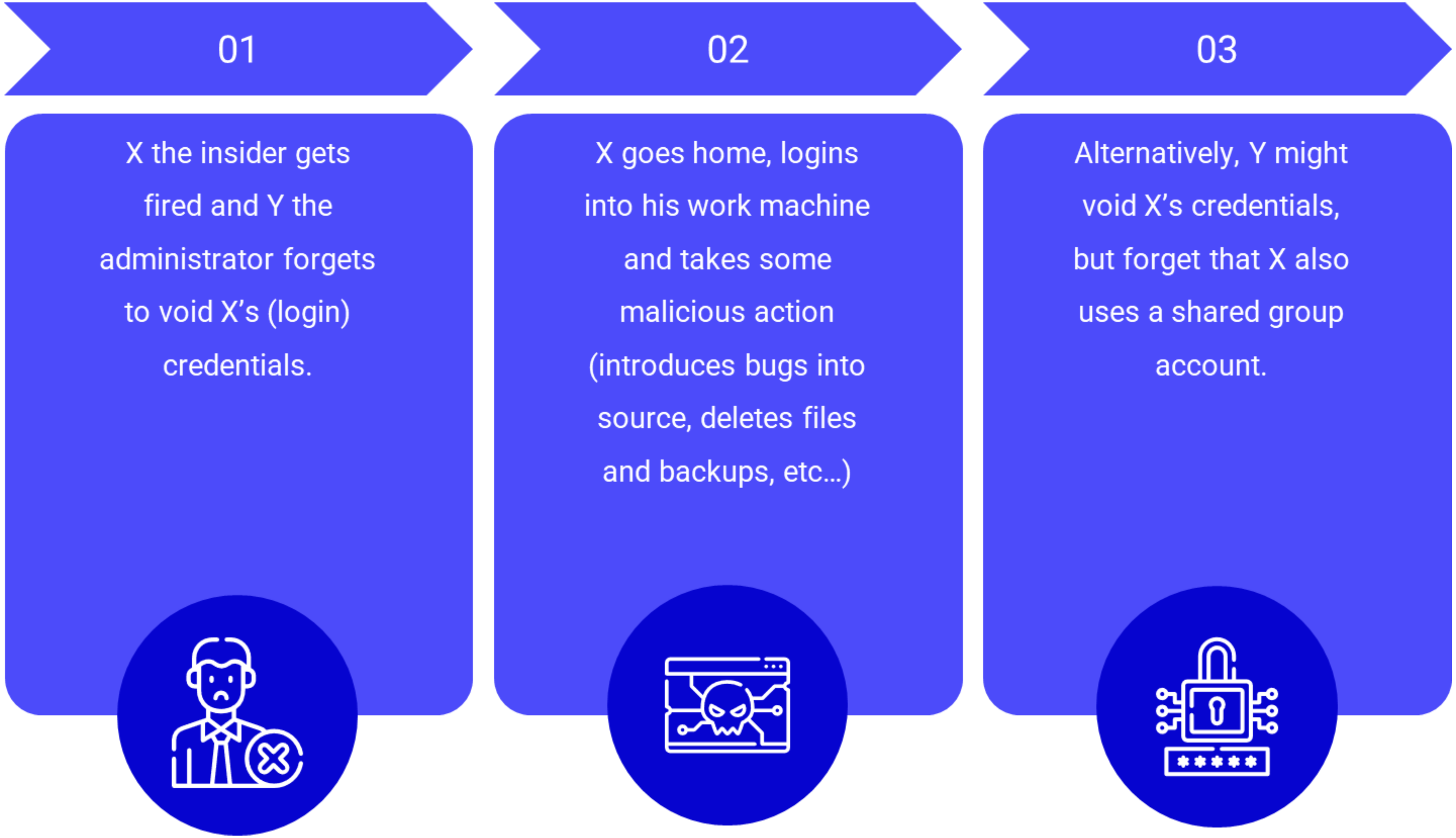
A Discussion of the Insider Threat

Infopercept

INVINSENSE

Example Insider Attack



01

X the insider gets fired and Y the administrator forgets to void X’s (login) credentials.

02

X goes home, logins into his work machine and takes some malicious action (introduces bugs into source, deletes files and backups, etc…)

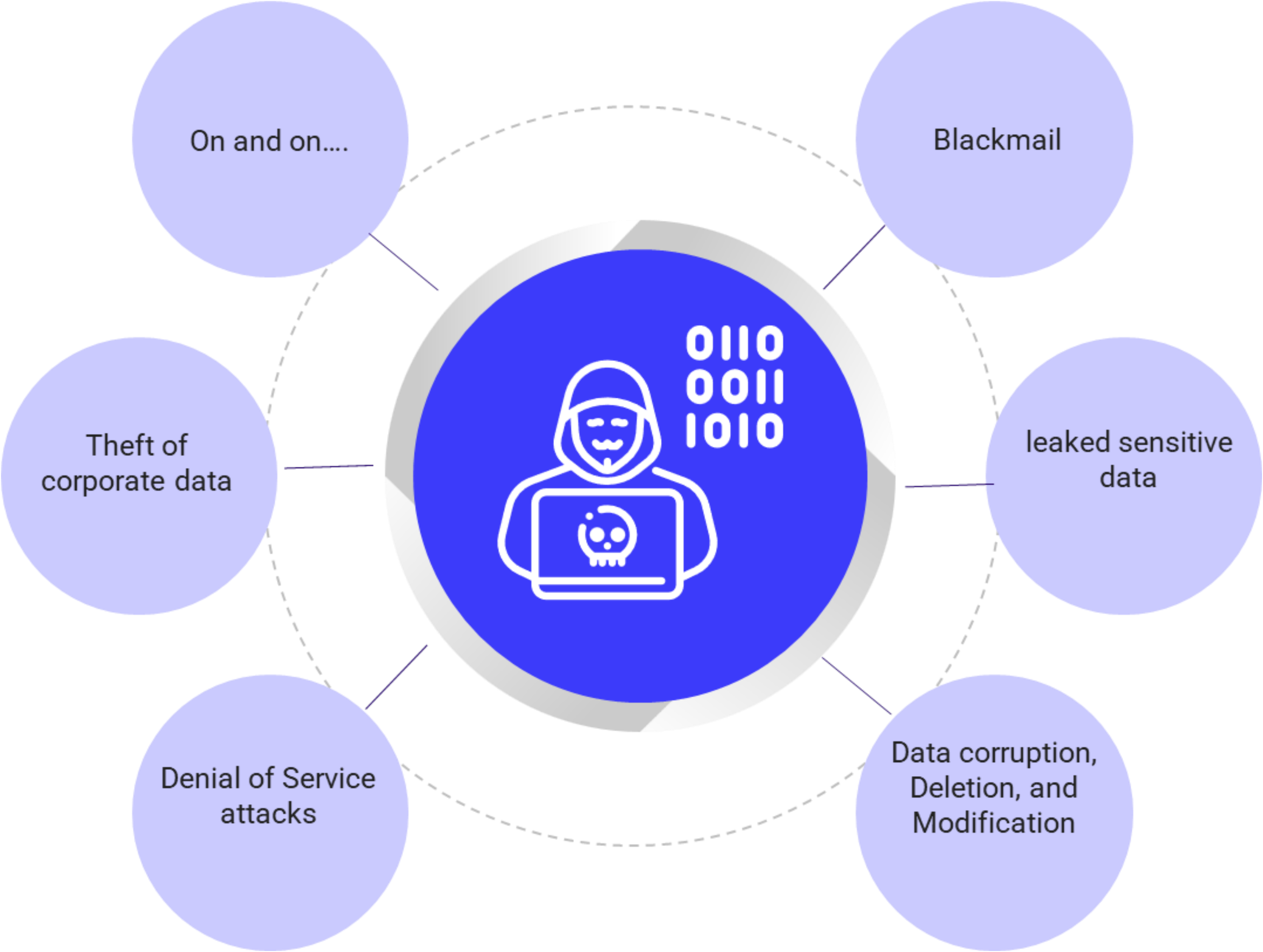
03

Alternatively, Y might void X’s credentials, but forget that X also uses a shared group account.

Proposed Definition

- A malicious insider is an adversary who operates inside the trusted computing base, basically a trusted adversary.
- The insider threat is an adversarial model encompassing all possible malicious insiders.

Example Threats



Statistics

- Attacks
- Insider attacks account for as much as 85% of all computer and Internet related crimes
- 75% of attacks causing at least $20,000 of damage are the direct result of malicious insiders
- Majority of insiders are privileged users and majority of attacks are launched from remote machines

Problem Discussion

- Typical adversarial models ignore the insider threat by assuming the TCB is free of threats
- Insider threat violates this assumption

Prevailing Sentiments (Myths?)

- Current systems are capable of countering the insider threat
- Insider threat is impossible to counter because of the insider's resources and access permissions
- Insider attacks are a social or organizational issue which cannot be countered by technical means

Remediation: Initial Thoughts

- Minimize the size of the TCB to decrease the number of possible insiders
- Distribute trust amongst multiple parties to force collusion
  - Most insiders act alone
- Question trust assumptions made in computing systems
  - Treat the LAN like the WAN
- Others ?

Is the insider threat unavoidable?

- If we define an insider as an adversary inside the TCB, can we ever eliminate the insider threat?
- Perhaps we can only reduce the number of possible insiders or the extent of possible damage?
- Perhaps we should rely on the “lone wolf” nature of insiders and distribute trust?

Partial list of technical test cases performed by Infopercept

- MiTM attacks
- WiFi attacks
- Kerberoasting
- Sniffing
- Network Jamming LLMNR Poisoning
- Phishing Simulation
- Port Scanning
- Smb relay attacks
- Network Discovery

- Token impersonation
- Pass TheHash Attacks
- Enumeration
- USB Drive
- IP/Mac Spoofing
- DNS Spoofing
- Twin WiFi Attacks
- Exploitation

Discussion

- Is the insider threat definition a good one?
- Is the insider an actual threat or just media hype?
- Can/do we build systems that already counter the insider threat?
- Is this worth our time?
- What’s the best paper you could imagine in this area?

ACTUAL THREAT

MEDIA HYPE

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

Imprint

© Infopercept Consulting Pvt. Ltd.

Address

3rd floor, Optionz Complex
Opp. Hotel Regenta,
CG Road, Navrangpura,
Ahmedabad - 380 009,
Gujarat, India.

Contact Info

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

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

Global Office

United State of America
+1 516 713 5040

United Kingdom
+44 2035002056

Sri Lanka
+94 702 958 909

Kuwait

India
+91 9898857117

Infopercept