

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Purple Teaming

Изпълняваме известни техники на нападатели по контролиран начин, рамо до рамо с вашите защитници, за да измерим какво точно засичат инструментите ви — и след това ги настройваме, докато започнат да засичат повече. Разработване на механизми за откриване, доказан срещу реално поведение.

ПОДХОДЯЩО ЗА	Екипи със SOC, EDR или SIEM, които искат да валидират и подобрят откриването
ПОЛУЧАВАТЕ	Матрица на покритието по ATT&CK; пропуски в откриването, настроени правила
ОБХВАЩА	Валидиране на откриването с ATT&CK;

Първо измерване, после подобрение

Да закупите инструменти за откриване не е същото като да откривате. Изпълняваме техники от матрицата на MITRE ATT&CK; докато екипът ви наблюдава, записваме какво се е задействало и какво не, и работим с вас, за да затворим пропуските — след което изпълняваме отново, за да докажем подобрението.

Това е най-бързият начин констатация на red team („вашият SOC пропусна това“) да се превърне в конкретно, изпробвано правило за откриване.

Какво обхващаме

- Изпълнение на техники от MITRE ATT&CK;
- Валидиране на откриването и известяването
- Преглед на покритието на EDR, SIEM и SOAR
- Разработване и настройка на правила за откриване
- Валидиране на процеса по реакция
- Докладване на покритието и повторно изпълнение

Как протича

- Планиране — Договаряме техниките и критериите за успех.
- Съвместно изпълнение — Изпълняваме техниките на живо заедно с вашите защитници.
- Анализ — Съотнасяме засеченото към ATT&CK; и откриваме пропуските.
- Настройка и повторно изпълнение — Подобряваме откриването и доказваме подобрението.

Какво получавате

- Матрица на покритието по ATT&CK; — Какво засичат защитите ви, техника по техника.
- Пропуски в откриването — Точно къде липсва телеметрия или известяване.
- Настроени правила за откриване — Нови и подобрени правила, разработени с вашия екип.
- Резултати от повторното изпълнение — Доказателство, че пропуските са затворени.

Методологии и стандарти, на които се опираме

MITRE ATT&CK; · Atomic Red Team · MITRE D3FEND · Правила за откриване SIGMA · Detection-as-code · MITRE ATT&CK; Navigator

Старши тестери. Доказателства за всяка констатация. Включен повторен тест. Минимум пет дни тестване. Обхват и примерни доклади — pxlsec.com/bg/services/purple-teaming.