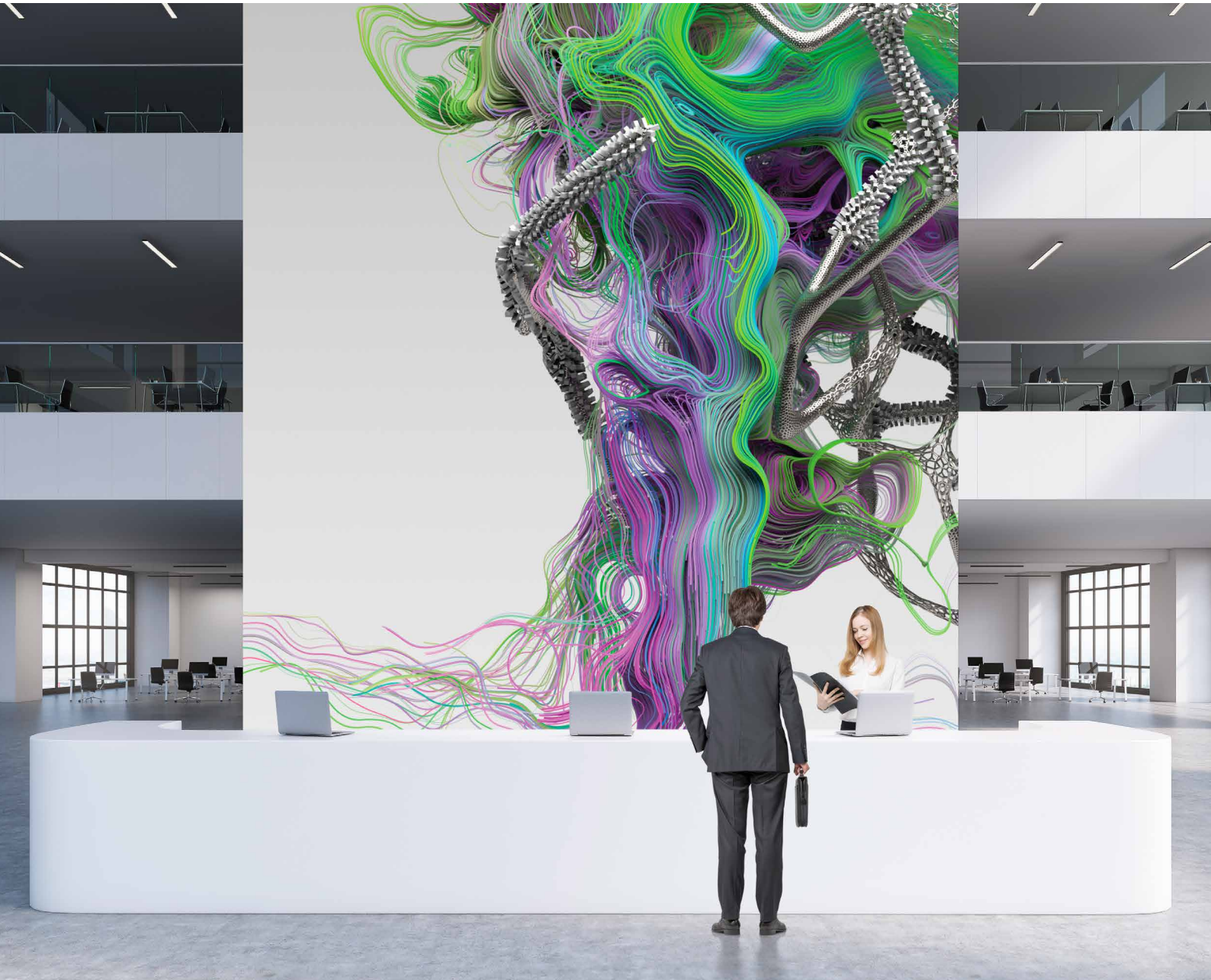
How to collect more hazard reports in CERT with custom sandboxing

Trend Micro™ Deep Discovery™ Analyzer uses XGen™ security to extend the value of your security investments



DOES THIS SOUND FAMILIAR?

You head the computer emergency response team (CERT) of a public authority or administration and your team of security specialists forms the central point of contact for all cybersecurity issues. You report on vulnerabilities, publish recommendations for action, and provide support in the event of security incidents. But, to create an accurate, up-to-date security picture, you need as much information as possible from each data center. The problem: since every authority and administration is usually responsible for its own IT and IT security, you have no direct insight into what is happening there. Instead, you rely on employees to report attacks. But unfortunately, that happens far too rarely.

EASIER SAID THAN DONE

The reason for the lack of transparency is usually because the reporting process is too cumbersome. For example, users can send suspicious emails to CERT that end up in the central CERT mailbox. Your employees have to pick them out of there, load them onto a USB stick by hand, and import them into a sandbox. After the analysis, they have to send the result back to the user prepared in such a way that it can be understood.

It takes hours or even days for the user to receive a response. The user usually doesn't want to or can't wait that long. So, they ignore the risks or don't send suspicious emails for review in the first place. You really can't afford this time-consuming process. Your team is already under pressure, you suffer from a shortage of skilled workers, and you need to manage your resources well.

Cybercriminals manage to smuggle dangerous files through to the user time and again, especially via email. This is because much of the traffic today is HTTPS-encrypted and therefore cannot be analyzed at the network level for legal reasons. Thus, you clearly need sandboxes on all endpoints where the files are in plain text—but that can be far too expensive.

WHAT NOW?

You need a central sandbox in the CERT that should be customizable and can be reached via a dedicated email addresses that can be connected to the security systems at the public authorities/administrations, allowing users or security systems to send suspicious messages directly to the sandbox.

Deep Discovery Analyzer custom sandboxing can support as many profiles as possible, allowing you to simulate different operating systems as needed, or to specifically build a particularly vulnerable environment. The sandbox can then communicate to the internet under special security measures, giving you the opportunity to investigate how an attack would proceed. A short, comprehensible message is automatically generated from the result of the analysis and sent back to the user, immediately notifying them what to do with the suspicious email. Meanwhile, CERT staff receive the detailed report and can investigate further if necessary.

Additionally, Deep Discovery Analyzer can easily integrate into the existing security infrastructure and offers comprehensive detection techniques supported by machine learning. For more information on the importance of automation and artificial intelligence (AI) in IT security, read "Top Security and Risk Management Trends" report from Gartner.

TREND MICRO TIP

Would you like more background information on a specific malware so you can better understand its distribution, lineage, and risk? Then choose a provider that can support you with advanced threat intelligence services.

KEY ADVANTAGES OF DEEP DISCOVERY ANALYZER

- Receive more data from the distributed data centers for a more comprehensive picture of the security situation.
- Save a lot of effort and unburdens your employees thanks to automation.
- Quickly receive analysis results so users at the public authority can continue working immediately
- Increases the acceptance of using the sandboxing service.
- Cost-effectively increase security in individual data centers without the need to install a separate sandbox at each endpoint.
- Makes it easier for employees to report security incidents and meet compliance requirements under the IT Security Act.

TRUSTED CYBERSECURITY PARTNER BY YOUR SIDE

With Deep Discovery Analyzer, you get an industry-leading sandboxing solution that uses advanced detection methodologies to deliver the highest detection rates with the lowest number of false positives. Trend Micro was named a Leader in the Forrester Wave™: Enterprise Detection and Response (1st quarter 2020) and is a leader in initial detection according to MITRE ATT&CK Evaluations - APT29.

Trend Micro (listed on the Tokyo stock market) has over 30 years of experience as a security solutions specialist. The company has been successfully managed for 15 years by its co-founder Eva Chen, internationally recognized as a leading woman in IT. Since its founding in 1988, Chen and her management team have ensured that the company has grown healthily and reinvests extensively in research and development, even in times of crisis.

Her motto: "Our only competition is cybercriminals, who must be stopped."

TREND MICRO™
Securing Your Connected World