Infopercept

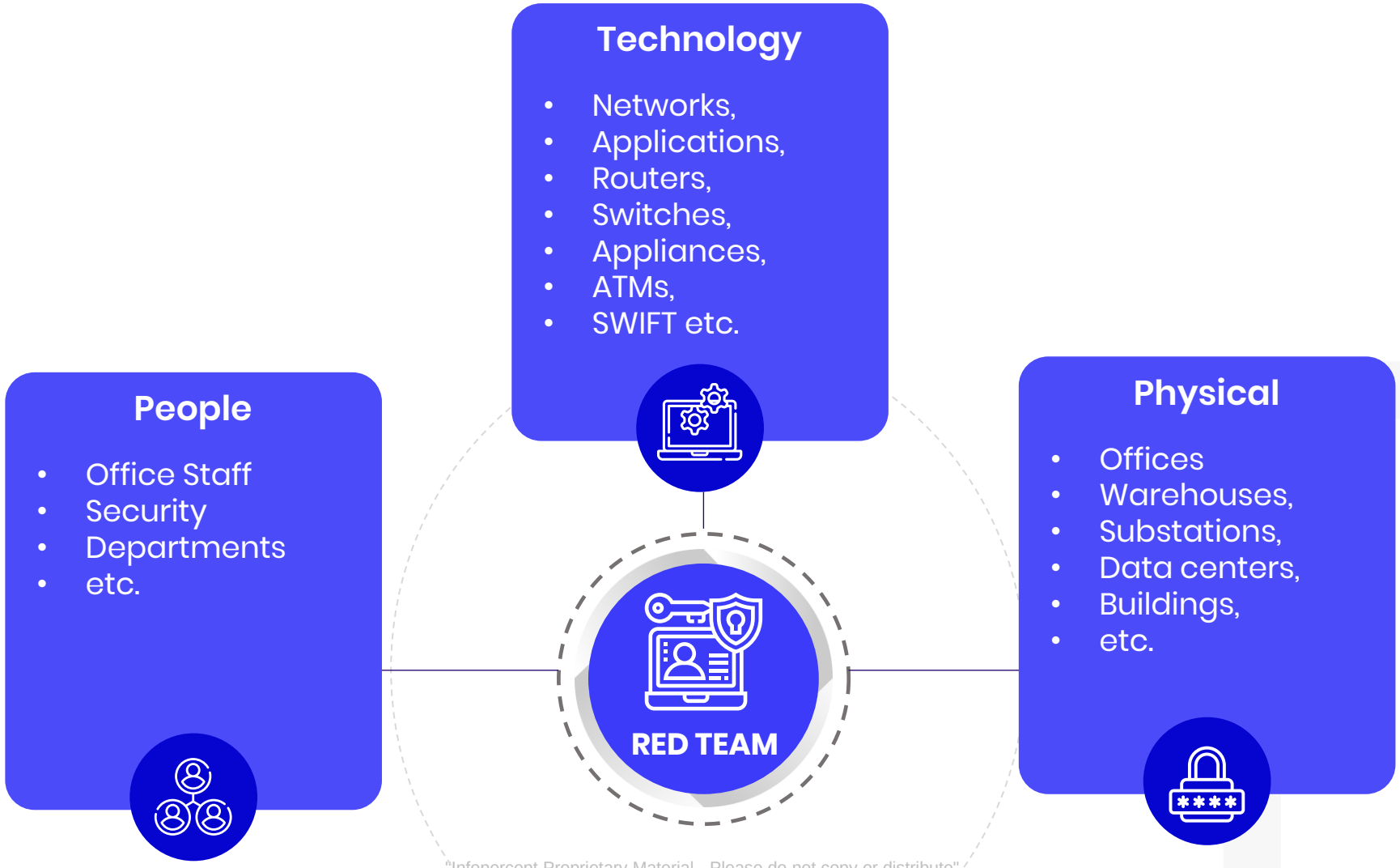
Your Ally in Digital Warfare

Red team Assessment

Technical -Approach

Objective

Objective of a red team test is to obtain a realistic level of risk and vulnerabilities against your Technology, People and Physical/ Facilities without causing business disruption.



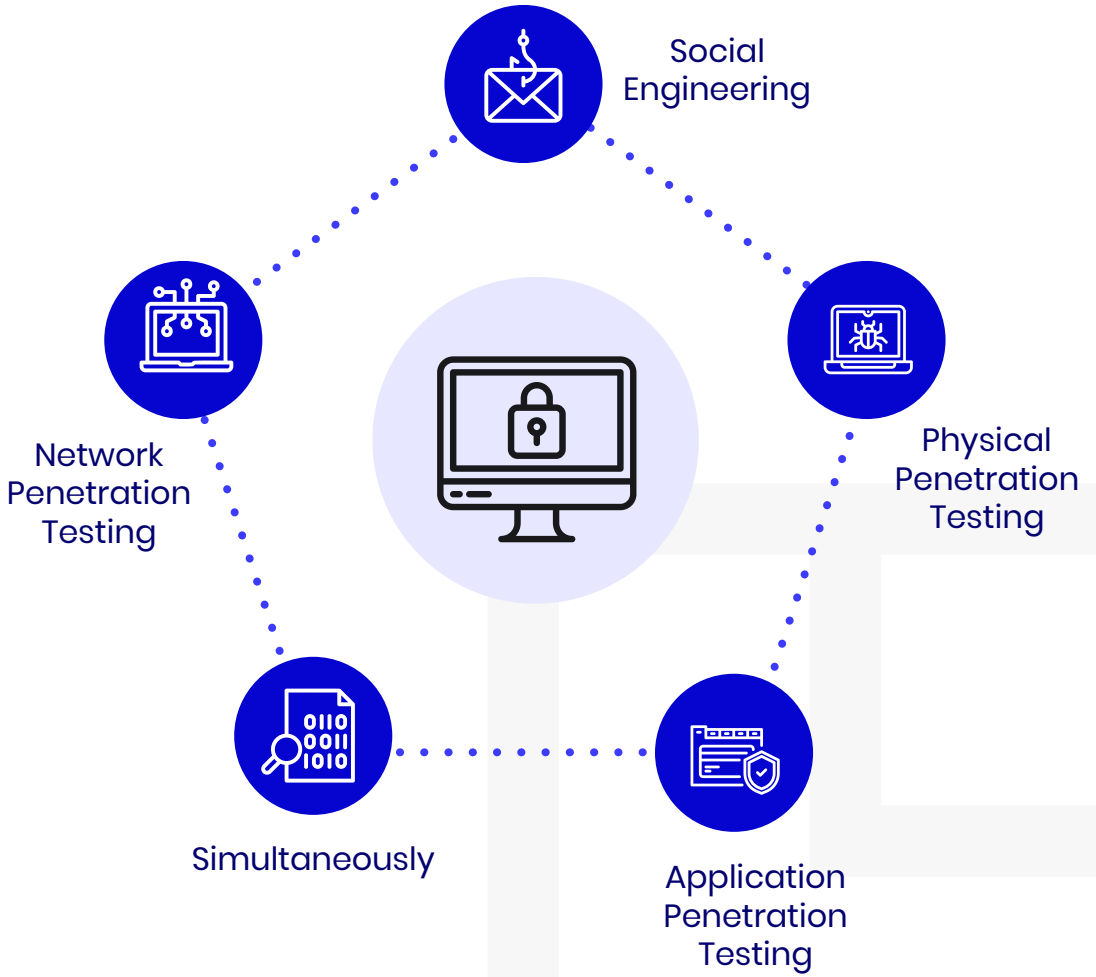
Objective

Our team will launch a well-planned attack involving several facets of social engineering, physical penetration testing, application penetration testing and network penetration testing, simultaneously. It's aimed at revealing real-world opportunities for malicious insiders or bad actors to be able to compromise all aspects of your organization in such a way that allows for unauthorized virtual and/or physical access to sensitive information leading up to data breaches and full system/network compromise.

Red Team testing begins with the collection of target data, which is analyzed for potential technical, physical, and social vulnerabilities. Exploits are then selectively executed to gather more information and control of target assets.

Compromised systems are used to establish persistence on the target network and to begin a new round of data collection within the environment. Information and access gained in early cycles is used to move the attacker closer to their objectives.

As opposed to traditional testing, which delivers a comprehensive review of all vulnerabilities and technical risks, during Red Team testing,

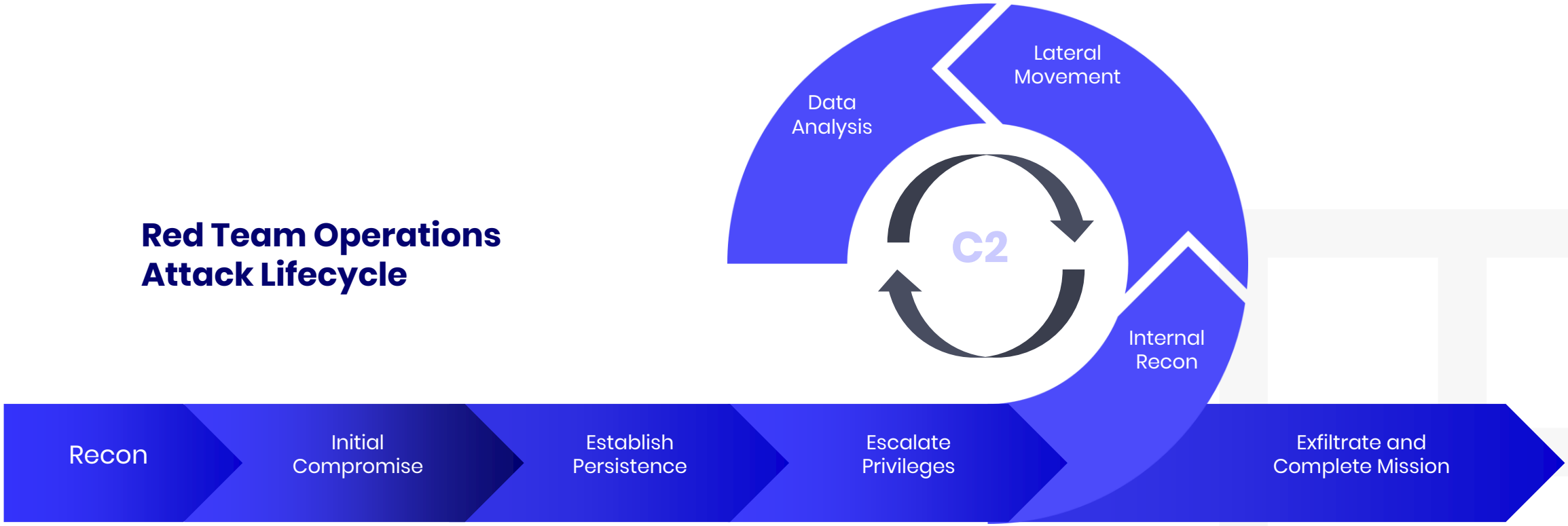


Our Approach

Infopercept

Every Red Team Operation is conducted using globally accepted and industry standard frameworks. In order to ensure a sound operation, Infopercept leverages industry standard frameworks as a foundation for carrying out Red Team Operations. At a minimum, the underlying framework is based on the NATO CCDCOE, OWASP goes beyond the initial frameworks themselves

Red Team Operations Attack Lifecycle



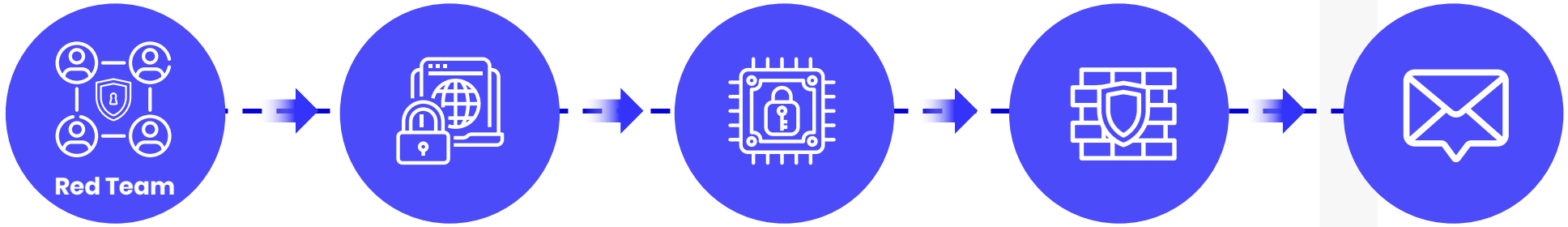
Pre-Engagement Meeting

Infopercept

A critical component of an Infopercept engagement is to clearly establish and agree to the Rules of Engagement ("RoE"). During our initial scheduling and kickoff session, the RoE for testing is established. Topics to be covered include:

- Purpose of and goals for testing
- Definition of scope and validation of targets Testing timelines and schedules
- Rules of engagement, levels of effort, and risk acceptance Reporting requirements and deliverables, timelines, and milestones
- Key personnel, roles and responsibilities, escalation rules, and emergency planning Infopercept attack source and reverse connect IP addresses

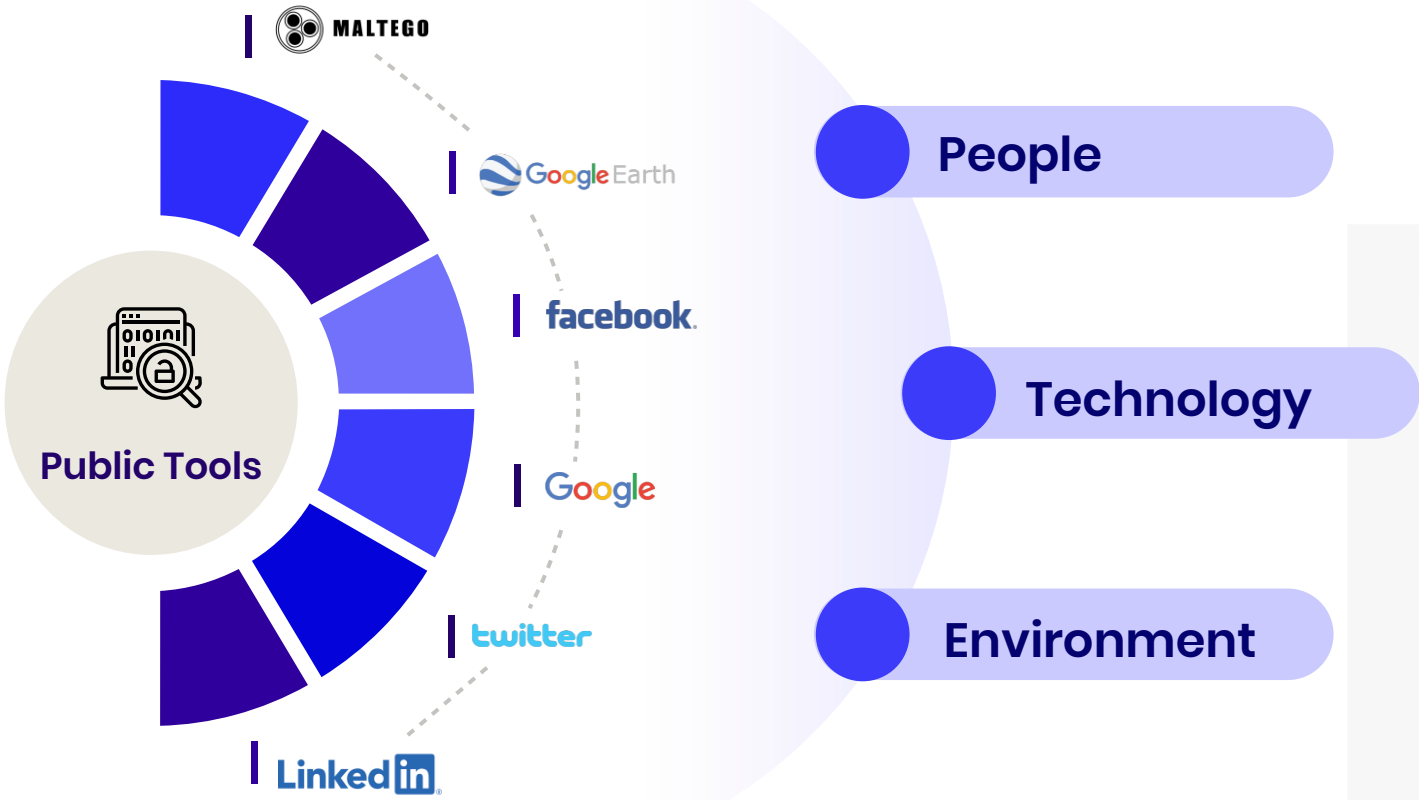
Infopercept will send a confirmation email following project kick-off to ensure agreement on these Items.



Reconnaissance

Infopercept

The first phase in a red team operation is focused on collecting as much information as possible about the target. Reconnaissance is one of the most critical steps. This is done through the use of public tools, such as Maltego, LinkedIn, Google, Twitter, Facebook, Google Earth, etc. As a result, it is usually possible to learn a great deal about the target's people, technology, surroundings and environment. This step also involves building or acquiring specific tools for the engagement.

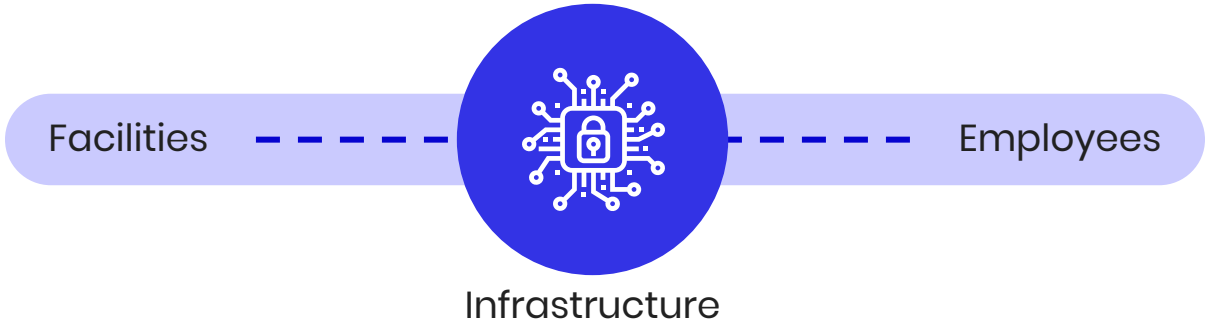


Initial Compromise

Infopercept

An important phase in a red team operation focuses on collecting information about infrastructure, facilities and employees. Open Source Intelligence Gathering can be quite telling about a target, its people, its facilities and its technical makeup, such as: physical/logical security controls, foot traffic, terrain etc. Through thorough analysis, it begins to paint a picture of the target and its primary operations. Effective weaponization involves preparation of the operation specific to the target taking into full account intel gathered from the reconnaissance stage. This commonly includes: crafting custom malicious file payloads, configuring hardware trojans, acquiring social engineering costumes, creating falsified personas/companies and much more.

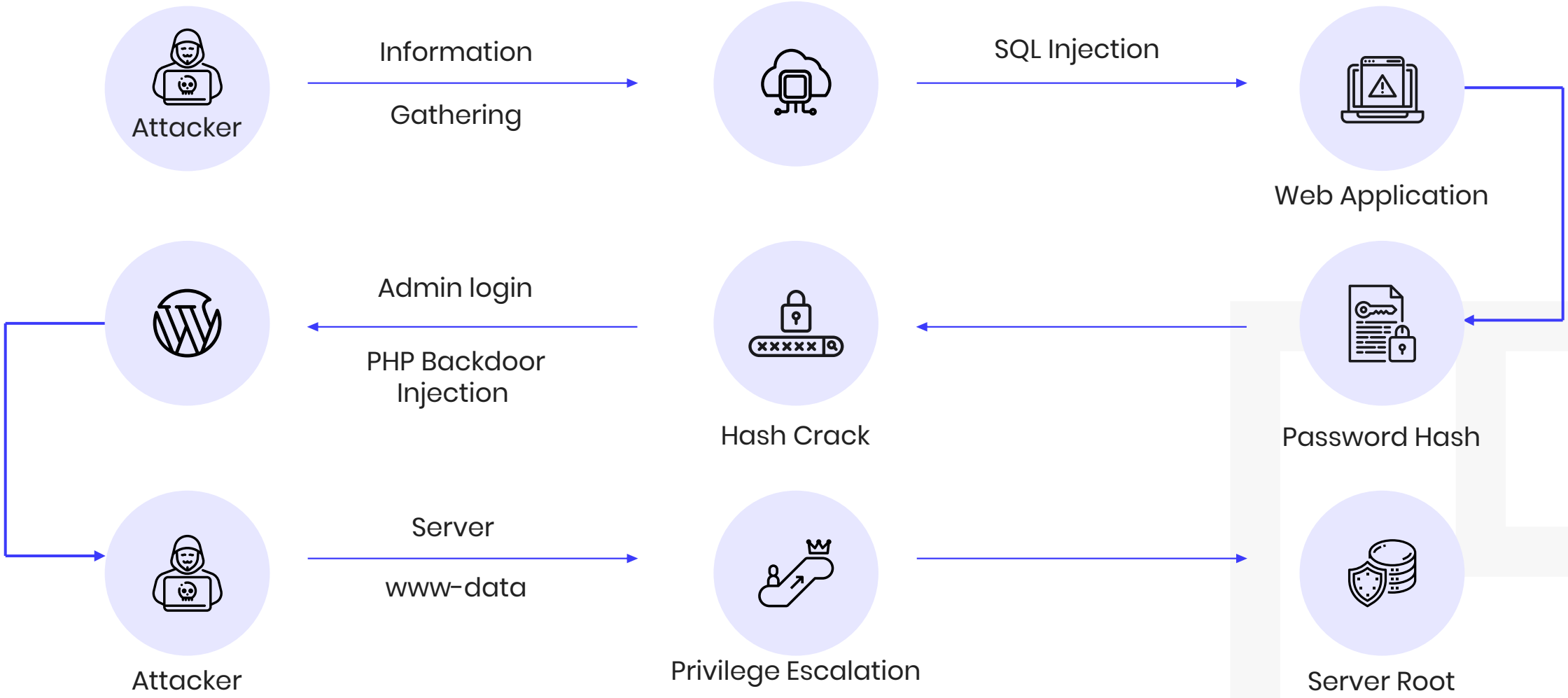
Infopercept consultants carry out the actions on the target(s) intended to reach the project operation's goals. Things like physically cloning badges, phishing, social engineering face-to-face targets, analyzing cyber vulnerabilities, planting hardware trojans for remote network persistence, etc. Among one of the most important objectives is to note the best opportunities for exploitation. At this point, the goal is to "break in" or compromise servers/apps/networks, bypass physical controls (i.e.: gates, fences, locks, radar, motion detection, cameras) and exploit target staff through social engineering by face-to-face, email, phone, fax or SMS. The exploitation stage enables the preparation for the escalation and installation phase.



Escalate Privileges

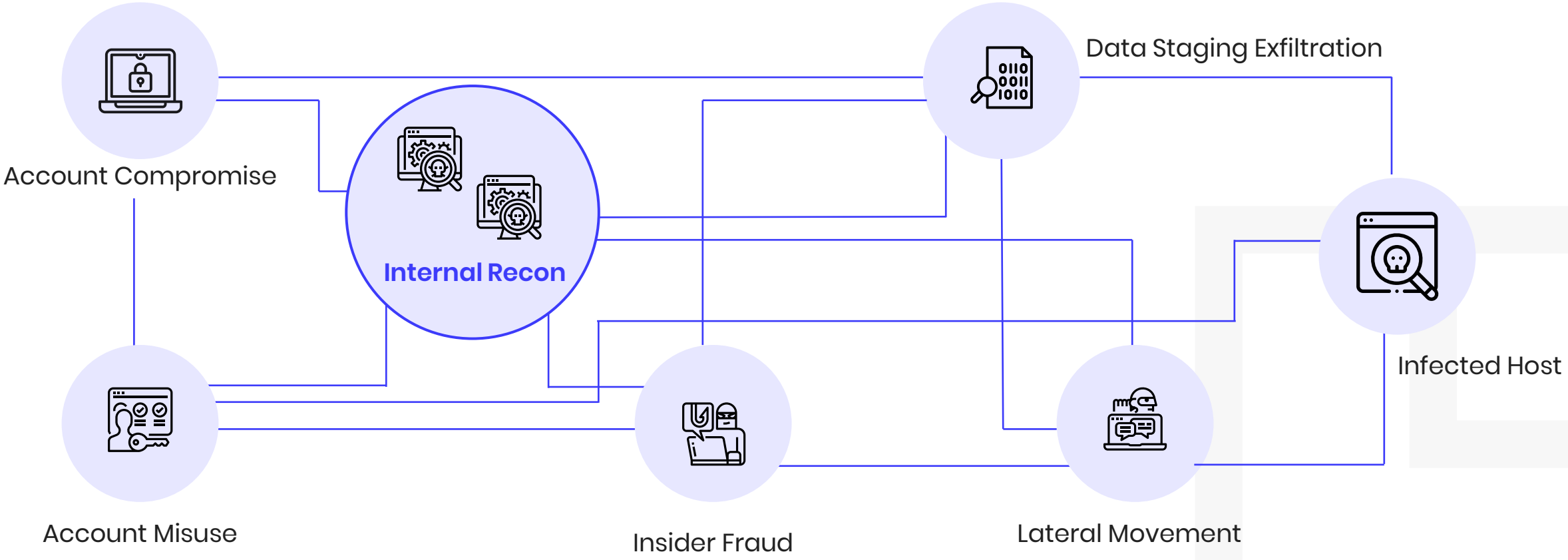
Infopercept

Things like privilege escalation on compromised servers, shells, malicious file payload installation, usage of physical key impressions and lock picked doors happen here



Internal Recon

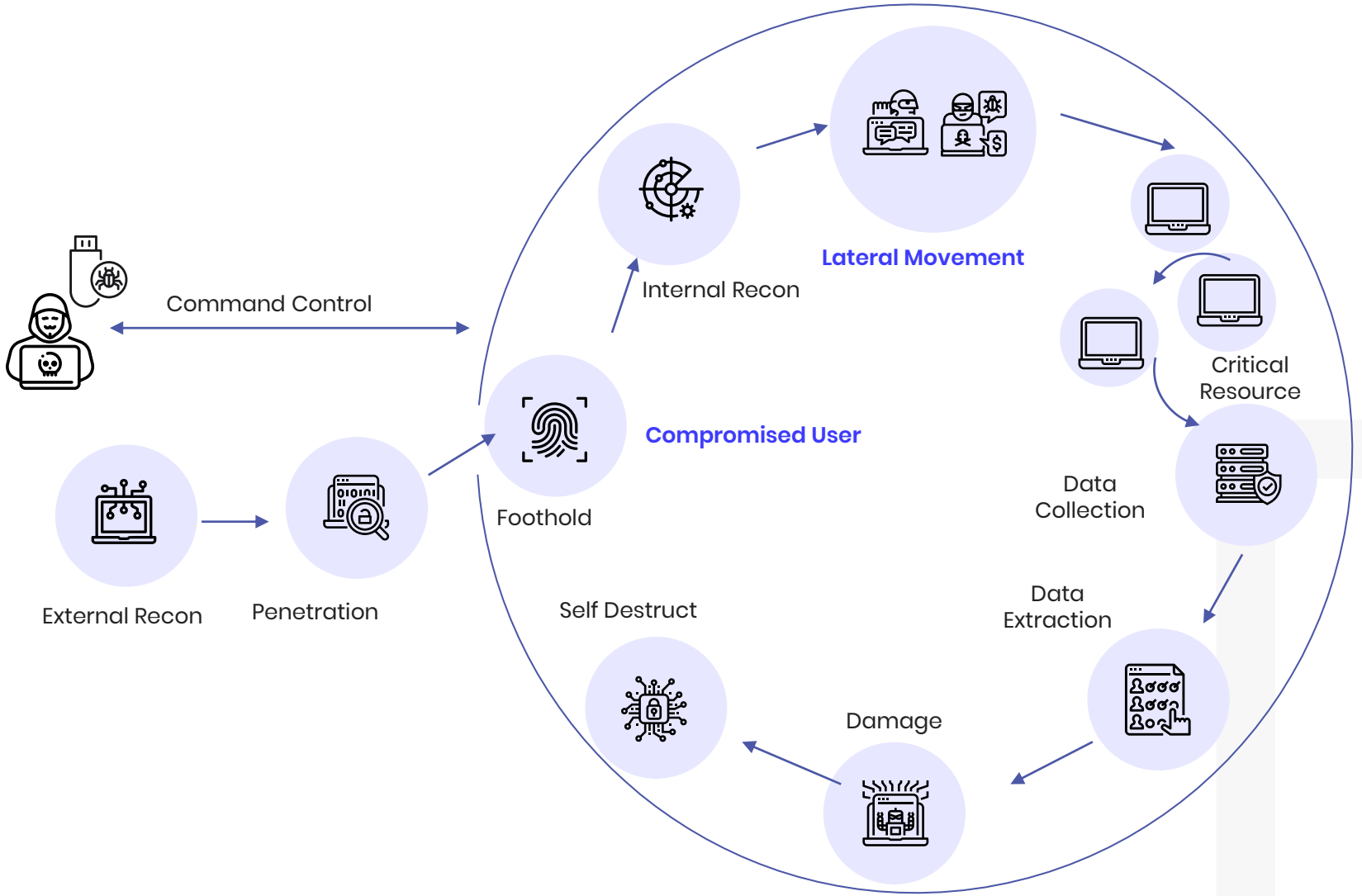
Infopercept takes steps to ensure remote access to exploited systems are stable and reliable setting the stage for data exfiltration and other post-exploitation tasks/goals. Internal recon is done to get as much as information of the network, key systems and existing security controls. On the physical and social side, manipulating people into enabling circumvention of physical barriers in order to create backdoors into facilities are key.



Lateral Movements

Infopercept

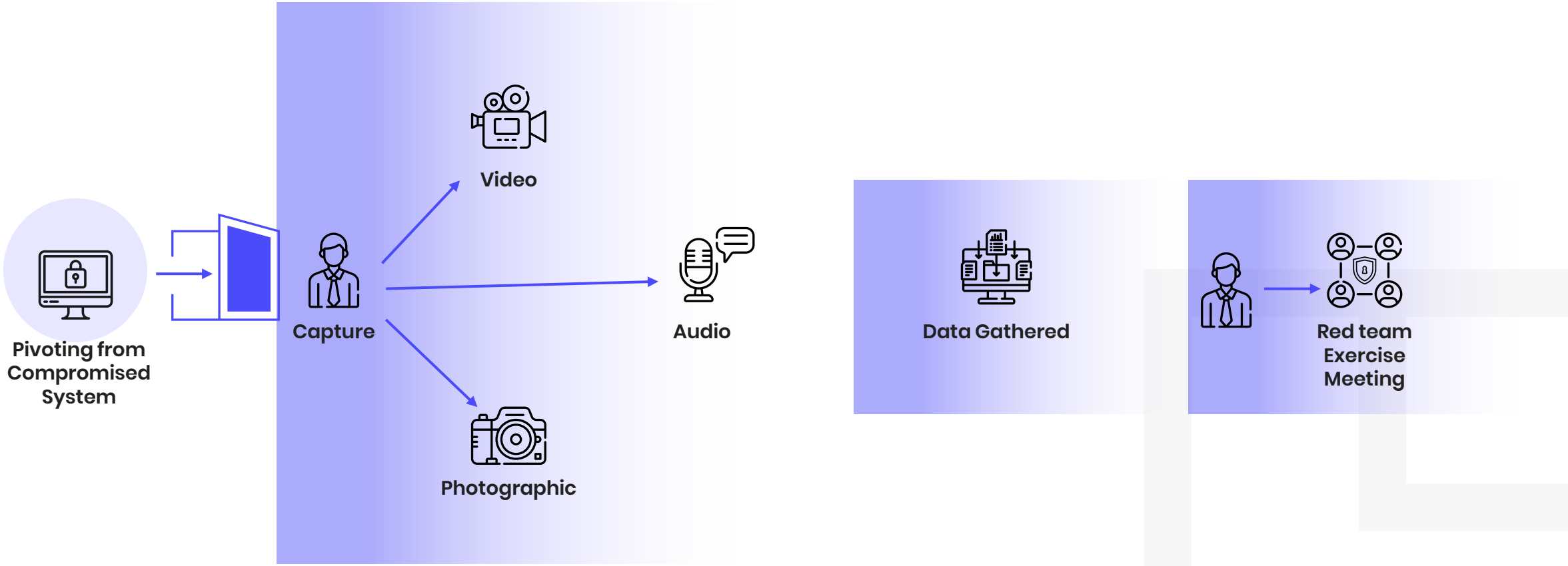
Actions on objective happens through lateral movement throughout the cyber environment as well as the physical facilities



Data Analysis

Infopercept

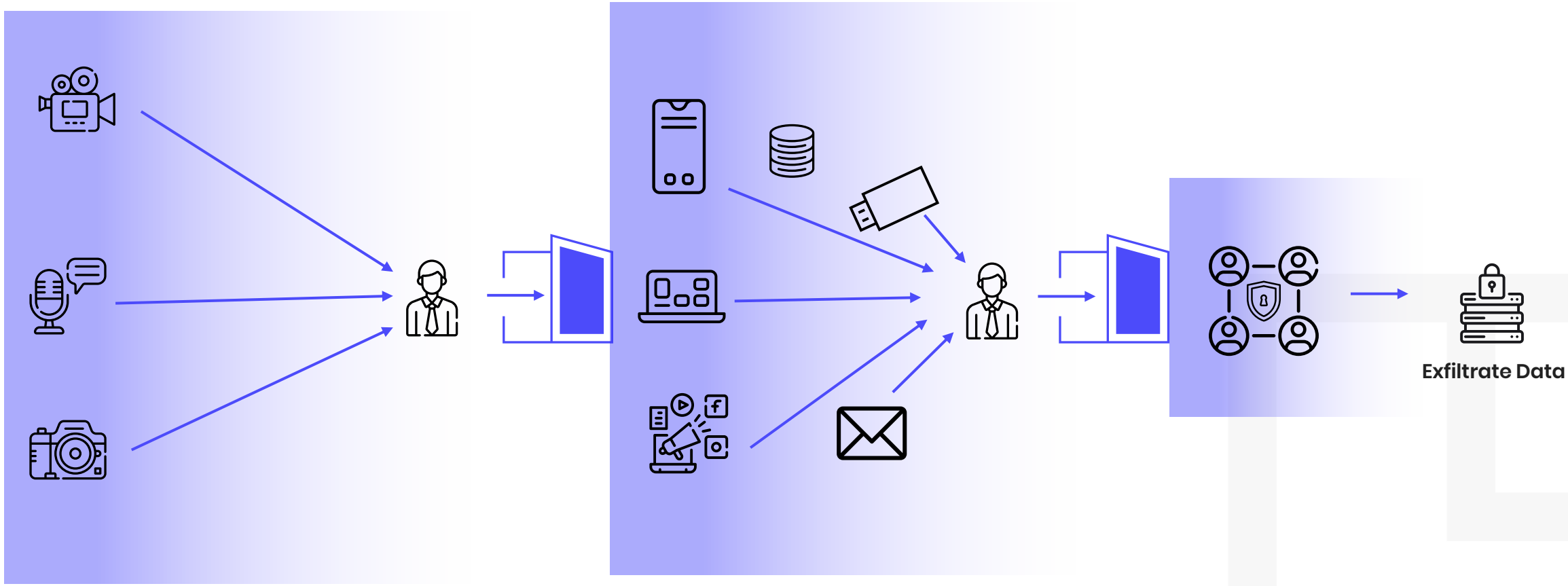
Pivoting from compromised systems and from breached physical security controls all along capturing video, audio and photographic evidence supporting each finding discovered. Data gathered is analyzed to ensure that it is meaningful for meeting the objectives of red team exercise.



Exfiltrate and complete mission

Infopercept

Ultimately, the team aims to exfiltrate data, information or physical assets the target deems critically sensitive. During this phase of Red Team Operation, the team aims to complete the mission and realize the agreed-upon objectives set by the client and Infopercept Security.



About Infopercept

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint

© Infopercept Consulting Pvt. Ltd. 2021

Publisher

H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info

M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

Global Offices

United State of America
+1 516 713 5040

United Kingdom
+44 2035002056

Sri Lanka
+94 702 958 909

Kuwait
+965 6099 1177

India
+91 9898857117

Infopercept