

## Unlock the value of your cybersecurity investment

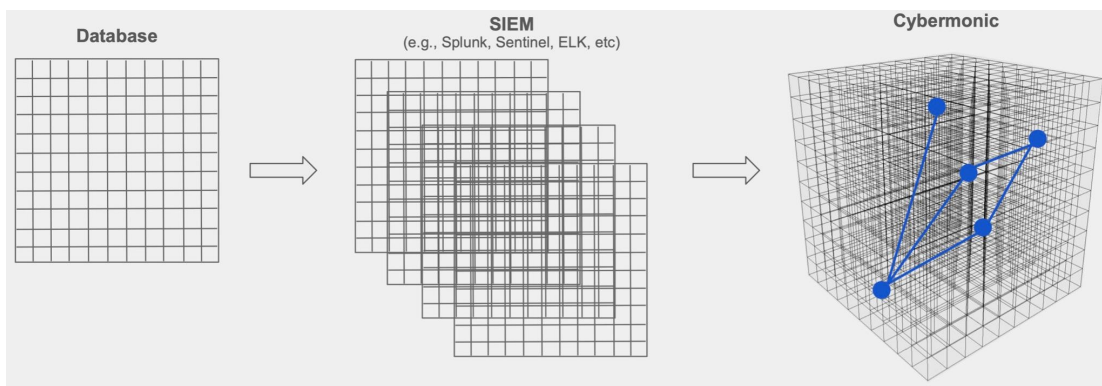
Cybermonic is an early-stage startup providing AI software for enterprise cybersecurity management. Its proprietary graph AI technology based on machine learning on graph data structures helps organizations make sense of the connected nature of their cybersecurity tools and data, ultimately supporting more efficient, more effective decision making.

### Under-staffed and Overworked Cybersecurity Teams

Close to half of cybersecurity incident responders have experienced burnout or extreme stress during the last year<sup>1</sup>. Organizations desperately need new technology that can automatically ingest and correlate many cyber data sources in their environments, and provide actionable insights that improve the effectiveness of their Security Operations Center (SOC) teams.

### Cybermonic Difference


Cybermonic’s innovative graph algorithmic approach to automatic correlation and contextualization is faster, more accurate, more flexible, and more cost-effective than existing solutions.



<sup>1</sup> ZDNet. [Your cybersecurity staff are burned out](#). August 2022.

- Provide comprehensive and automatic visibility across all cyber data
- Automatically break the barriers of siloed data within individual logs and data sources
- Graph AI provides instant and automatic correlation and analysis across all data sources for actionable knowledge

## Rule-based vs. Graph-based Cyber Analysis

<pre> Logs   filter ActivityId == "ActivityId with Blablabla"   summarize max(Timestamp), min(Timestamp)   extend Duration = max_Timestamp - min_Timestamp  wabbitrace   filter Timestamp &gt;= datetime(2015-01-12 11:00:00Z)   filter Timestamp &lt; datetime(2015-01-12 13:00:00Z)   filter EventText Like "NotifyHadoopApplicationJobPerformanceCounters"   extend Tenant = extract("tenantName{[*,]},", 1, EventText)   extend Environment = extract("environmentName{[*,]},", 1, EventText)   extend UnitOfWorkId = extract("unitOfWorkId{[*,]},", 1, EventText)   extend TotalLaunchedMaps = extract("totalLaunchedMaps{[*,]},", 1, EventText)   extend MapsSeconds = extract("mapMilliSeconds{[*,]},", 1, EventText, type=double)   extend TotalMapsSeconds = MapsSeconds / TotalLaunchedMaps   filter Tenant == 'Dev01' and Environment == 'HadoopDev2'   filter TotalLaunchedMaps &gt; 0   summarize sum(TotalMapsSeconds) by UnitOfWorkId   extend JobMapsSeconds = sum_TotalMapsSeconds * 1   project UnitOfWorkId, JobMapsSeconds   join wabbitrace   filter Timestamp &gt;= datetime(2015-01-12 11:00:00Z)   filter Timestamp &lt; datetime(2015-01-12 13:00:00Z)   filter EventText Like "NotifyHadoopApplicationJobPerformanceCounters"   extend Tenant = extract("tenantName{[*,]},", 1, EventText)   extend Environment = extract("environmentName{[*,]},", 1, EventText)   extend UnitOfWorkId = extract("unitOfWorkId{[*,]},", 1, EventText)   extend TotalLaunchedReducers = extract("totalLaunchedReducers{[*,]},", 1, EventText)   extend ReducesSeconds = extract("reduceMilliSeconds{[*,]},", 1, EventText, type=double)   extend TotalReducesSeconds = ReducesSeconds / TotalLaunchedReducers   filter Tenant == 'Dev01' and Environment == 'HadoopDev2'   filter TotalLaunchedReducers &gt; 0   summarize sum(TotalReducesSeconds) by UnitOfWorkId   extend JobReducesSeconds = sum_TotalReducesSeconds * 1   project UnitOfWorkId, JobReducesSeconds   join wabbitrace   filter Timestamp &gt;= datetime(2015-01-12 11:00:00Z)   filter Timestamp &lt; datetime(2015-01-12 13:00:00Z)   filter EventText Like "NotifyHadoopApplicationJobPerformanceCounters"   extend Tenant = extract("tenantName{[*,]},", 1, EventText) </pre>	<h3>Rule-based</h3> <ul style="list-style-type: none"> <li>• Good at detecting individual events, bad at telling whole story</li> <li>• Requires writing query scripts that are complex and brittle</li> </ul>	
	<h3>Graph-based</h3> <ul style="list-style-type: none"> <li>• No writing queries</li> <li>• Complete correlation across all sources</li> </ul>	

## Design partner program

The Cybermonic system delivers 10x-20x speedup in threat analysis, and 95% alert reduction via correlation, deduplication, and prioritization compared to other commercially available tools, allowing the analysts to focus on the most critical events in the network.

We are accepting applications for new design partners who are forward thinkers interested in accessing Cybermonic’s cutting-edge technology and shaping the future of cyber defense. If you are interested in a low level of effort pilot project, with no cost to you, please contact [info@cybermonic.com](mailto:info@cybermonic.com) for more information.