Threat Landscape Design

This landscape design is heavily inspired and borrowed from [ENISA Threat Landscape Methodology — ENISA (europa.eu)](https://urldefense.com/v3/__https:/www.enisa.europa.eu/publications/enisa-threat-landscape-methodology__;!!LgPfcEISpGU!ur07-xa2YjEASBsVFGLzwkPiBoe3axZ5m0693rLW35_MHj5mh78tovlAy7yuQ9NAXaB9$) – the author **highly** recommends reviewing this resource. In the Annex of this document includes *multiple*templates, while only the generic template from ENISA is referenced here.

This document also references heavily the *Company Baseball Card*which is recommended tocomplete **before** the threat landscape**.**

**Overview:**

With all intelligence products, your scope, audience and objectives should be clearly identified and documented before starting the threat landscape process. These elements should be shared with all analysts that are participating in the threat landscape design and reporting to ensure consistency in the approach and final product.

This document is supposed to provide a general overview of the options and approaches that could be taken from a generic level. You *must* customize this for your organization and audience.

**General insights you hope to gain or report on from this data:**

* How does your company’s level of threat pressure compare to industry average? Are you getting more MFA attacks? More credential phishing? Why might that be and how can you reduce the risk?
* Is there an increase in risk due to an increase in the **volume** of activity or the **impact** of the activity?
* Which threat actor goals (financial, hacktivism) and targeting methods (CVEs, applications, specific job titles, geolocation) are likely to align with the way we do business?
* How easy is it to discover that we do business in a way that is attractive to those threat actors? (media coverage, job descriptions, OSINT, etc) Has that changed over time?
* How does the sophistication and resource level of threat actors whose goals may align with the way value or money moves through our organization? Do you have low sophistication ecrime actors trying to get gift cards, or highly motivated nation-state backed espionage groups using sophisticated bribing and blackmail techniques to get source code?
* What are the threat pressures against our third-party relationships critical to our ability as a company to execute on value creation?

**Driving principles:**

* Does each part of your threat landscape clearly communicate the “So what does it matter to [organization]?” clearly?
* Does your threat landscape provide clear observations, predictions from those observations and recommendations which are actionable? Have you asked for each landscape element “Ok, so what do we do about it?”
* Accurate and analytical – multiple sources where possible, ensure that analytical writing standards for level of confidence statements are standardized and followed across the landscape report

**Purpose:**

* Strategic decision-making
* Risk management
* Policy making
* Prioritizing policy recommendations
* Prioritizing security and risk spend
* Identifying opportunities for training, exercises and capacity building

**Connected to Intelligence Requirements:**

Your Threat Landscape should, where possible, reference the intelligence requirements (IRs) or priority intelligence requirements (PIRs) it is intended to address. Some examples of intelligence requirements that are often addressed in a threat landscape are:

* What is the trend of ransomware campaigns over the last 12 months?
* What campaigns specifically targeted entities similar to our vertical and operating geolocations?
* What changes in tactics and techniques are being used in those campaigns? How do they compare with our security controls in those areas?

**Company Baseball Card for Relevance:**

Using the *Company Baseball Card* to make powerful, relevant observations in your threat landscape. Typically this is used as a brainstorming session for the strategic summary and recommendations slide.

|  |  |  |
| --- | --- | --- |
| **Company Insight** | **Threat Activity Data** | **Insights and Observations for analysis** |
| Type of Data mapped to Crown Jewel applications | Vulnerability Exploitation targeting applications that house critical data | Rate of vulnerability disclosure and exploitation for key systems |
| Asset management and vulnerability data | CVEs targeted in attack patterns for events that resulted in breaches | Breaches at other organizations originating from |
| Company locations | Country and Region Cyber Threat Scores (Mandiant as an example)  Regional trends in attack patterns or malware | Increase or decreasing attacks in some locations  Known regional targeting by threat actors aligned with operated business locations |
| Third-party relationships | Categorization of third-party by industry  Threat activity by industry  Third-party incidents over time (increase or decrease)  Type of third-party compromise (zero-day, social engineering, supply chain) and type of event (ransomware, data leak, supply chain) | Which third-party relationships are increasingly at risk because of increased targeting or attacks  Which third-party relationships had a breach or attack last year? What was the impact?  How are the third-parties being compromised? Does that translate into unique risk for our organization? |
| Methods of access | Targeting of VPN, RFP, MFT, services  Exploitations or breaches a result of targeting those technologies | Services or servers under increased risk of attack, which may need more aggressive patching / monitoring / security controls |
| Methods of authentication | Targeting of MFA or federated identify services (Oauth, SAML, etc)  Targeting of service desk / help desk for social engineering  Exploitations or breaches a result of targeting those technologies | Services or servers under increased risk of attack, which may need more aggressive patching / monitoring / security controls or change in type of implementation |
| Products critical to the organization’s success | Exploitations or breaches a result of targeting those technologies  Breaches or attacks on those companies  Trending of activity against those products (increasing threat pressure? More password spraying? More injection attempts? Less? Tied to specific times of year or events?)  What policy exceptions to any of those products have? | Increasing threat actor interest in products critical to success  Type of attacks seen and predicted against those critical products  Any security exceptions that should be reviewed? |
| Brands | Level of brand impersonation attempts  Types of brand impersonation attempts by type and goal | Brand impersonation trending up or down  Which brands and what goals (fraud aimed at employees, fraud aimed at customers, procurement fraud, SEO manipulation, cred harvesting, etc)? |
| Major lines of business categorized by vertical | Comparing threat pressure observed against industry average | Compare the amount of phishing attacks, exploitation attempts (WAF and Firewall) and malware executions against industry averages – is our organization getting more or less of these than our peers? |
| Geopolitical or social statements or stances made by the company | Threat actors’ types that are relevant to these positions (right wing extremists, abortion rights hacktivists, animal rights hacktivists, etc) and the level of activity of these actor groups | Recent statements and the threat actors/hacktivist groups that may react to them  Any increase / decrease of threat activity observed at the time |
| Describe how the value chain moves through the company | Fraud schemes that target certain processes where money is transferred or paid  Targeting of individuals based on role and access type to the value chain, such as accounts payable personnel.  Identification of key IP that maybe of interest to certain nation states | Relevant threat actor campaigns targeting similar value chains  Attack patterns associated with attacking similar value chains  Which roles / employees at most risk of being targeted  What IP/data is in those value chains that maybe of interest to nation-state actors, what security controls are around that data in comparison to those actors TTPs |
| What do we look like to attackers? What does OSINT on ourselves show? | What attack surface is easily known to actors?  What vulnerabilities are easy to identify on that attack surface?  What information about products, technology, and third-party relationships can be easily found? (social media, job postings, etc)  Any notable sentiment or trending topics on the company?  Who is discoverable through OSINT appears to be in roles that are targeted for phishing? (example has “administrator” in title and works in technology role, has “procure” or “procurement” in the title, etc) |  |
| Malware detection results | Malware trends | Are we seeing increased detection results that align with malware trends? For example if Qakbot is reported to be increasing overall for the past two months, but Qakbot detection have decreased, that may mean detection engineering needs to review malware variant testing, or that our org is actually targeted more often by a different malware  Are we seeing increase or decrease in some malware detections over time? |
|  |  |  |

**Generic Threat Landscape Structure (ENISA)**

* **Cover Page:** title, reporting period, publication date, TLP and reference or DOI)
* **About** the organization
* **Objective(s) of the report:** what's within the scope of the report, its objectives and the target audience
* **Methodology and approach:** the methodology used to produce the report, including information about the datasets such as the different types and amounts. Stakeholders that contributed information can be named.
* **Acronyms and glossary**
* **Table of contents**
* **Executive summary:** the overall risk-based understanding of the threat horizon, including forecasts, assessments, key takeaways, top insights, most important observations or findings and trends.
* **The sector (if applicable)**
  + Identification of the sector (an explanation or description of the industry sector).
  + The specificity of the sector (presenting the different stakeholder groups, critical functions or assets pertinent to the industry sector). For each category, a mini (or full) threat landscape can be provided.
    - It is most common for a report on the threat landscape of an industry sector to present overviews of the different threat landscapes pertinent to stakeholder or critical function groups. Those can be perceived as mini threat landscapes within the main threat landscape report and include content similar to the ones provided in executive summaries, identification of relevant adversaries and their characteristics (e.g. motivations and capabilities), noteworthy incidents and attack vectors.
    - A threat matrix can be populated that describes the risk an adversary poses to the critical function or stakeholder. Such an approach translates directly to the tactics, techniques and procedures used in attacks.
* **Threat actor categories or types**
  + The status of activity [regarding cybercrime, nation-state threats, insiders, hacktivists, etc.] over the reporting period for a particular industry sector
  + Information about the characteristics of a threat actor category or type such as motivations, capability and objectives.
  + Trends and most noteworthy incidents (briefly). From a strategic point of view, to emphasize the importance of the incidents, the report can describe the impact in terms of financial losses, downtimes and number of affected stakeholders. From a tactical perspective, the important characteristics of an attack can be described briefly.
  + From a tactical point of view, ATT&CK heatmaps or ATT&CK lists for each actor type can be included to indicate the most common TTPs targeting the sector.
* **Threat groups or activity groups** 
  + An overview of adversaries that target the sector.
  + Details on groups that have been observed to be active in the reporting period.
    - The groups need to either target the sector directly or, if they are opportunistic, it should have been assessed that their operations will affect entities and stakeholders or functions within the industry sector.
    - Categorization is possible based on actor types and motivations.
  + Significant incidents can be described.
  + From a tactical perspective, ATT&CK heatmaps or ATT&CK lists or tables for each adversary group can be included to indicate their most common TTPs.
  + Mitigations when possible (for example when an activity group corresponds to a particular malware) can be provided for more technical audiences.
* **Cyberthreats** 
  + Describe cyberthreats relevant to the sector, including trends, attack vectors and recommended (high-level) mitigations pertinent to the threat.
  + For each threat, major incidents can be described concisely (a tabular format can be used).
  + From a tactical (more technical) perspective, ATT&CK heatmaps or ATT&CK lists or tables for each cyberthreat can be included to indicate most common TTPs.
* **Defensive recommendations** 
  + Due to the unique technological environments of the sectors and their critical functions and stakeholders, the report can provide and describe best practices for defense.
* **Appendices:** information that may not need to be part of the main document, such as details for technical audiences.
  + List of sector incidents with references
  + TTPs - (e.g. the MITRE ATT&CK® Framework could be used)
  + Commonly used tools
  + CVE weaponization

While I do use the above format, except each section *always* contains a slide or a “one-pager” that has a summary of the content formatted to be:

* Observations
* Predictions
* Recommendations

This is a repeatable “take away” section for your leadership to specifically look at for a quick summary of what they may want to assign for action or follow up.

Here is an example of how this content may look:

**Observation(s):**

* [Organization] is targeted by credential theft attempts more that healthcare and pharmaceutical industry average per Proofpoint TAP
* Credential theft attempts are trending upwards for the past two quarters per Proofpoint TAP
* Cloud-conscious threat actors are focused on obtaining credentials for administrators (Mandiant, Crowdstrike, HHS)
* "Cloud Services" is one of the top departments that receive malicious emails in their inboxes per Proofpoint TAP
* Credential phishing continued to inboxes through attachments is a low-priority Proofpoint alert for the SOC

**Prediction(s):**

[Organization] is experiencing an increased threat pressure focused on credential theft, using campaigns which are using sophisticated enough campaigns to make it past or security controls and target cloud technology administrators. While a significant portion are blocked by Proofpoint TAP security controls, there are campaigns which are being delivered to user's inboxes observed in the past quarter. [Organization] playbooks for SOC response currently have these delivered emails with malicious attachments for credential phishing at an extremely low priority for investigation, which increases the time possible for a user to be successfully attacked before malicious emails are removed. This represents an increased risk to [Organization] which is likely to continue to increase over time. Moderate confidence of an exposure of cloud administrative credentials within the next year if not mitigated.

**Recommendation(s):**

* Consider targeting the Cloud Services team for enhanced security training regarding phishing, MFA fatigue, MFA bombing, SIM swamping protection
* Evaluate the cloud administrators and digital workplace platform services team’s email security rules for potential improvements
* Add additional playbooks for investigating phishing email attachments which have been continued to user’s inboxes

A generic powerpoint template called THREAT LANDSCAPE PRESO TEMPLATE is also provided. I recommend, where possible, to encourage your stakeholders to move away from powerpoints as their means of intelligence reporting and to word documents for better readability, but this is not always possible.