الفوائد:تحديد الأولويات بذكاء: يساعد المحللين في التركيز على المؤشرات التي تُحدث أكبر ألم للمهاجم (مثل TTPs بدلاً من تجزئة الملفات).تفكير موجه ضد الخصم: يحول نهج الدفاع من مجرد مراقبة مؤشرات تقنية إلى فهم سلوك الخصم وتحركاته.إطار لصيد التهديدات: يوفر خريطة للمحققين لاتباع نهج الكشف المستدام وطويل الأمد.تحسين استخدام الموارد: يوجه الجهود نحو الكشف عن المؤشرات الأعلى قيمةً،