Traffic Light Protocol (TLP)

Sharing intelligence with other organisations can be extremely beneficial, from building the organisation's reputation to preventing supply chain attacks, but at the same time we don't want to go around disclosing that an attack has taken place in some circumstances. Traffic Light Protocol, shortened to TLP, is a way of classifying information for sharing and is commonly used for security reports and threat intelligence. We'll go through a few examples, but first let's cover the history of TLP and introduce you to the different classifications.

WHAT IS THE TLP?

The **Traffic Light Protocol** was originally created in the early 2000s by the UK Government's National Infrastructure Security Coordination Centre to promote greater sharing of sensitive information. While not originally designed specifically for cybersecurity, our industry has widely adopted this approach for sharing sensitive information relating to cyber attacks and internal documentation.

The purpose of TLP is to allow the author of the original information to state how they want their information to be circulated, such as sharing only with specific individuals, within an organisation, within trusted communities, or in the public domain. It is extremely important that if you ever receive a document that uses the TLP system that you do not breach the intended level of distribution, as the entire protocol relies on trust.

TLP: WHITE

Information that is classed as TLP WHITE can be publicly shared, but copyright rules still apply. Reports or updates that use this TLP are distributed freely for the good of everyone.

Example:

The US Cybersecurity and Infrastructure Security Agency (CISA) shares a number of TLP:WHITE analysis reports on malware, and freely shared the related indicators of compromise. Other organisations offer the ability for anyone to subscribe to an email listing that will send out security updates and reports which can be freely shared. We suggest students take a look at a couple of the CISA analysis reports, they're awesome! – https://us-cert.cisa.gov/ncas/analysis-reports

TLP: GREEN

TLP: GREEN

Information that is classed as TLP GREEN may be sharing within communities, such as information sharing and analysis centres (ISACs), which are groups of organisations operating in the same industry or industries. This information should not be shared outside of the intended communities, such as posting it publicly on the internet.

Example

'Organisation A' operates in the aviation industry and forms an ISAC with four other companies who all operate in aviation too. One day Org A is subject to a cyber attack from APT33, an Iranian-based threat actor that has been known to target this sector. During the incident response process Org A collects a number of indicators of compromise (IoCs) such as the email address that sent a spear phishing email, hashes of malicious files, IP addresses used for command-and-control communication, and so on. Org A has the choice to disclose the IOCs ISAC member organisations to help other companies defend themselves from the same threat actor, but this means these companies (which may be competitors in the business space) will know Org A has been the victim of a successful cyber attack (which could damage reputation, projected sales, stock price, etc if it is leaked to the public).

TLP: AMBER

Information that is classed as TLP AMBER may only be shared internally within an organisation on a need-to-know basis to limit who has access to the information.

Example

Penetration test reports, red team engagement report, and vulnerability scan results are likely to be TLP AMBER as they contain information about serious security flaws that can be exploited to achieve certain actions. Only specific individuals within the organisation would need to see these documents, and if they were publicly disclosed there is the chance that malicious actors will find these sensitive reports and could use them to launch effective cyber attacks against the organisation, because they now have detailed information about the systems, network layout, and vulnerabilities present within that company.

TLP: RED

Information that is classed as TLP RED is **extremely** sensitive and could have severe consequences if it falls into the wrong hands. If an online or in-person meeting is classed as TLP RED then the information should not be shared with anyone that isn't present in the meeting. Regarding electronic communication such as emails, if an email is TLP RED then only the listed recipients should be exposed to the material, and it should not be shared under any circumstances without the author's permission.

Example:

During a threat hunt the blue team has discovered what they believe to be an advanced adversary within the network that has Domain Administrator privileges (the highest possible access and permissions). A meeting occurs between the hunting team, the security incident response team (SIRT), and other personnel. Due to the nature of this attack the organisation doesn't want any information getting out that could alert the adversary that they have been discovered, so only the persons in the meeting are permitted to discuss what has happened.

Previous Topic

Mark Complete

Back to Lesson