RADAR SERVICES

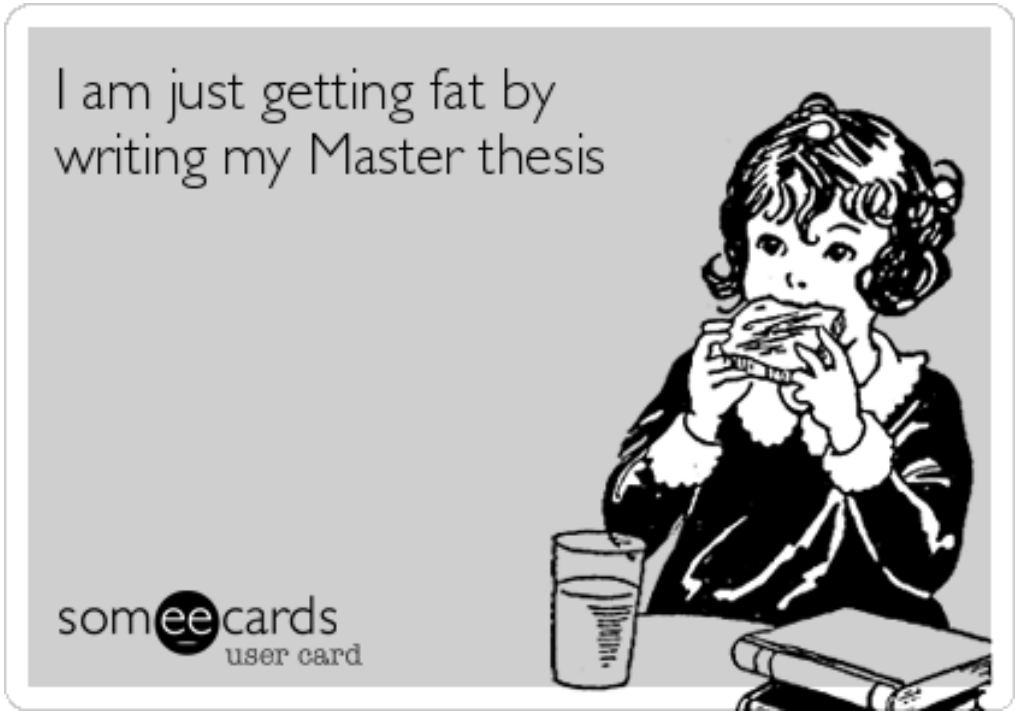
Lure Box

Using Honeytokens for Detecting Cyberattacks

Christoph Malin, IT-SECX 2017

ABOUT ME

- **Academic Career**
  - Bachelor degree in IT Security (FH St. Pölten)
  - Master degree in Information Security (FH St. Pölten)
- **Currently working at**
  - RadarServices in Vienna
    - Intelligence Research & Analysis
    - Security Operations Center (SOC)



WHY IS THIS TOPIC RELEVANT?

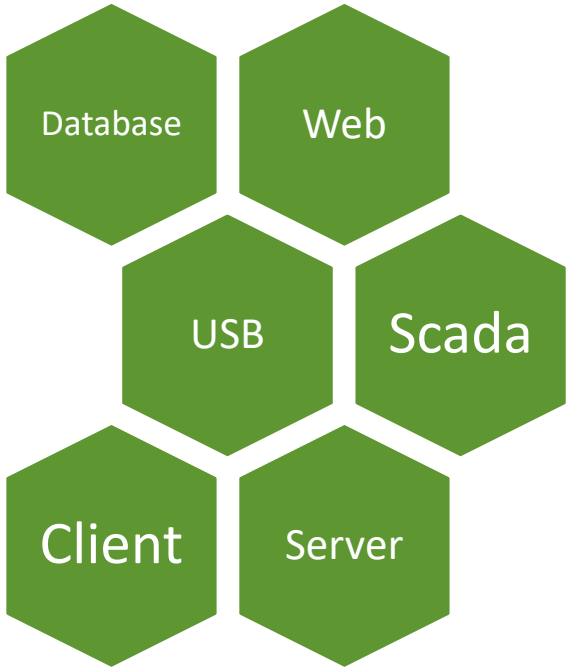
https://haveibeenpwned.com/

- **LinkedIn**
  - 2012: More than 100 million accounts stolen
  - 2012-2016: LinkedIn claimed it were only 6.5 million accounts
  - 2016: LinkedIn found out that it were 100 million accounts

Honeypot & Honeytoken

HONEYPOT

- “A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.” Lance Spitzner, 2002
- More than 200 different honeypot systems available for free https://github.com/paralax/awesome-honeypots



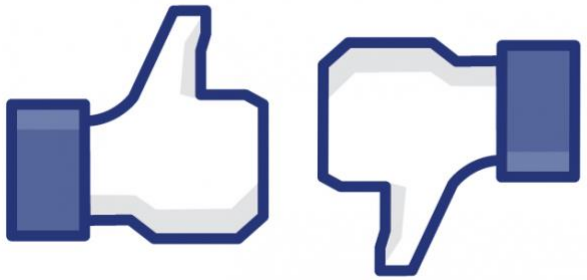
HONEYTOKEN | DEFINITION

- Augusto Paes de Barros coined the term *honeytoken* in 2003
- Also known as *Canarytoken*, *Decoy* and *Lure*
- Lance Spitzner published "**Honeytokens: The other Honeypot**" in 2003

- "**A honeytoken is, a honeypot that is not a computer.**" Lance Spitzner
  - Credit card number
  - PowerPoint presentation
  - Database entry
  - …

HONEYTOKEN | PROS AND CONS

- **Pros**
  - Cheap (they can be created really fast)
  - No license costs
  - Can be placed in various systems



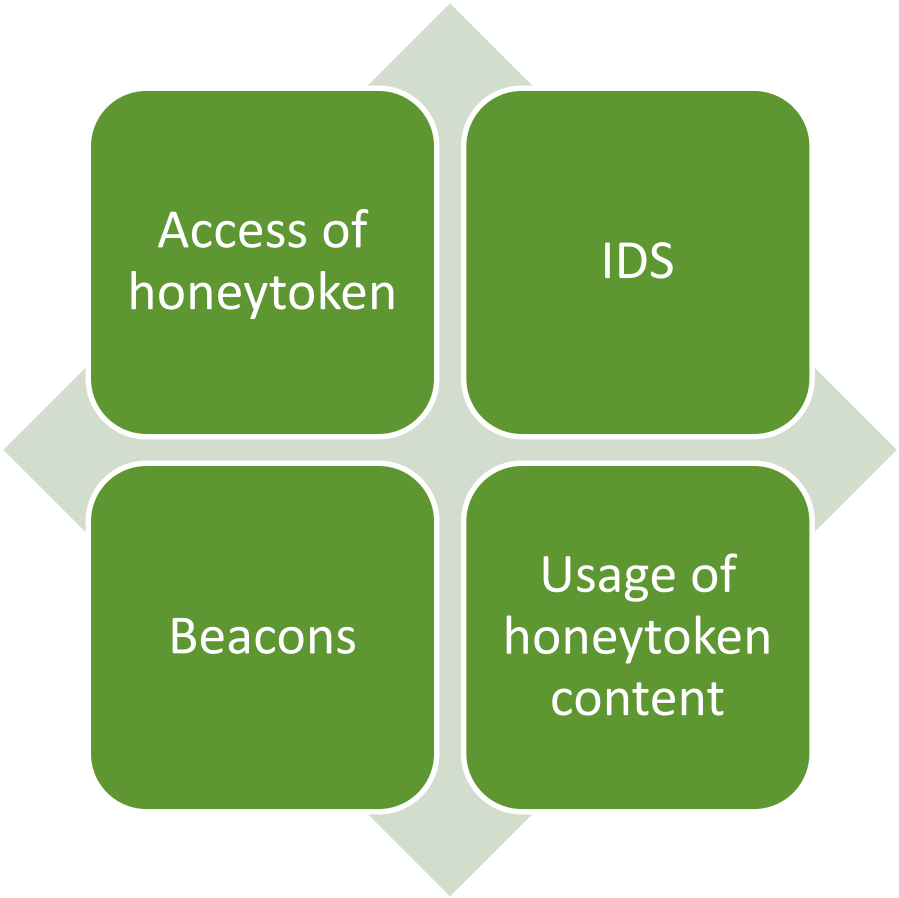
- **Cons**
  - Attack will only be detected when attacker is accessing/using the honeytoken
  - Attacker could detect that he/she accessed a honeytoken

HONEYTOKEN | PROJECTS AND TOOLS

- **Canarytoken** (https://canarytokens.org)
  - Webservice where you can generate honeytokens online.
    You receive a mail when someone accessed the honeytoken.
  - URL tokens, DNS tokens, email tokens, Microsoft Word documents, Adobe PDF documents, SQL Server database, websites and QR codes

- **DCEPT** - Domain Controller Enticing Password Tripwire (https://github.com/secureworks/dcept)
  - Honey credentials are placed in the memory of a windows machine.
  - An alert is generated when the domain controller receives a kerberos packet containing the honey credentials.

HONEYTOKEN | DETECTION MECHANISMS



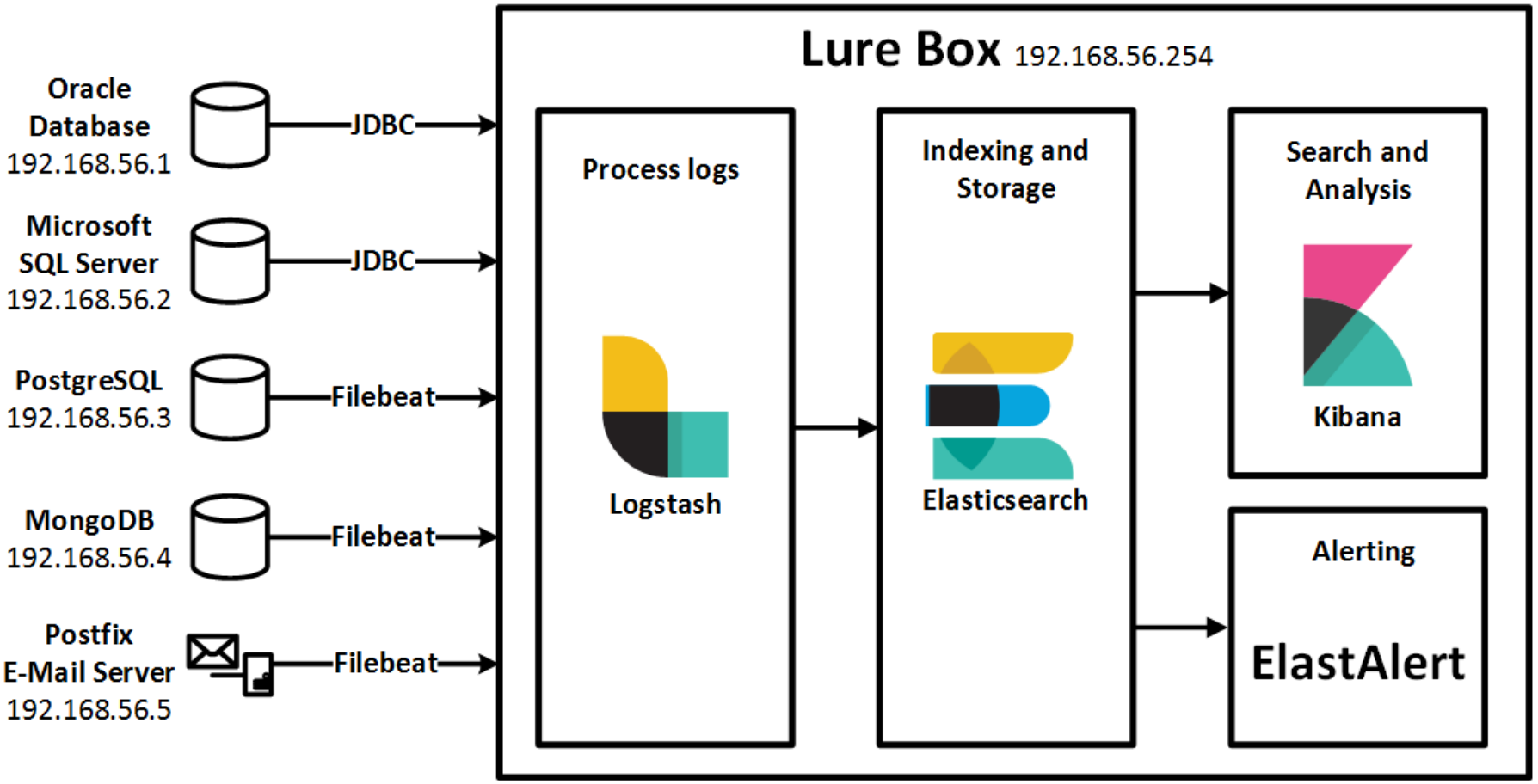
HONEYTOKEN | USAGE SCENARIOS

Files • Documents (.txt, .doc, .xls,.pdf etc.) • Beacon traps • Emails • Logs • Databases • Recent/deleted documents	**Network** • Network table caches poisoning (ARP, DNS, NetBios etc.) • Mounted devices (printers, cameras etc.) • (half) open connection to decoys • Host and ImHost files
Applications • Session apps (SSH, FTD, RDP, clients etc.) • Browsers (history, passwords, bookmarks etc.) • App uninstall information	**Credentials** • Passwords and Hash injections • Windows Credentials Manager • Password Managers

Applying Deception Mechanisms for Detecting Sophisticated Cyber Attacks, TopSpin 2016

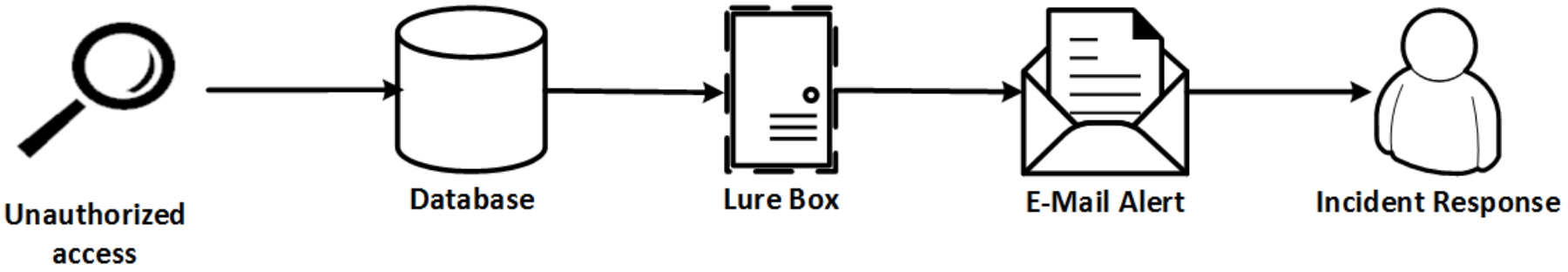
Lure Box

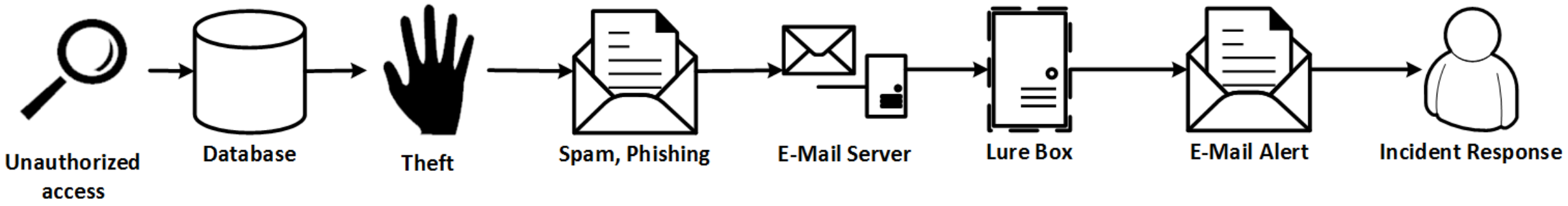
LURE BOX | IMPLEMENTATION



RADAR SERVICES

LURE BOX | EXAMPLE SCENARIO





LURE BOX | DEMO

- **Oracle Database**
  - Salary table is a honeytoken
  - Two employees in employee table are honeytokens

EmployeeID	LastName	FirstName	Birthdate	City
4	Park	Margaret	19.09.1947	Calgary
5	Johnson	Steve	03.03.1965	Calgary

CONCLUSION

- **Lure Box – next steps**
  - Website
  - Creating a collection of use case scenarios
  - Creating a collection of tutorials about auditing configuration
  - Build up an online community
  - Performance tests
  - Research about placement and generation of honeytokens

Q&A

https://github.com/LureBox