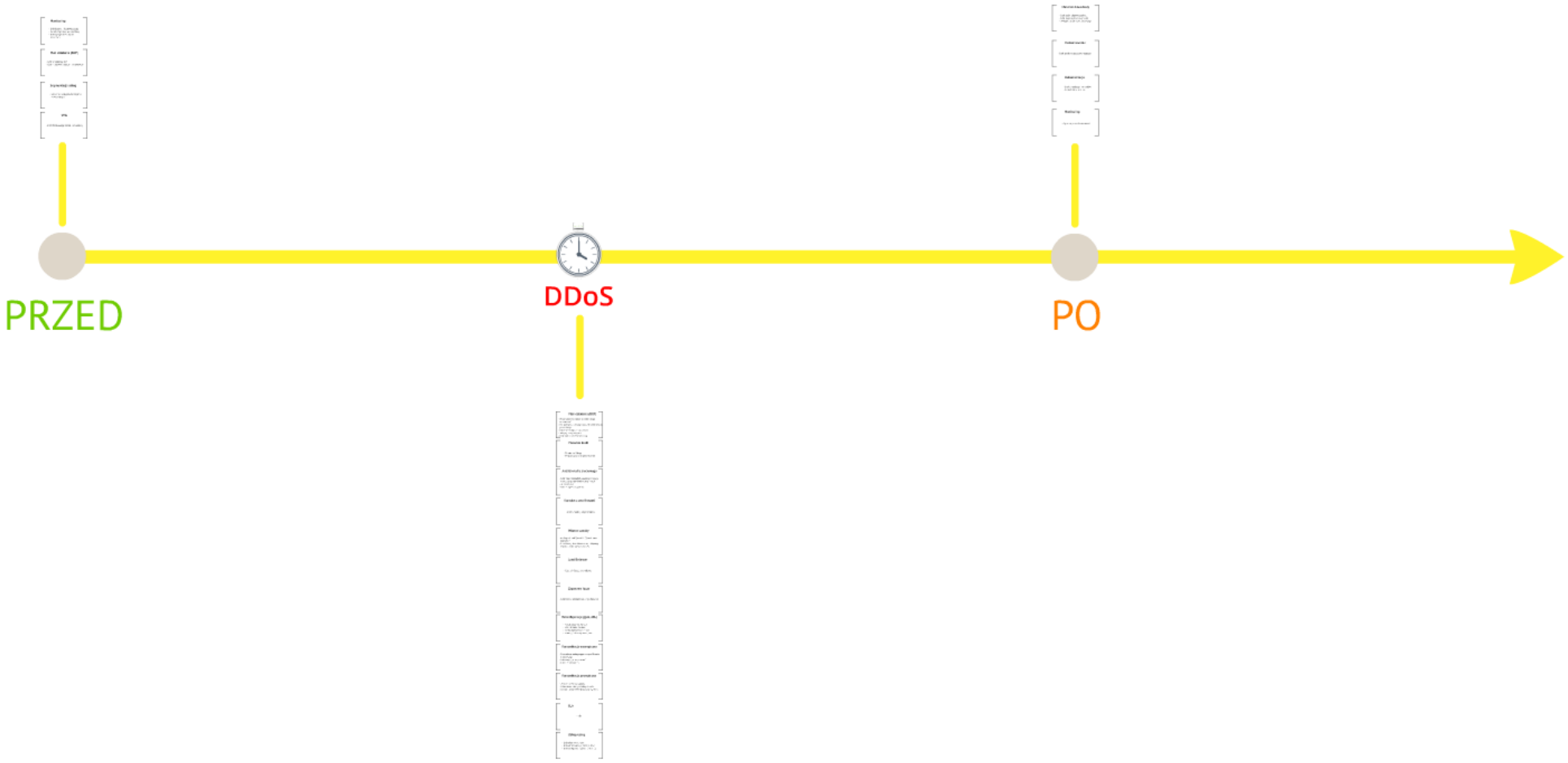

PRZED
DDoS
PO

Borys Łącki

ATAK DDoS – JAK NIE STRACIĆ GŁOWY NA FRONCIE?

SECURITY CASE STUDY 2014

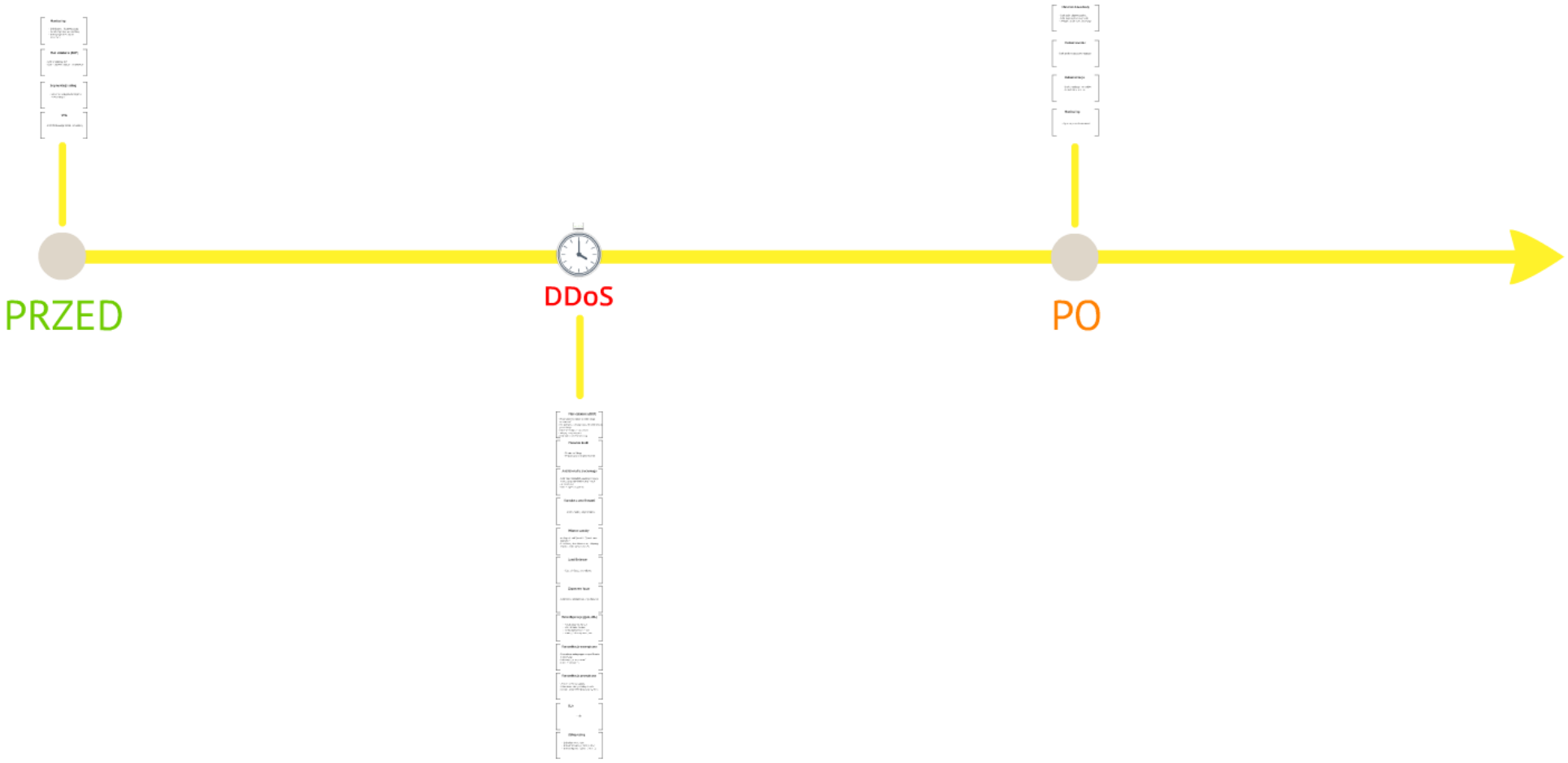
LOGICALTRUST

Naszą misją jest ochrona naszych Klientów przed realnymi stratami finansowymi. Wykorzystując ponad 10 lat doświadczenia, świadczymy usługi z zakresu bezpieczeństwa IT:

- **Testy penetracyjne**
- **Audyty bezpieczeństwa**
- **Szkolenia**
- **Konsultacje**
- **Informatyka śledcza**
- **Aplikacje mobilne**

Borys Łącki

- **SECURE, Atak i Obrona, Internet Security Banking, SecureCON, SEConference, SekIT, ISSA, Open Source Security, PLNOG, (...)**
- **7 lat blogowania o cyberprzestępstwach: www.bothunters.pl**


PRZED
DDoS
PO

Monitoring

- Brak dodanej kluczowej usługi
- Monitoring z sieci wewnętrznej
- Brak oprogramowania na serwerach

Plan działania (BCP)

- Brak aktualizacji BCP
- Brak kluczowych danych kontaktowych

Segmentacja usług

- Serwer dla usług zewnętrznych i wewnętrznych

VPN

- Brak dodatkowego kanału komunikacji

Plan działania (BCP)

- Pracownicy nie wiedzą co robić i kogo informować
- Kto podejmuje decyzje i czy jest upoważniony przez Zarząd
- Klient informuje o problemach
- Wszyscy robią wszystko
- Brak opisu krytyczności usług

Pierwsze kroki

- Brak opisu krytyczności usług

Pierwsze kroki

- Telefon na Policję
- Poszukiwanie cyberprzestępców

Analiza ruchu sieciowego

Analiza ruchu sieciowego

- Brak rozwiązania/dedykowanej maszyny/ konfiguracji/planów/instrukcji w BCP
- Wireshark GUI
- Dane z logów co godzinę

Kontakt z zew. firmami

Kontakt z zew. firmami

- Brak aktualnej listy kontaktów

Własne zasoby

- cat log.txt | awk '{print $4 }' | sort | uniq
  BIG DATA?
- Nieaktualny stan dokumentacji dotyczący fizycznej dostępności serwerów

Load Balancer

Load Balancer

- Działa != Działa prawidłowo

Zapasowe łącze

Zapasowe łącze

- Brak testów przełączania w tryb fail-over

Rekonfiguracja (QoS, ACL)

Rekonfiguracja (QoS, ACL)

- Aktualizacja ACL via CLI
- ACL – IP False Positive
- Skomplikowany QoS = DoS
- Serwery DNS w tej samej sieci

Komunikacja wewnętrzna

- Dziennikarz podszywający się pod Klienta biznesowego
- Informacje „po znajomości”
- E-mail z szantażem

Komunikacja zewnętrzna

Komunikacja zewnętrzna

- *Problem został rozwiązany*
- Różne komunikaty od różnych osób
- Komunikat na WWW (Facebook, Twitter)

SLA

- > 8h

Zakup usług

Zakup usług

- Brak ofert/firm/umów
- Brak infrastruktury (interfejs 10G)
- Brak konfiguracji (wysoki DNS TTL)

Materiał dowodowy

- Brak osoby odpowiedzialnej
- Brak miejsca przechowywania
- Wyłącznie zrzut ruchu sieciowego

Podsumowanie

- Brak spotkania podsumowującego

Dokumentacja

- Brak aktualizacji i wniosków
- Co zadziałało, a co nie

Monitoring

- *Czy to na pewno koniec ataku?*

Dziękuję za uwagę

Borys Łącki
b.lacki@logicaltrust.net

SECURITY CASE STUDY 2014