CAPABILITY DRIVEN TESTING

SPECIALISED INFORMATION SECURITY
CONSULTANCY SERVICES

INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

Capability Driven Testing

Modern information systems attacks are a significant departure from the traditional threats addressed by corporate IT teams.

The 'Classical' approach of using antivirus to defend against malware written by bored teenagers, or installing firewalls to ward off network worms, does not address the real risks most 21st century intellectual-property-centric organisations now face.

Capability Driven Testing addresses these risks.

What is Capability Driven Testing?

Defence, response and assurance activities are continuously evolving to match today's threats through an increasing focus on security testing that actually addresses the techniques and methodologies used by 'real world' attackers.

In any given attack, there are a number of tasks an attacker *must* conduct in order to be successful: Each of these steps is now being referred to in the security industry as the 'Intrusion Kill Chain'.

Capability Driven Testing (CDT) Exercises allow an organisation to actively and effectively test their current defence, response and reporting capabilities against this Intrusion Kill Chain.

Each is carefully crafted to explicitly test operational detection and response capability across *every* aspect of the Intrusion Kill Chain.

How is Capability Driven Testing Different?

Figure 1 demonstrates the different phases of the Kill Chain.

Traditional assurance services (e.g. penetration testing) do not provide good coverage of the tool and rootkit installation, command and control, and actioning phases.

CDT does: Ensuring the appropriate exercising and development of *all* the Kill Chain phases.

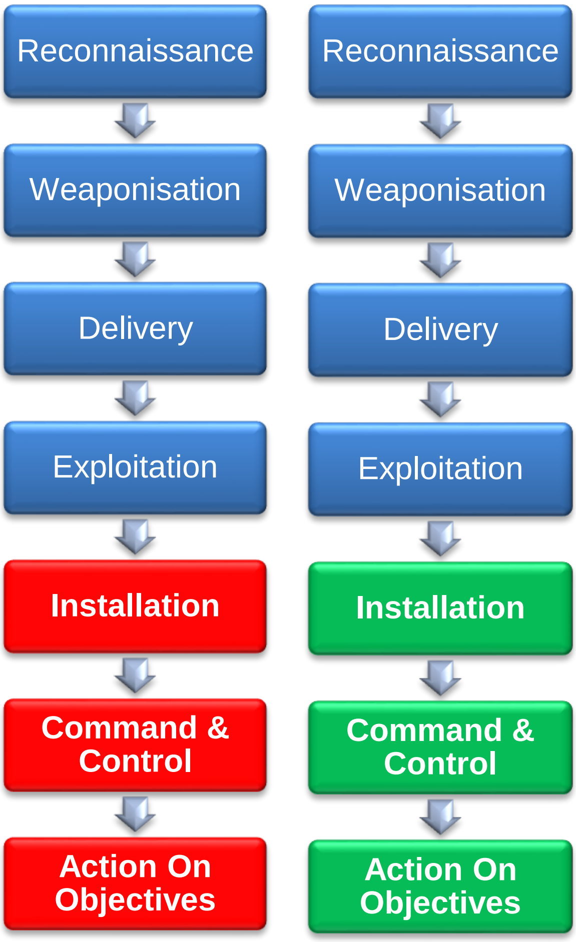


Figure 1: Comparison between more traditional assurance services and Capability Driven Testing.

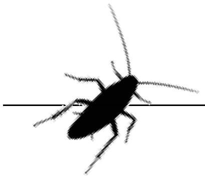
How is Capability Driven Testing Useful?

A CDT Exercise is more focused and structured than other, more 'traditional', assurance testing; it is a process-driven approach, with clear business goals, with a greater emphasis on follow-up capability.

This is because an organisation's detection and mitigation proficiencies are fully tested and measured under CDT, with its extra emphasis on education. Something the traditional assurance services lack.

During the course of a CDT Exercise, an organisation's operational teams will be tested at varying levels, dependant on current capabilities.

Such levels could include the following attacker profiles:



Did you know a group of cockroaches is called an "Intrusion"?

1. Unsponsored attacker (using common ‘off the shelf’ tools and techniques);
2. Rogue System Administrator (or similar attacker, with significant technical skills, but not necessarily security-focused); and/or
3. State-Sponsored Attack Group (with access to private tools and sophisticated malware, using the most effective current techniques).

Such exercises allow for the identification of operational security gaps, and can provide assistance in the design and implementation of effective detection capability and attack countermeasures.

Why Should We Implement Capability Driven Testing?

Today, attacks affecting an organisation’s bottom-line, are those with specific business goals in mind (e.g. data theft, IP, business plans), or those leveraging a business to attack its customers or partners.

The perpetrators who carry out such attacks are increasingly professional: Trained, resourced and tasked with targets and goals by their paymasters.

At the business level, CDT provides performance metrics to key stakeholders, thereby having the ability to demonstrate ROI, where applicable, on infrastructure assets (auto-detection capability, AV systems, incident response competency, etc.).

Additionally, CDT is a far better learning experience for the organisation’s personnel.

CDT will ensure an organisation’s capability gaps are identified, and countermeasures implemented, with maximum effectiveness.

What is Insomnia Security’s Approach?

Insomnia Security believes modern assurance testing should simulate attacks against all aspects of the Intrusion Kill Chain, and will tailor CDT to an organisation’s business requirements.

Insomnia Security’s approach to the CDT Exercise process consists of the following four key steps:

1. Exercise design and deployment;
2. Exercise setup and preparation;
3. Live exercise execution; and
4. Exercise debrief and report generation.

The following outlines in detail Insomnia Security’s approach to a CDT Exercise:

CDT Exercise Design and Development

CDT Exercises are designed and developed to provide organisations with ‘real world’, highly representative simulations of modern network attacks.

Each exercise is individually designed for the organisation, with a fully customisable level of attacker sophistication, target goals, and tool chains.

CDT Exercise Setup and Preparation

A typical engagement would consist of an initial self-assessment questionnaire, which profiles organisation’s existing security controls, and its practices for handling post-intrusion activity.

This self-assessment questionnaire also helps to establish specific business-level goals which would be valuable to different attackers.

These goals would then be used to help guide the behaviour of the assessment team.

For example, a government department may be concerned about the ex-filtration of sensitive data from the desktop network; a petroleum company may be concerned about remote access being leveraged as an access method for intruders; or a financial institution about implants designed to obtain Track 2 information.

CDT Live Exercise Execution

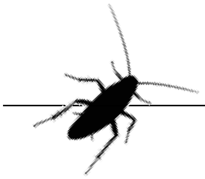
CDT Testing execution is ideally initially conducted as a ‘walk-through exercise’ with relevant network and security operations teams.

This being done to ensure capability gaps are identified and countermeasures implemented with maximum effectiveness.

Exercises should be revisited or replayed in the future, without operational team knowledge, to test that implemented solutions are effective and being maintained as a part of day to day operations.

CDT Exercise Debrief and Report Generation

During the CDT Exercise execution, specific focus is placed on documenting both detection successes and failures: Capabilities are discussed and dissected, and improved techniques for detection and mitigation are fully documented.



At the termination of the exercise, this information is captured into a comprehensive CDT Exercise Report, and this sent to key client staff for their review.

The CDT Team Exercise Debrief involves a full and compressive walkthrough of the resulting report with key client staff, alongside the Insomnia Security team, to ensure capability gaps are thoroughly understood and fully addressed.

What Sort of Testing is involved?

The following demonstrates the types of testing Insomnia Security could carry out within an organisation over the course of a CDT Exercise.

Installation:

- Elevation of Privilege detection and prevention;
- Custom malware installation and execution;
- AV detection and response validation; and
- AV bypass detection.

Command and Control:

- Detection of common Command and Control (C2) Egress Types;
- DNS C2 blacklist and detection; and
- Non-C2 Egress (E-mail, etc.).

Lateral Movement and Action Objectives:

- Internal network reconnaissance; and
- Active directory and centralised authentication attacks.

Additional Malicious Activity:

- Dual VPN usage; and
- Rogue system administration actions.

During the course of a CDT Exercise, all key organisational staff would be provided with training in active countermeasures, in order to address any gaps Insomnia Security uncovered while testing.

In essence, Insomnia Security uses two distinct approaches over the course of a CDT Exercise:

1. Controlled: Which allows operational team participation, with an Insomnia Security consultant on hand for direct guidance; and
2. Active: The revisiting of post-Exercise implemented solutions to ensure their effectiveness, which is done without operational team awareness.

Utilising 0day Exploits

Insomnia Security can make use of ‘0day’ (‘zero-day’) vulnerabilities, and associated exploits, during CDT Exercises.

These may either be privately discovered by Insomnia Security, or via our third party partner Exodus Intelligence (https://www.exodusintel.com/).

The use of such unpatched vulnerabilities during CDT Exercises enables us to fully test an organisation’s layered defences against the very latest, up-to-the-minute threats.

Our Contact Details

For sales enquiries: sales@insomniasec.com

All other enquiries: enquiries@insomniasec.com

Auckland office: +64 (0)9 972 3432

Wellington office: +64 (0)4 974 6654

www.insomniasec.com