NTT offers Cyber Threat Sensor to clients in wake of SolarWinds attacks

Tuesday 19 January, 2021

As multiple vulnerabilities are discovered, NTT provides 30 day trial at no charge

UK, London – 19 January 2021 - NTT Ltd., a leading global technology services company, has today announced it is offering qualified clients a free-of-charge specialized sensor capability*. This will enable enterprises and public sector agencies to make an initial determination of their risk and potential means to mitigate attacks related to the recent SolarWinds incidents.

In December 2020, a supply chain attack through SolarWinds' commonly-used network management software allowed malware to be distributed to at least 18,000 organizations around the world. Additional threats have also since been identified, potentially exposing organizations' applications and data. NTT's view on these recent attacks can be seen here**.**

In response to these supply chain attacks, NTT will provide companies that believe themselves to be at risk of compromise with their 30-day trial of our Specialized Sensor for SolarWinds Detection and Alerting across all platforms other than Azure, at no charge.

This offering includes:

- Deployment of a specialized sensor in AWS and Google Cloud Platform environments for the detection of Indicators of Compromise (IOCs) specific to the SolarWinds breach.
- Near real time notification to a client's security organization in the event a compromise is detected.
- An actionable incident report delivered automatically, immediately upon detection of IOCs linked to the SolarWinds compromise.

Organizations can then engage with NTT for a more in-depth review, analysis, recommendations, and remediation including a rapid incident compromise assessment. NTT can also provide ongoing managed security services such as Security Operations Center as a Service (SOCaaS) and develop a Strategy for Supply Chain Security Assurance, to help clients monitor their technology assets and reduce risk from future threats.

Matt Gyde, President and CEO, Security Division at NTT Ltd., says, "Threat actors have exploited disruption during the COVID-19 crisis to launch an accelerated wave of cyberattacks around the world. The SolarWinds incidents were orchestrated by sophisticated operators and exploit the broad distribution of commonly-used software packages. NTT has now moved to proactively offer clients a way to identify potential problems in their technology infrastructure and take the steps needed to close those gaps."

"At NTT our ongoing commitment is to make the world a better place through the power of technology, as we all navigate the new normal, we have an opportunity to build a better, connected future. With innovation, the possibilities to use technology for good are endless," concludes Gyde.

For more information regarding the offer please visit our website here**.**

** Current and prospective clients that meet NTT's criteria are eligible for this offer.*

About NTT Ltd:

NTT Ltd. is a leading global technology services company. We partner with organizations around the world to shape and achieve outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital and secure. As a global ICT provider, we employ more than 40,000 people in a diverse and dynamic workplace that spans 57 countries, trading in 73 countries and delivering services in over 200 countries and regions. Together we enable the connected future. Visit us at hello.global.ntt

Related Sectors:

Computing & Telecoms ::

Related Keywords:

Cyber Attack :: Cyber Threat :: Cybersecurity :: Tech For Good :: Data Center :: Ransomware :: Malware :: Intelligent Cybersecurity ::

Scan Me:

Media Enquiries:

Marian Scala

T: +27 11 575 1541

E: marian.scala@global.ntt

Hotwire for NTT Ltd.

Beth Sissons

beth.sissons@hotwireglobal.com

Company Contact:

NTT Ltd.

E. ntt@hotwireglobal.com
W. https://hello.global.ntt/

Additional Contact(s):
Hotwire for NTT Ltd.
Hannah Lock
hannah.lock@hotwireglobal.com

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.nttltd.pressat.co.uk