





THREAT HUNTING PROGRAM MATURITY MODEL

	LEVEL 0 INITIAL	LEVEL 1 REACTIVE	LEVEL 2 DEFINED	LEVEL 3 REPEATABLE	LEVEL 4 INTEGRATED	LEVEL 5 OPTIMIZED
<div>Talent</div> <div></div>	<ul style="list-style-type: none"><li>▶ A career development path does not exist or is informal.</li><li>▶ A hunter training program does not exist or is informal</li></ul>	<ul style="list-style-type: none"><li>▶ A career development path is informally documented for all associate levels.</li><li>▶ Available training programs are documented.</li><li>▶ Role descriptions and expectations are documented and communicated.</li></ul>	<ul style="list-style-type: none"><li>▶ A career development path is formalized, documented, and communicated for all associate levels.</li><li>▶ A formal recruiting plan is in place.</li></ul>	<ul style="list-style-type: none"><li>▶ A formalized career development path is executed upon consistently.</li><li>▶ A formalized training program for all levels is established and its completion tracked.</li><li>▶ Compensation correlates to documented performance management expectations and contributions.</li></ul>	<ul style="list-style-type: none"><li>▶ Target metrics on workforce efficiency and effectiveness are identified and measurements are in place for actual results.</li><li>▶ A formal succession plan is in place.</li></ul>	<ul style="list-style-type: none"><li>▶ Key workforce targets are reached consistently for all areas.</li><li>▶ Workforce measurements are re-evaluated and validated continuously.</li></ul>
<div>Data</div> <div></div>	<ul style="list-style-type: none"><li>▶ Visibility of hunting data sources is unknown.</li><li>▶ Quality of hunting data sources is unknown.</li></ul>	<ul style="list-style-type: none"><li>▶ Visibility and quality of hunting data sources is partially understood.</li><li>▶ Hunting data sources are informally documented.</li><li>▶ Collection tools passively collect data.</li></ul>	<ul style="list-style-type: none"><li>▶ Visibility and quality of hunting data sources is informally measured.</li><li>▶ All available hunting data sources are formally documented.</li><li>▶ Collection tools permit active data collection.</li></ul>	<ul style="list-style-type: none"><li>▶ Visibility and quality measurements for hunting data sources are in place for actual results.</li><li>▶ Automated data collection is executed consistently.</li><li>▶ Hunting techniques inconsistently include data science.</li></ul>	<ul style="list-style-type: none"><li>▶ Hunting data sources provide &gt;90% visibility for all enterprise defined critical assets.</li><li>▶ Hunting techniques consistently include data science.</li><li>▶ A standard for enterprise wide logging is documented and socialized.</li></ul>	<ul style="list-style-type: none"><li>▶ Hunting data sources provide &gt;80% visibility for enterprise across network and endpoint.</li><li>▶ Normalization and standardization of hunting data sources is fully automated.</li><li>▶ All hunt operations include data science techniques.</li></ul>
<div>Methodology</div> <div></div>	<ul style="list-style-type: none"><li>▶ A hunting framework does not exist or is informal.</li><li>▶ Hunt operations do not exist in a central capacity.</li></ul>	<ul style="list-style-type: none"><li>▶ A hunting framework is informally documented.</li><li>▶ Hunt operations are informally executed when incident response activity is minimal.</li></ul>	<ul style="list-style-type: none"><li>▶ A hunting framework is formalized and communicated.</li><li>▶ Hunt analytics are formalized and documented.</li><li>▶ Fully centralized hunt operations continue regardless of incident response activities.</li></ul>	<ul style="list-style-type: none"><li>▶ A formalized hunting framework is executed upon consistently.</li><li>▶ Hunt outcomes are consistently documented.</li></ul>	<ul style="list-style-type: none"><li>▶ Newly developed hunt analytics are shared with the threat hunting community.</li><li>▶ Hunt outcomes are consistently socialized with and acted upon by impacted stakeholders.</li></ul>	<ul style="list-style-type: none"><li>▶ Threat hunting framework is re-evaluated and validated continuously.</li><li>▶ Stakeholder feedback validates that the hunt outcomes meet or exceed stakeholder expectations.</li></ul>
<div>Metrics</div> <div></div>	<ul style="list-style-type: none"><li>▶ Few or no metrics are identified, tracked, or reported.</li></ul>	<ul style="list-style-type: none"><li>▶ Key metrics are identified and measurement elements are accurate.</li><li>▶ Key metrics are reported on an ad hoc basis.</li></ul>	<ul style="list-style-type: none"><li>▶ Measurement of actual performance to target metrics is accurate and communicated to management and associates.</li></ul>	<ul style="list-style-type: none"><li>▶ Metrics are formally tracked and reported to management on a consistent schedule.</li></ul>	<ul style="list-style-type: none"><li>▶ Improvements are prioritized for areas where performance is not meeting target goals.</li><li>▶ Hunt outcomes included in risk assessments.</li></ul>	<ul style="list-style-type: none"><li>▶ Key metric targets are reached consistently for all areas.</li><li>▶ Actual performance metric calculations are fully automated.</li></ul>