OTHF Strategy

# Maturity Models

The Open Group information security management maturity model (O-ISM3) describes a maturity as the measurement of an organization’s ability implement continuous improvement practices within a particular discipline. With a focus on continuous improvement, maturity models are well suited for assessing threat hunting operations.

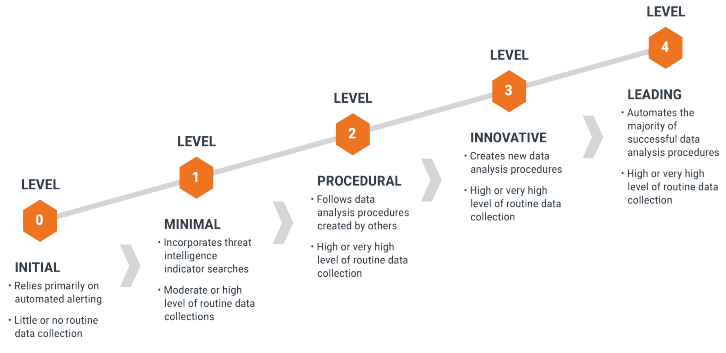
Why maturity models are important for threat hunt teams:

* Benchmarking – Determine where the threat hunt team is in terms of current state and compare against goals and objectives for performance improvement.
* Performance Improvement – With a model a threat hunt team can directly track their operations against the best practices defined by the model. Maturity models can help organizations identify gaps which a plan that addresses specific issues.
* Unified improvement language – Implementing a maturity model ensures that the entire threat hunting organization is aligned on future goals and using the same language to discuss capabilities that would enable the organization to increase their maturity with respect to the model.

The SQRRL “A Framework for Cyber Threat Hunting”[[1]](#footnote-1) white paper is one of the most important papers released to the world of threat hunting and serves as a foundational part of the OTHF. Within SQRRL’s works, they introduce the concept of threat hunting specific maturity model and a set of criteria in which a threat hunting program can be evaluated against.

Through the introduction of a maturity model, SQRRL created a way for threat hunt teams to build short-, medium-, and long-term goals through some high-level characteristics associated with the varying levels of maturity. Depending on the organization, they may want to have more specific requirements and assessment criteria laid out within the model and so the OTHF has created a maturity model that organizations can use to assess their maturity against.

## SQRRL Maturity Model



SQRRL Hunting Maturity Model

Full details of the SQRRL Maturity Model can be found in the whitepaper: <https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf>

## OTHF Maturity Model

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LEVEL 0  Ad Hoc | LEVEL 1  Foundational | LEVEL 2  Functional | LEVEL 3  Effective | LEVEL 4  Optimal |
| - A process is not defined and has no standardized process - Relies primarily on automated alerting. Little or no routine data collection | - A process area is loosely defined - Capabilities are based mainly on tribal knowledge and are not aligned to industry standards  - A process area lacks standardized process documentation Leverage threat intelligence to retrospectively search data sets for IOCs. Ad-hoc data searches for adversary tools (tribal knowledge) | - A process area is formally defined with supporting capabilities  -A standardized and documented process supports Capabilities  - Leveraged MITRE ATT&CK to drive change towards platforms that support real-time and metadata collections at scale. | - A process area is formally defined with supporting capabilities  -Capabilities are supported by a well-defined, standardized, and documented process.  - Formal procedures are defined for common tasks  - Incorporation of a detection framework and threat hunting development loop. Threat hunting is a driver for automated detection. Threat hunts are executed as part of a detection framework where successful hypothesis-based hunts are executed and then transitioned into automated detections. | - A process area is formally defined with supporting capabilities  - Capabilities are supported by a well-defined, standardized, and documented process.  - Formal procedures are defined for common tasks  - Centralized data and platform leveraging standardized data sources and structure supporting an intelligence-driven threat hunting framework. Strategic threat assessments provide tactical intelligence that drives the threat hunting development lifecycle.  - Processes are measured, automated, and continuously improved |

### Assessment Criteria

This section outlines the assessment criteria for each process area in scope

Subcategories Criteria

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **LEVEL 0** | **LEVEL 1** | **LEVEL 2** | **LEVEL 3** | **LEVEL4** |
| **PEOPLE** | - A threat hunting role does not exist or is informal - A skills catalog does not exist. No hunter training program is available | A threat hunting team exists but role description and expectations are informal documented and communicated.  - A rudimentary skills catalog exists, with no defined criteria, requirements, or a plan. No hunter training program is available. | A threat hunting team exists with dedicated roles and expectations are formally documented and communicated.  - A functional skills catalog exists, with defined criteria, requirements, or a plan. However, the skillset is assessed by the TH program leadership on an ad hoc basis.  There is no formalized plan for addressing gaps. No hunter training program a | - A effective skills catalog exists, with defined criteria, requirements, or a plan. However, skillset is assessed by the TH program leadership on a ad hoc basis. Criteria and requirements are defined, and a formalized mentoring program is in place for bridging the skills gaps  - A formalized training program is established for all levels of hunters.  - A formal recruiting plan is in place. | - A robust skills catalogue exists, with a defined criteria, requirements, or a plan. However skillset is assessed by the TH program leadership as well as through self-assessment on a regular basis. Criteria and requirements are well defined, and a formalized mentoring program is in place for bridging the skills gaps.  -A cross training program is in place for inter-departmental training  - A formal recruiting plan is in place. |
| **PROCESS** | - A hunting framework does not exist or is in its infancy  - Threat hunting does not exist | - A hunting framework is informally documented - Threat hunting is mainly a reactive service when incident response activity arises - The process area covers less than 50% of the organization | - A hunting framework is formalized and documented  - Threat hunting is proactively continued regardless of incident response activities  - No automated detection framework in place.  - The process area covers 50% to 75% of the organization | - A formalized hunting framework is regularly executed. Outcomes are consistently discussed with impacted stakeholders.  - A Threat Hunting mission statement has not been defined.  - Hunts are constantly documented and reviewed with the ability to be turned into automated detection  - The process area covers 75% to 90% of the organization | - The threat hunting frameworks is regularly reviewed and validated for efficiency. - A clear Threat Hunting mission statement has been defined and understood by the team.  - Stakeholder feedback validates that the hunt outcome meets or exceeds expectations.  - Newly developed are shared with the threat hunting community.  - Hunts are constantly documented and reviewed and turned into automated detection  - The process area covers 90% to 100% of the organization |
| **DATA SOURCE** | - Visibility on data sources is unknown  - Quality of data sources is unknown - No tools or processes to passively collect data | - Visibility on data sources is partially understood  - Data sources are informally documented - Tools are present to passively collect data  - The data sources covers less than 50% of the organization | - Visibility and quality of data sources are informally measured  - Available hunting data sources are formally documented  - Collection tools are part of the threat hunt program too actively collect data  - The data sources covers 50% to 75% of the organization | - Visibility and quality on data sources is formally measured and in place  - Data collection is executed consistently  - Hunting techniques include data science  - The data sources covers 75% to 90% of the organization including critical assets | - A standard exists for enterprise wide logging and documentation  - Standardization of hunting data sources is fully automated  - Hunt operations include data science techniques  - The data sources cover 90% to 100% of the organization across network and endpoint. |
| **THREAT INTEL** | - Threat intelligence is not a function within the organization or is still in its infancy  - Threat intelligence is never or rarely collected  - No CTI technology  - No technology integration or Data is raw and unformatted. | - Threat intelligence sharing is reported on an ad hoc basis. Expectations are informal documented and communicated.  - Threat intelligence scope is global and org specific  - Threat Intelligence platform exists with updated feeds  - Technology Integration: SIEM, Firewall/Proxy, or IDS/IPS | - Threat intelligence sharing is a separate function within the organization and expectations are formally documented and communicated.  -Threat intelligence scope is global, org specific, and industry specific.  -Teams take external and internal data input to shift from a reactive to a proactive posture.  - Threat intelligence platform exists alongside an IOC tool  - Technology Integration: TIP, SIEM, Firewall/Proxy, or IDS/IPS is being integrated within threat intel | - Threat intelligence sharing is a separate function within the organization and expectations are formally documented and communicated.  - Region-specific, global, industry-specific, org specific  - Contributors and members of organizations such as Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs)   - Automation of some threat intelligence analysis tasks  - Technology Integration: TIP, SIEM, defensive tools, incident response system, and all security data is being integrated within threat intel  - Supports IR engagements based on knowledge of the adversaries involved | - Threat Intelligence is a key function that allows the business to make operationally and strategically aligned decisions. - Create tactical an strategic TI - Team has the capability to build custom applications and processes  - Majority of TI is automated  - Advanced analytics and orchestration capabilities - Region-specific, global, industry-specific, org specific  - Contributors and members of organizations such as Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs)  - A sophisticated threat intelligence platform exists that allows the team to build out a SOAPA |
| **METRICS** | - Few or no metrics are identified, tracked, or reported | - Key metrics are reported on an ad hoc basis  - Key metrics are identified and measurement elements are accurate | - Performance targets such as operational metrics and key performance indicators is accurate and communicated to management | - Metrics are formally tracked and reviewed. Output is communicated and reported to management on a regular schedule.  - Improvements are discussed but not a critical priority | - Improvements are prioritized for areas where performance is not meeting target goals.  - Operational metrics are updated in real-time via automation  - Hunt outcomes included in risk assessments |

1. https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf [↑](#footnote-ref-1)