GFCE
Global Forum on Cyber Expertise

Global Good Practices

Practice: Produce and present trusted metrics about systemic risk conditions

#HealthMetrics

All those figures on a medical test report do not mean much to us — we need a doctor to analyse various data, contextualise it for our body and lifestyle, and present us with the findings in a comprehensive way. The same goes for network health — trusted data needs to be turned into vetted and well-presented metrics, to increase awareness and incentivise action by responsible companies, organisations, and institutions.

Related thematic areas:

Research and development

Cooperation and community building

Incident management and infrastructure protection

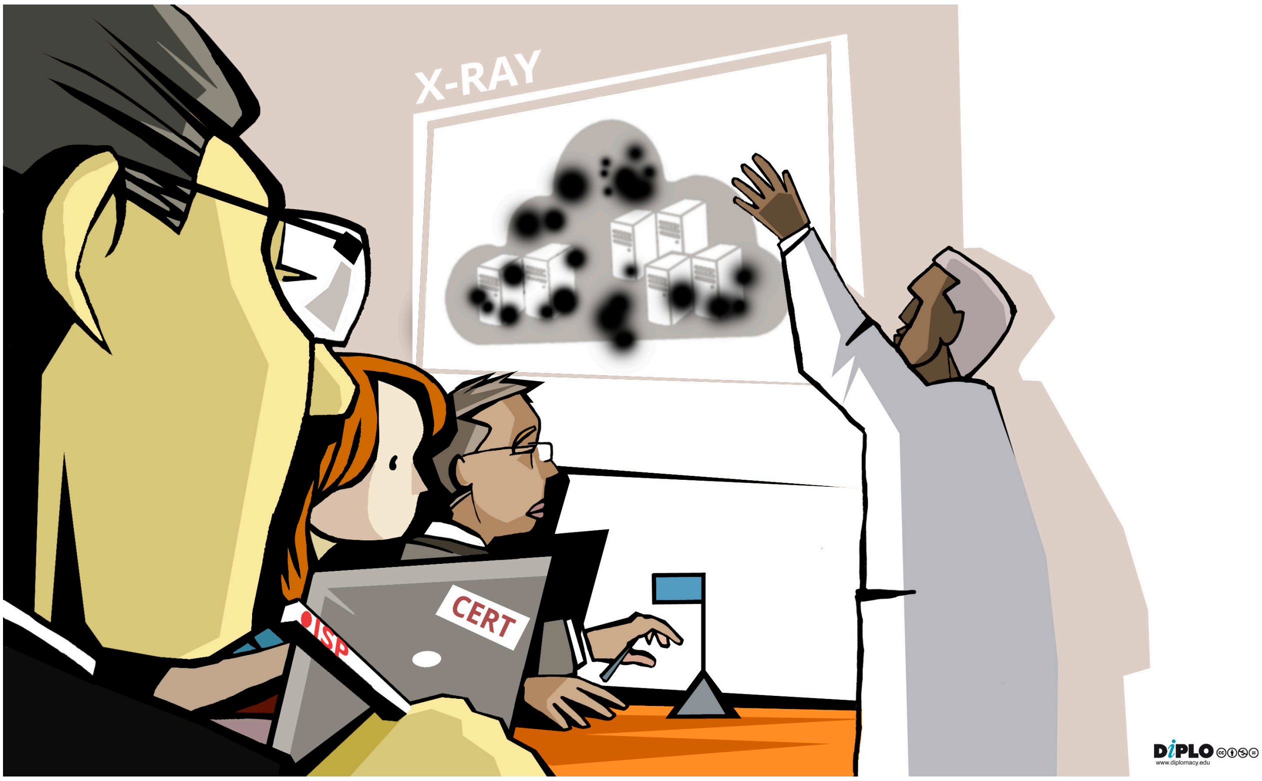
Culture and skills

Of particular interest to:

Description

Statistically mature and vetted metrics, rather than raw data, should be presented to the parties in charge of keeping the network clean. The development and application of statistical methods to data allows for measurement and contextualisation of key indicators of malicious activity and risk conditions. Metrics should be normalised transparently, so that users can interpret and use the data in their own way.

A statistics platform, featuring metrics and data visualisation, allows for the measurement of key indicators of malicious activity and risk conditions, and enables analytical insight about patterns, priorities, and trends for action. Such intelligence can be used by the CERT/CSIRT community, security sector, corporations, and organisations. If the metrics are regularly published in reports about the health of the cyber-ecosystem and the mitigation impact, the decision-making level — including CEOs and government ministers — could become more aware and ready to act.



Actors (or who this is for)

Everyone can benefit from obtaining trusted, clear, comprehensible data about the health of cyberspace:

- CERTs can use it to enhance the trust of their partners, to prepare situational awareness, and to issue early warnings.
- Network operators are expected to monitor the conditions of their networks and act accordingly. Clear metrics can assist them in identifying risks and trends.
- Security departments in companies, institutions, and organisations can likewise benefit from receiving clear metrics on trends in their environment.

- Governments can improve policy and operational responses to risks, if they are regularly informed about the health of the national network and the environment.
- Academics and researchers can use metrics to pursue additional research work.

In addition, several stakeholders can contribute to improving metrics. CERTs and network operators can feed into the metrics with particular data sets, as well as with information about the specific local use of the Internet and its services. If metrics methods are transparent, academics and researchers can validate them and help with improvements, and experts can replicate them for different purposes.

The big picture

The prevention of cyber-incidents is primarily based on a healthy cyberspace. On the operational level, CERTs can point to critical risks, while operators should mitigate flaws in their networks. On a policy level, policymakers should decide on strategic steps and action plans. All of them would benefit from trusted and processed intelligence about the health of the network presented in formats comprehensible to them.

Existing cybersecurity practice focuses on minimally processed data, commonly present in raw format which is useless to anyone but a particular niche of technical operators. Higher quality and more actionable data should be turned into metrics, through the analysis of carefully selected and processed comprehensive data sources and visualised presentations.

Using such metrics for regular monitoring of the health of the networks can assist CERTs in communicating with partners and provide them with a trusted picture of the condition of their networks. Operators and companies, organisations, and institutions in general can enhance their skills for understanding risks, thanks to clear risk indicators provided by the metrics. The metrics can increase the capacity of the decision-making level in corporations to assess risks and provide resources for mitigation. Similarly, they can improve awareness among policymakers and state decision-makers about cyber-risks, and enable them to more clearly recognise what policy approaches could help mitigation. Not least, thanks to the visualised and comprehensible metrics — possibly presented to the wider audience through CERTs — end-users can become more aware of the security risks and increase their demand for a cleaner network and safer cyberspace.

In addition, the continuous measurement of network health can lead to noticing improvements and identifying mitigating factors, which may allow the extension of lessons learned and good practices in mitigation.

Instructions

Metrics should be based on trusted, comprehensive, and pre-processed data sources, such as those developed through the clearinghouse approach (***#Clearinghouse***).
To make it action-oriented, metrics need to be based on the statistical analysis of raw data.

If possible, data should also be normalised for local Internet conditions or network usage. For instance, the majority of scanning and analyses have been conducted in the IPv4 space, yet with the increasing use of IPv6, it is necessary to consider the implications of IPv6’s massive address allocation and its impact on normalising results across groups of addresses. Also, bandwidth consumption and usage differ significantly between different regions. For example, even minor habits, such as the tendency for American computer users to leave their systems on all the time, can affect propagation and botnet impact. Normalisation should be done at the level of the metrics, and with transparent methods so that users can understand how it is done. It also allows comparability and eliminates the need to interpret the data on the client’s side. Local partners, such as ISPs and CERTs, can help with understanding local factors and feed them into the normalisation methods.

The metrics should be presented in an accessible and transparent format, with regular updates. For instance, an online platform could feature metrics searchable by country or geographical region, by network (e.g. Autonomous System Numbers), and by risk. Visuals, such as maps and graphs, are of particular relevance for easier understanding by various stakeholders.

Of particular relevance for outreach to decision-makers and CEO-level professionals is publishing regular (e.g. biannual) analysis reports featuring trends, risks, and mitigation impacts. Such reports should be accompanied by materials for policymakers about how to understand the metrics — what they show, and what mitigation approaches are possible. This can be linked with the production of training materials for various stakeholders.

There are several challenges to take into consideration. It is essential to build trust among other possible partners that should contribute to and use the metrics, which takes time. Processed data may not lead to actions by operators if they are not correlated with actionable steps a provider can take. When it comes to the presentation of metrics, it is very important that it does not include naming and blaming, as this would reduce trust and the readiness of third parties to act accordingly. The metrics are there to monitor the health of the network, and to incentivise parties to contribute to the mitigation of identified risks.

On a more general level, measuring network conditions is not the only possible measurement, and it does not necessarily reflect comprehensively the actual state of security for a particular environment. It may therefore be important to seek links with other initiatives that implement different measurements, such as the number of vulnerabilities within a product, or the use of penetration testing, to compile a more comprehensive view.

Timing

The timeline vastly depends on technical and operational capabilities and specific needs. Developing trusted metrics that can also be useful and easily readable by a variety of actors requires at least a year, with ongoing improvements.

Example

The GFCE initiative CyberGreen makes the cyber-ecosystem healthier through measuring, visualising, and mitigating negative impacts. Its Statistics platform v.2 features metrics-based measurement and visualisations as well as the ability to compare across countries and autonomous systems.

Several partners are using CyberGreen metrics for decision-making and additional research. Singapore uses the metrics to move policymakers to act. The Singapore ICT Minister has presented the results to other ICT ministers in the ASEAN region and encouraged them to use the platform and metrics to facilitate national and regional mitigation campaigns, while CyberGreen assisted with establishing a regional platform to follow the health statistics of each country in the region, and provide capacity building materials. Japan is also encouraging partners in Asia-Pacific and other intergovernmental forums to start using it, while ITU-ARCC is using CyberGreen metrics and training materials to encourage its members to act.

The biannual report published by CyberGreen has been used by many stakeholders, and has been presented at ministerial level (such as at G7 and G20) for several years to raise awareness among decision-makers.

CyberGreen's current sponsors include JPCERT/CC, the Singapore CSA, and the UK FCO. These, and other policymakers, benefit from having increased visibility of the risk levels that are present in their countries.

Source, support, and mentoring

CyberGreen Statistics platform:
http://stats.cybergreen.net/

Contact CyberGreen:
https://www.cybergreen.net/contact/

Contact point:
Yurie Ito (yito@cybergreen.net)