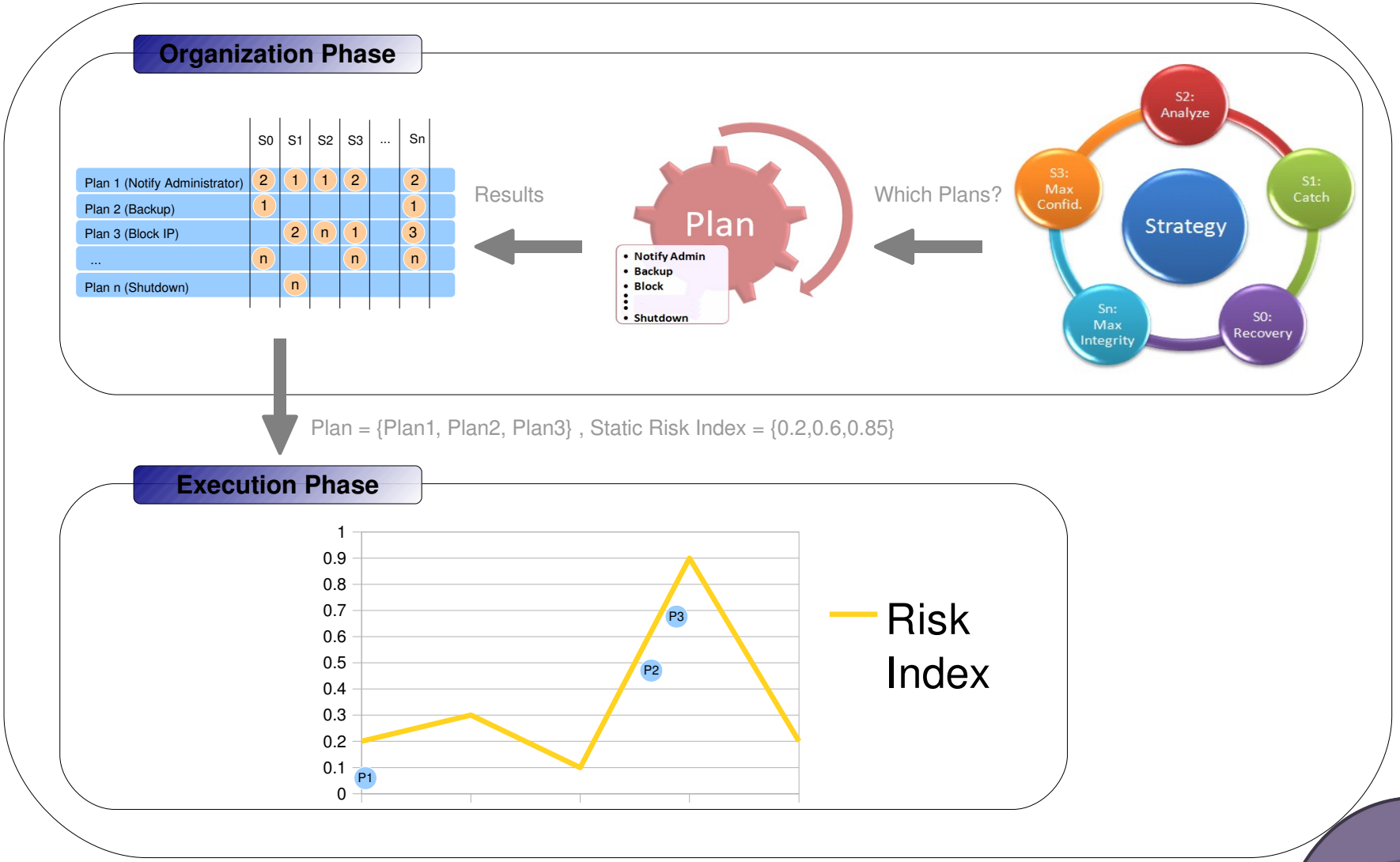
System Health Monitoring Architecture



Prevention

- Prevention component will try to run good strategies for trigger reactive measures with the objective of:
  - Preventing the problem growth
  - Returning system to the healthy mode

Prevention Structure



Prevention - Plan

- IP Blocking
- Dropping Packets
- Killing Process
- Reboot
- Shutdown
- TCP Reset
- Delete files
- Run Virus Check
- Turn off the services
- Applying Patch

- Change All Passwords
- Format the Hard Disk
- ...
-

References (1)

[1] http://en.wikipedia.org/wiki/Anomaly

[2] http://en.wikipedia.org/wiki/Anomaly_detection

[3] Stein G., Bing C., Wu A. S. and Hua K. A., **Decision Tree Classifier For Network Intrusion Detection With GA-based Feature Selection**, Proceedings of the 43rd annual Southeast regional conference, Georgia, ISBN:1-59593-059-0 , pp. 136-141, 2005

[4] http://en.wikipedia.org/wiki/Fuzzy_logic

[5] Yu D and Frincke D, **Improving the quality of alerts and predicting intruder's next goal with Hidden Colored Petri-Net**, Computer Networks, pp. 632–654, 2007

[6] Anuar N. B., Sallehudin H., Gani A. and Zakaria O., **Identifying False Alarm for Network Intrusion Detection System Using Hybrid Data Mining and Decision Tree**, Malaysian Journal of Computer Science, ISSN 0127-9084, pp. 110-115, 2008

[7] Ozyer T., Alhajj R. and Barker K., **Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule pre-screening**, Journal of Network and Computer Applications, SSN:1084-8045, pp. 99-113, 2007

[8] Jin H., Sun J., Chen H. and Han Z., **A Fuzzy Data Mining Based Intrusion Detection Model**, 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, pp. 191-197, 2004

[9] http://en.wikipedia.org/wiki/Neural_network

[10] Xu Q., Pei W., Yang L. and Zhao Q., **An Intrusion Detection Approach Based On Understandable Neural Network Trees** , Journal of Electronics, pp. 574-579, 2007

[11] Bouzida Y. and Cuppens F. , **Neural networks vs. decision trees for intrusion detection**, IEEE / IST Workshop on Monitoring, Germany, September, 2006

References (2)

[12] http://en.wikipedia.org/wiki/Support_vector_machine

[13] Rung-Ching Chen, Kai-Fan Cheng, Ying-Hao Chen, Chia-Fen Hsieh, **Using Rough Set and Support Vector Machine for Network Intrusion Detection System**, First Asian Conference on Intelligent Information and Database Systems, pp. 465-470, 2009

[14] Khan L., Awad M. and Thuraisingham B., **A new intrusion detection system using support vector machines and hierarchical clustering**, ISSN:1066-8888, pp. 507-521, 2007

[15] Liu J. C., Lin C. H., Yu J. L., Lai W. S. and Ho C. H., **Anomaly Detection Using LibSVM Training Tools**, International Journal of Security and Its Applications, Vol.2 , No.4, ISBN: 978-0-7695-3126-7, pp. 166-177, 2008

[16] Zhang R., Zhang S., Muthuraman S. and Jiang J., **One class support vector machine for anomaly detection in the communication network performance data**, Proceedings of the 5th conference on Applied electromagnetics, wireless and optical communications, Spain, ISBN:1790-5117, pp. 31-37, 2007

[17] Abraham A, Jain R., Thomas J. and Han S. Y., **D-SCIDS: Distributed soft computing intrusion detection system**, Journal of Network and Computer Applications, pp. 81–98, 2007

[18] http://en.wikipedia.org/wiki/Bayesian_network

[19] Abdelhamid, **Réseaux Bayésiens Naïfs Augmentés TAN pour les Systèmes de Détection d'Intrusions**, PhD thesis, Université de Nice Sophia Antipolis, 2007

[20] Abouzakhar N., Gani A., Manson G., Abuitbel M. and King D., **Bayesian Learning Networks Approach to Cybercrime Detection**, In proceedings of the 2003 PostGraduate Networking Conference, Liverpool, United Kingdom, 2003

References (3)

[21] http://en.wikipedia.org/wiki/Hidden_Markov_model

[22] Forrest S., Hofmeyr S.A. and Somayaji A., **The Evolution of System-call Monitoring**, Proceedings of the Annual Computer Security Applications Conference, USA, ISBN1063-9527, pp. 418-430, 2008

[23] Forrest S., Hofmeyr S.A., Somayaji A. and Longstaff T.A., **A sense of self for Unix processes**, Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 120–128, 1996

[24] Feng Li, Wang W., Zhu L. and Zhang Y., **Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation**, Journal of Network and Computer Applications, pp. 721-732, 2009

[25] http://en.wikipedia.org/wiki/K-nearest_neighbor_algorithm

[26] Adetunmbi A.O., Falaki S.O., Adewale O.S. and Alese B.K., **Network Intrusion Detection based on Rough Set and k-Nearest Neighbour**, International Journal of Computing and ICT Research, Vol. 2, No. 1, pp. 60 – 66, 2008

[27] Lazarevic A., Ertöz L., Kumar V., Ozgur A., Srivastava J., **A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection**, In Proceedings of the Third SIAM International Conference on Data Mining, 2003

[28] Chandola V., Banerjee A. and Kumar V., **Anomaly Detection: A Survey**, ACM Computing Surveys, Vol. 41(3), 2009

[29] Cherednichenko S., **Outlier Detection in Clustering**, 2005

[30] Wang Q. and Megalooikonomou V., **A Clustering Algorithm for Intrusion Detection,** The SPIE Conference on Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, Florida, vol. 5812, pp. 31–38, 2005

[31] Chandola V., Banerjee A. and Kumar V., **Anomaly Detection: A Survey**, ACM Computing Surveys, Vol. 41(3), 2009

References (4)

[32] Haslum K., Abraham A. and Knapskog S., **DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment**, Third International Symposium on Information Assurance and Security, IEEE Computer Society press, USA, ISBN 0-7695-2876-7, pp. 183-188, 2007

[33] Salfner F. and Malek M., **Using Hidden Semi-Markov Models for Effective Online Failure Prediction**, 26th IEEE International Symposium on Reliable Distributed Systems, pp.161-174, 2007

[34] Feng Li, Wang W., Zhu L. and Zhang Y., **Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation**, Journal of Network and Computer Applications, pp. 721-732, 2009

[35] Mu C. P., Huang H. K. and Tian S. F., **Online risk assessment of intrusion scenarios using D–S evidence theory**, In Proceedings of 13th European symposium on research in computer security a LNCS, Málaga, Spain, ISBN 978-3-540-88312-8 , pp. 35-48, 2008

[36] Mu C. P, and Li Y., **An intrusion response decision-making model based on hierarchical task network planning**, Journal of expert systems with applications, 2009

[37] N. Stakhanova, S. Basu and J. Wong, **Taxonomy of Intrusion Response Systems**, International Journal of Information and Computer Security. Vol. 1. No. 1/2, pp.169-184, Inderscience, 2007

[38] Foo B., Wu Y., Mao Y., Saurabh Bagchi, Spafford E, **ADEPTS: Adaptive Intrusion Response Using Attack Graphs in an E-Commerce Environment**, International Conference on Dependable Systems and Networks, pp. 508-517, 2005

[39] Wu Y. S., Foo B., Mao Y. C., Bagchi S. and Spafford E. H., **Automated adaptive intrusion containment in systems of interacting services**, The International Journal of Computer and Telecommunications Networking, ISSN:1389-1286, Pages 1334-1360, 2007

References (5)

[40] Xiao F., Jin S. and Li X., **A Novel Data Mining-Based Method for Alert Reduction and Analysis**, Journal of Network, vol. 5, pp. 88-97, Jan. 2010

[41] Stakhanova N. and Mell P., **Guide to Intrusion Detection and Prevention Systems,** http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[42] Payne D.B. and Gunhold H.G., **Policy-based security configuration management application to intrusion detection and prevention**, 2009 IEEE International Conference on Communications, Dresden, Germany, 2009

[43] Haslum K., Moe M. E. G. and Knapskog S. J., **Real-time intrusion prevention and security analysis of networks using HMMs**, 33rd IEEE Conference on Local Computer Networks, Montreal, Canada, 2008.

[44] Zhu B. and Ghorbani A. A., **Alert correlation for extracting attack strategies**, International Journal of Network Security, vol. 3, pp. 244-258, 2006.

[45] Kruegel C. , Valeur F. andVigna G., **Alert Correlation**, in Intrusion Detection and Correlation, first edition, vol. 14., Ed. New York: Springer, 2005, pp.29-35.

[46] Curtis A. And Carver J., **Adaptive agent-based intrusion response**, Ph.D thesis, Texas A&M University, USA, 2001.

Thank you