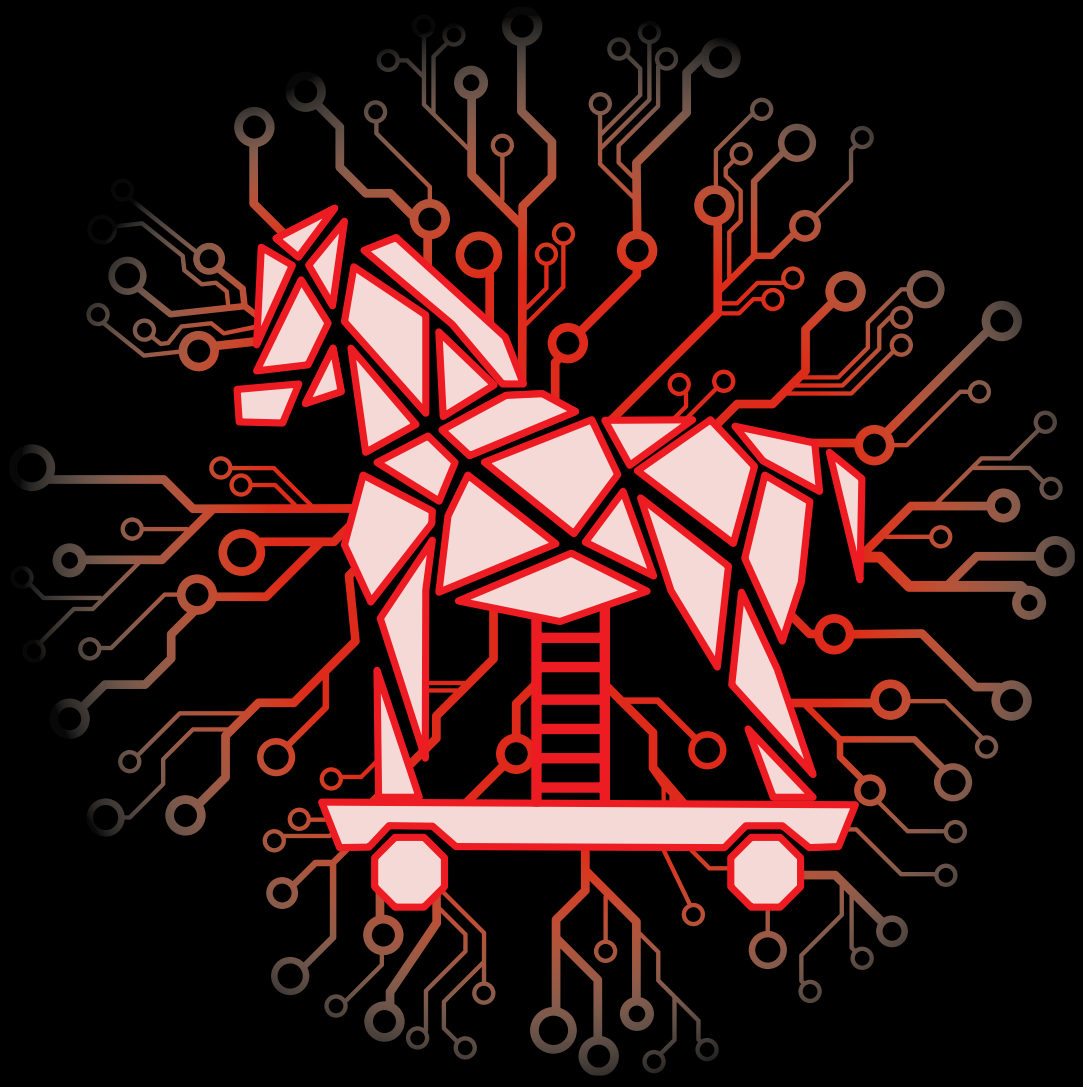
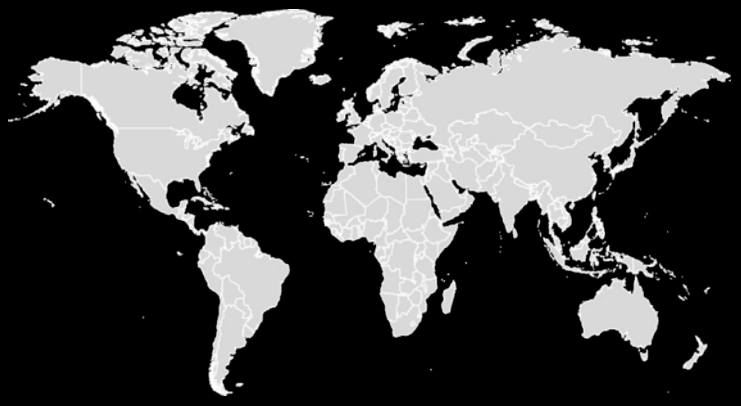
Deloitte.
デロイト トーマツ



Red Team Operations Attackers Report 2020

Overview of key engagement results

Red Team Operations (RTO) Global and Japan trends 2020



Covid-19 will reshape the focus of incident response and monitoring

Due to the dramatic increase in remote telework as result of the COVID-19 outbreak, our clients are increasingly concerned about the cyber security implications of remote work environments and whether their existing security controls are still effective. Clients are including in the scope of their Red Teaming engagements scenarios to assess their security solutions, monitoring teams and incident response procedures with a particular focus on remote work systems and endpoint security.

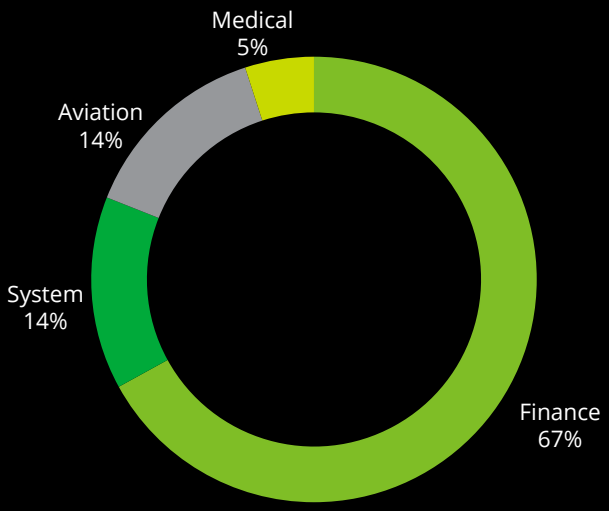
In Japan, we are expecting an increase in the demand of Threat-Led Penetration Testing (TLPT)

In October 2018, the Financial Service Agency of Japan has set out a number of initiatives to highlight the need for Threat Led Penetration Testing to reinforce Japan's cyber security capabilities. Because of this, we have seen a steady increase in the demand of TLPT projects.

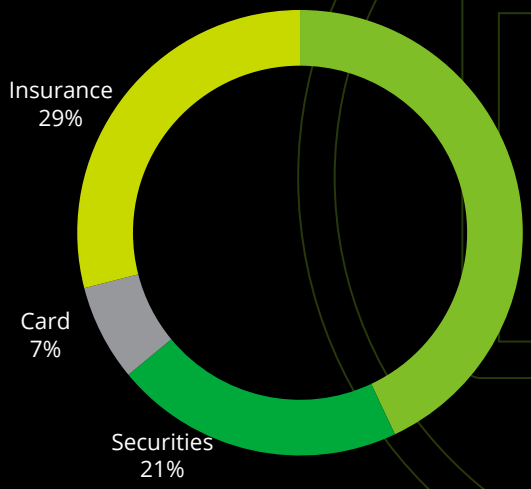
Industry insights, engagement types and response overview

Engagement activities by Industry in Japan

In Japan, the majority of RTO engagements are provided to the Financial Services Industry (FSI).



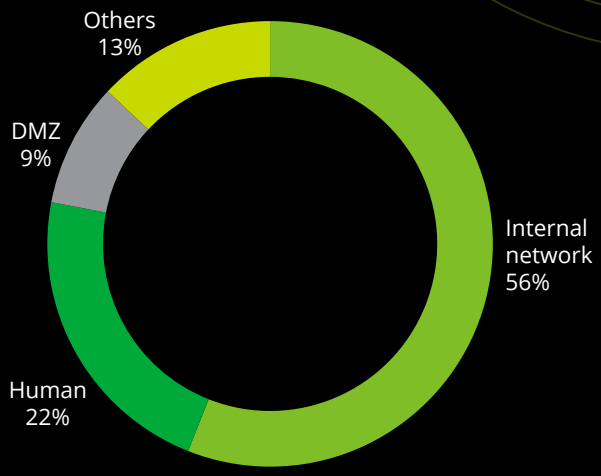
Within FSI, the Banking sector comprises the highest percentage of RTO projects - with over 40% of the engagement share.



Key Engagement Targets

Clients have been focusing on their internal network protection when engaging Deloitte in Japan. These engagements typically start from a client's workstation.

Human aspects of cyber resiliency are often tested by using phishing campaigns targeting company employees as an entry point to infiltrate the environment.



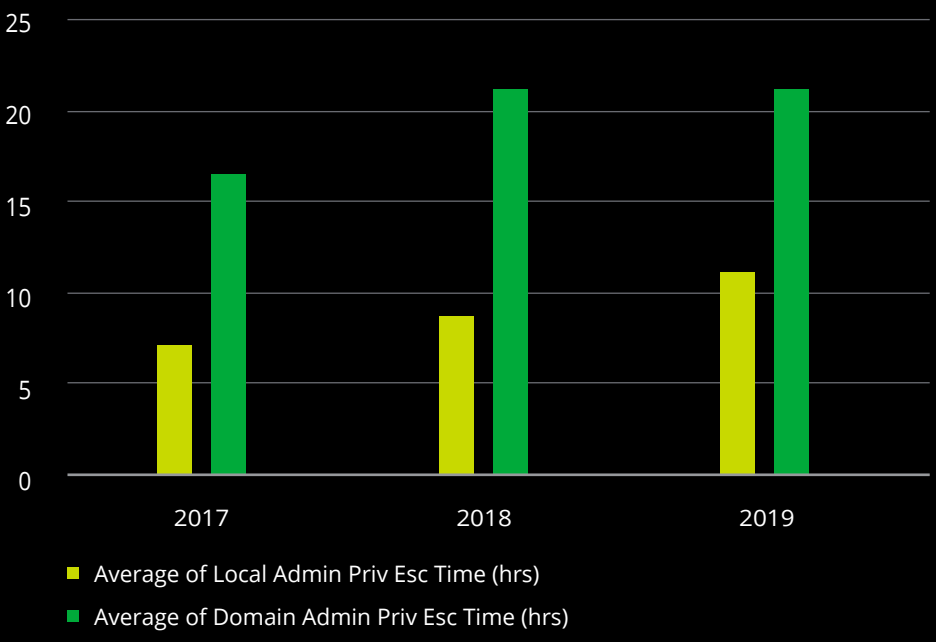
Attacker performance and Client resiliency

Local Admin and Domain Admin Privileges

It is common, during RTO engagements, to have as primary or secondary objectives the need to obtain local and domain admin privileges. The time our team needs to gain these credentials is usually indicator of the cyber maturity level of an organisation.

Across all sectors the time our team needs to obtain administrative level privileges is increasing, which is a sign that the defensive teams of our clients are becoming more advanced and their organizations are becoming more resilient.

Since most organisations use Microsoft Windows® based environments, one of the most important metrics is the average time to Local and Domain Administrative privileges. While this is not the only metric, it is a reliable one. Overall we have noticed that the advantage is constantly switching between the blue and red team as time progresses and that with more testing and practice the defensive teams of our clients are becoming better.



How often do we get in?

96%
of the time

Excludes engagements where obtaining Local/Domain Admin privileges is not required

Attacker performance and Client resiliency

How far do we usually get?
Within the engagement window we have a success rate of 94% of obtaining the crown jewel objectives.

Crown jewels are personalised to each client and engagement and are defined in the initial client discussions between the client and Deloitte since they are defined in the initial discussion between the client and the RTO team.

Typical Crown Jewels chosen by our Clients

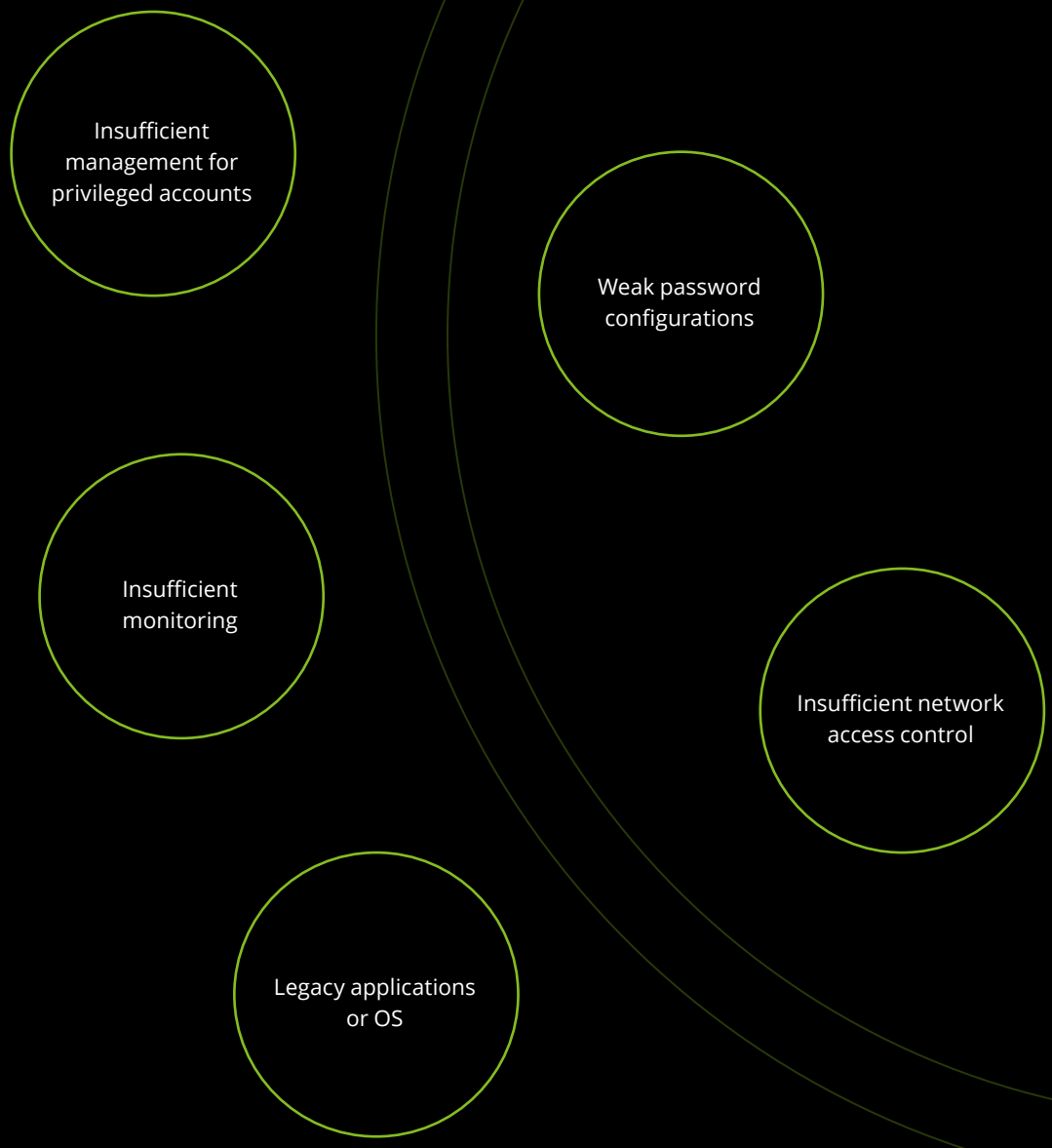
Attacker performance and Client resiliency

How many issues do we usually find?

Clients who have an ongoing security assessment relationship with us have benefited by implementing the recommendations we have made over the years. This reduces the number of vulnerabilities and weaknesses which can be exploited by an attacker.

On average, our team discovers between three and seventeen issues during each engagement that are reported to the client.

Typical issues reported to Clients



Client resiliency by industry and engagement types

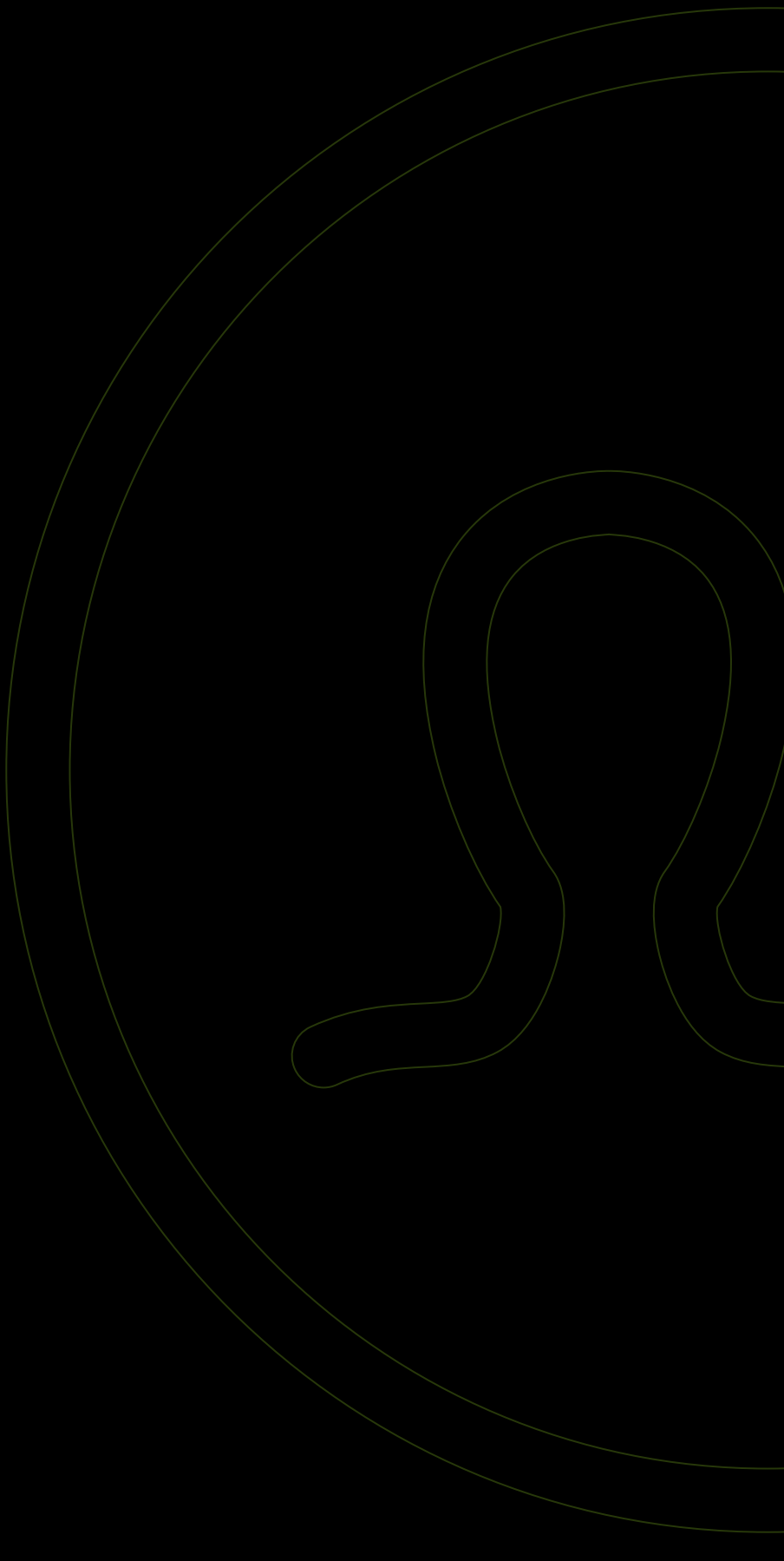
On average, by industry, Insurance and Aviation (Airports) appear to be more resilient during RTO engagements. By comparison Healthcare clients (hospitals) required the least amount of time for our team to gain privileged access.

Contacts

Masafumi Nomiyama
masafumi.nomiyama@tohmatsu.co.jp

Ari Davies
ari.davies@tohmatsu.co.jp

Carlo Emmanuele Geraci
carlo.geraci@tohmatsu.co.jp



Deloitte Tohmatsu Cyber LLC
Mail ra_info@tohmatsu.co.jp
URL www.deloitte.com/jp/en/dtcy