
LABYRINTH
WITH secure
Kako se zapravo tvrtke brane?
A1 ICT Distribucija

Company M

- Proizvodna tvrtka
- 100+ zaposlenih

- Sigurnosna rješenja:
  - Firewall
  - Windows Defender
  - Zaštita emaila za M365
  - Backup s kritičnih servera

- Menagementu prioritet zadovoljstvo zaposlenih:
  - Dopuštene slabe lozinke
  - Malo ili bez ograničenja dostupa internim sistemima
  - Često korisnici imali admin prava

- Aktivno testirali EDR rješenje

Company M – incident

Početni koraci

Nisu odkrili pravog vektora napada. Najbolja interpretacija logova je pristup putem otvorenog Remote Desktopa na server

Širenje malware po drugih serverima

Širenje malware po radnim stanicama

KRIPTIRANJE

Početak kriptiranja

Na manjem djelu mreže, gdje je bio instaliran EDR počeli su prvi alarmovi

IT ekipa počela gasiti i izolirati uredjaje i ubrzano instalirati EDR na sve ostale radne stanice i servere

ČIŠĆENJE

S korištenjem EDR i brze reakcije uspjeli su identificirati vse uredjaje s malware-om

EPILOG

Menagement dozvolio je investiciju u dodatna rješenja: sad koriste puni SOC ukupno sa XDR

Company t

Ne znamo koje alate i koji korisniki su bili kompromitirani.

Prvi indici o problemima tek kad se usporio server.

Nemamo podataka o početku, koje bi koristili za promjenu sigurnosnih pravila na svim rješenjima.

Širenje malware po drugih serverima

Širenje malware po radnim stanicama

KRIPTIRANJE

Početak kriptiranja

Na manjem djelu mreže, gdje je bio instaliran EDR počeli su prvi alarmovi

IT ekipa počela gasiti i izolirati uredjaje i ubrza instalirati EDR n sve ostale radne stanice i servere

Prvo su trebali imati velike probleme, kako bi promijenili to što su znali već prije.

reakcije uspjeli su identificirati vse uredjaje s malware-om

ILOG

nagement dozvolio investiciju u dodatna rješenja: sad koriste puni SOC ukupno sa XDR

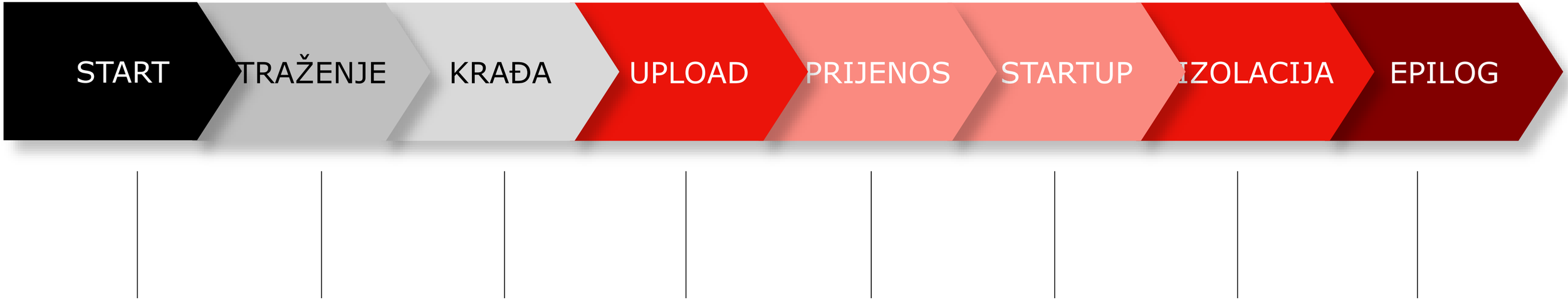
Company K

- Usluge
- 200+ zaposlenih

- Sigurnosna rješenja:
  - Firewall
  - Zaštita emaila
  - Backup
  - Napredna zaštita radnih stanica s EDR
  - Kontrola mreže s postavljenim mamcima
  - Ograničena prava korisnika
  - Redoviti pen-testovi
  - Edukacija zaposlenih na području cyber security higiene

- Menagement podržava investicije u cyber security

Company K – incident



midjourney.exe
Korisnik pokrenuo tool za AI kreaciju fotografija kako bi koristio WebAPP

Pokrenuti proces je skupio vse informacije o korisniku, sistemu, mreži i dostupnim serverima.

Proces je iz memory uzeo sve lozinke i uradio eksport lozinka iz svih browsera

Credential theft

Sve ukupno poslano je na javno dostupne web servise (twitter / X, reddit i pastebin)

Iz tih istih web servisa preneseni su komadi novog fajla, koji je kreirao novi malware i novi proces

Taj novi fajl je stavljen u startup folder za automatsko pokretanje

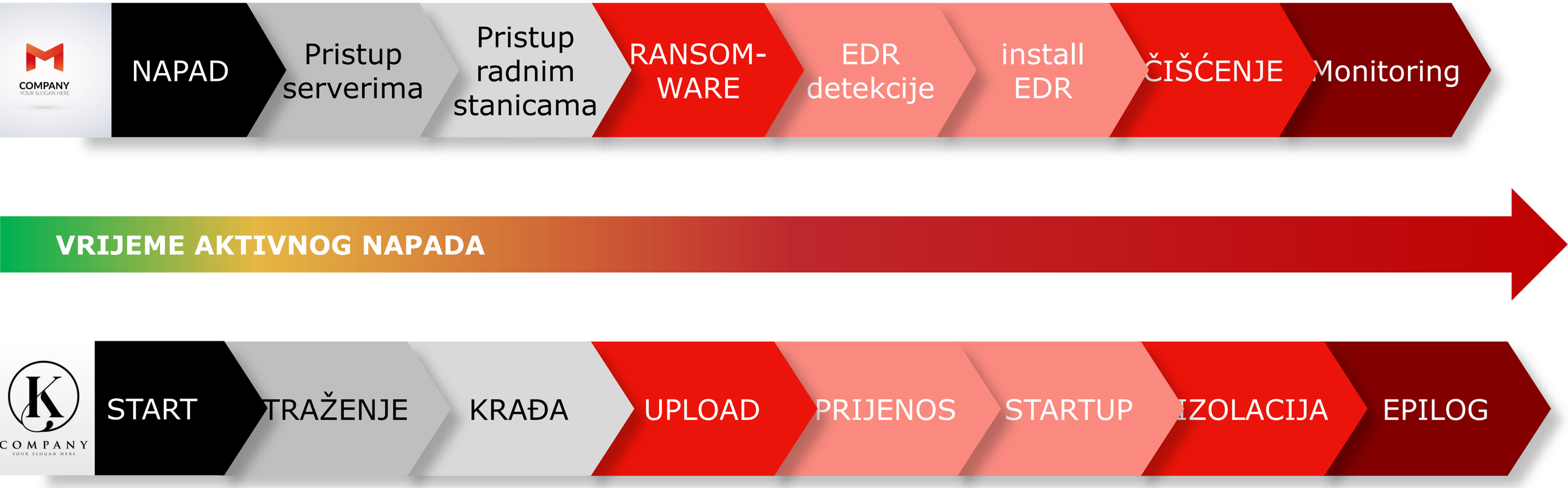
Reakcija EDR

EDR je uz analizu eventa sam diago „SEVERE" alarm i pokrenuo automatski response - IZOLACIJA

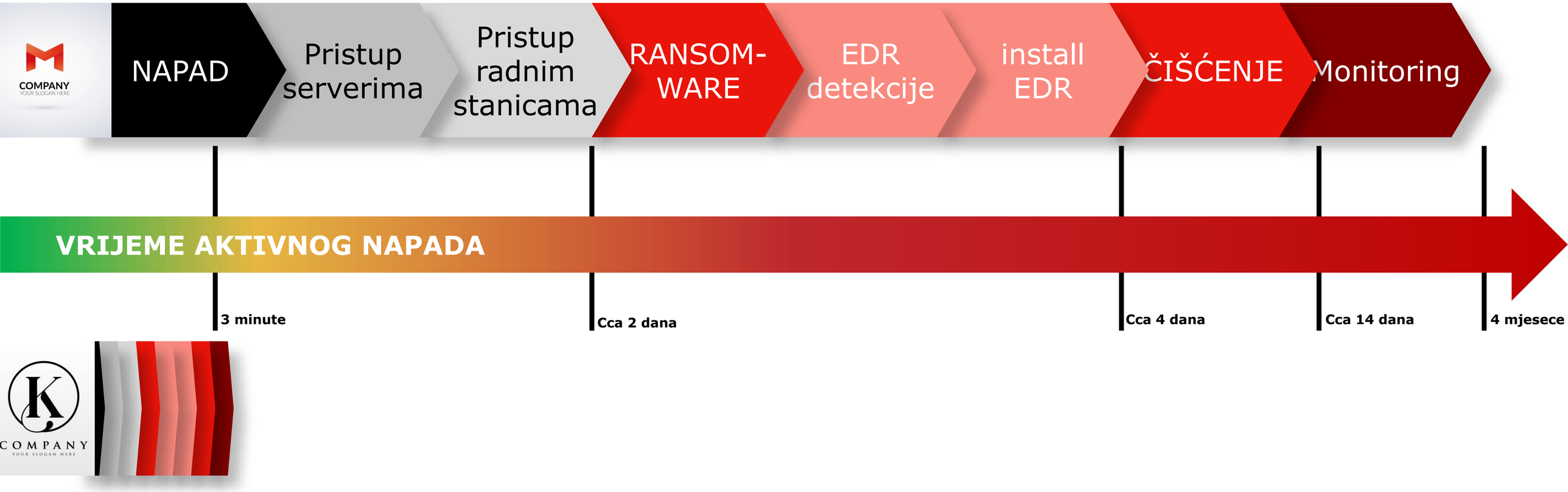
Šteta

Šteta je minimalna – ograničena na promjenu ukradenih lozinka.

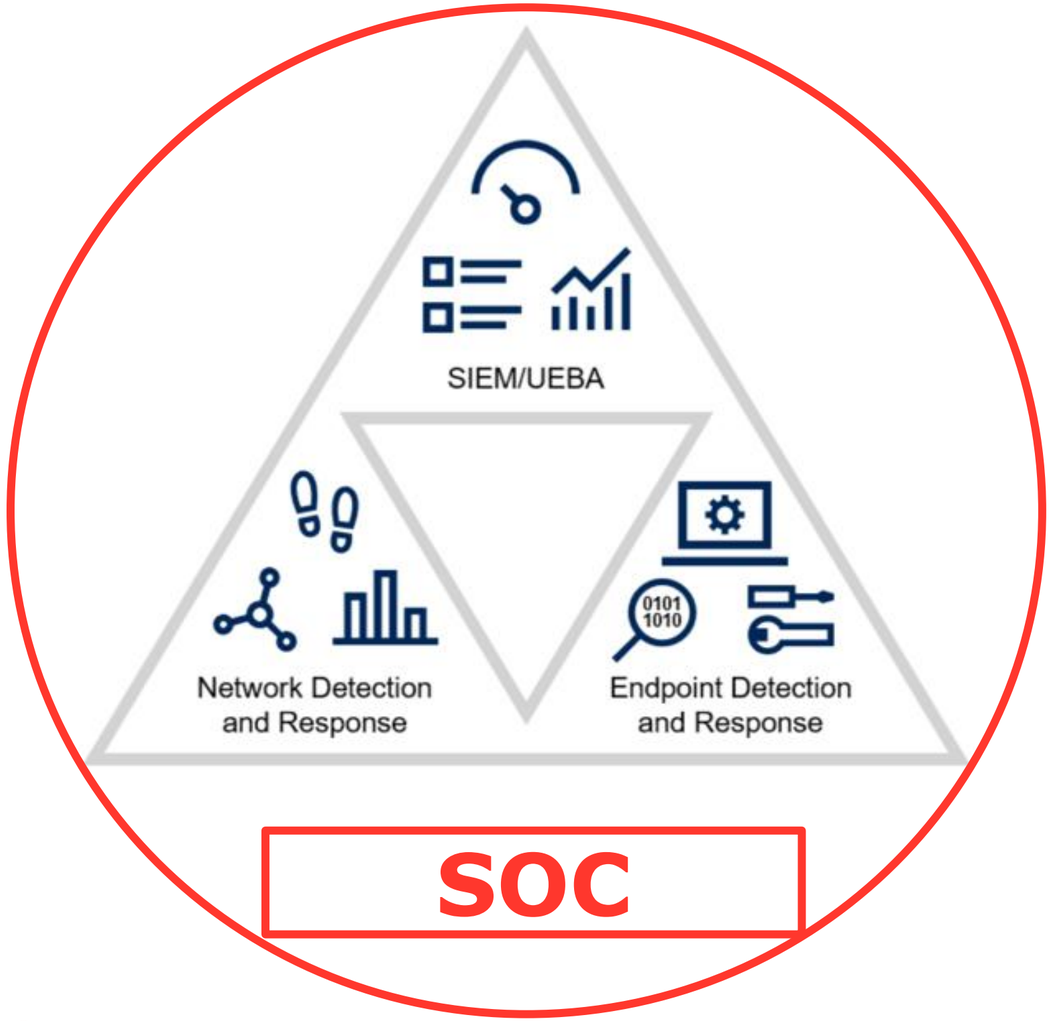
Usporedba incidenta



Usporedba incidenta



Ključ je u vidljivosti

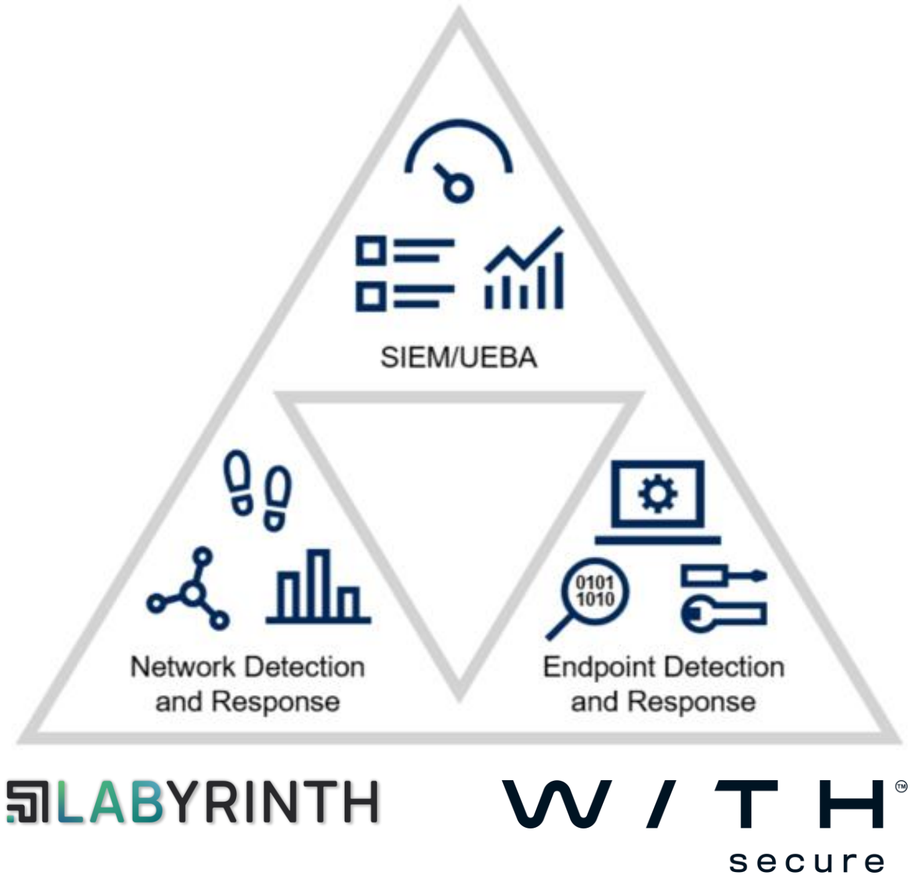


Detekcije na mreži
Identifikacija sumnjivih mrežnih aktivnosti s monitoringom prometa za unutarnje i vanjske prijetnje

Detekcije na radnim stanicama i serverima
Praćenje pokretanja procesa i otvaranje fajlove, aktivacije mrežnih konekcija, aktivnosti u memoriji sistema

SIEM/UEBA:
Skupljanje, analiza i korelacija informacija i aktivnosti svih sistema (sigurnost, infrastruktura, korisnici)

Ključ je u vidljivosti



Detekcije na mreži
Identifikacija sumnjivih mrežnih aktivnosti s monitoringom prometa za unutarnje i vanjske prijetnje

Detekcije na radnim stanicama i serverima
Praćenje pokretanja procesa i otvaranje fajlove, aktivacije mrežnih konekcija, aktivnosti u memoriji sistema

SIEM/UEBA:
Skupljanje, analiza i korelacija informacija i aktivnosti svih sistema (sigurnost, infrastruktura, korisnici)