Hunters / vmware Carbon Black Solution Brief

Connect Threat Detection and Response Across the Entire Attack Surface

SOC teams today are facing an unprecedented challenge at sifting through the tremendous amount of security data generated by the variety of tools living in silos and the lack of automation of repetitive tasks, preventing them to scale and focus on remediating threats in time.

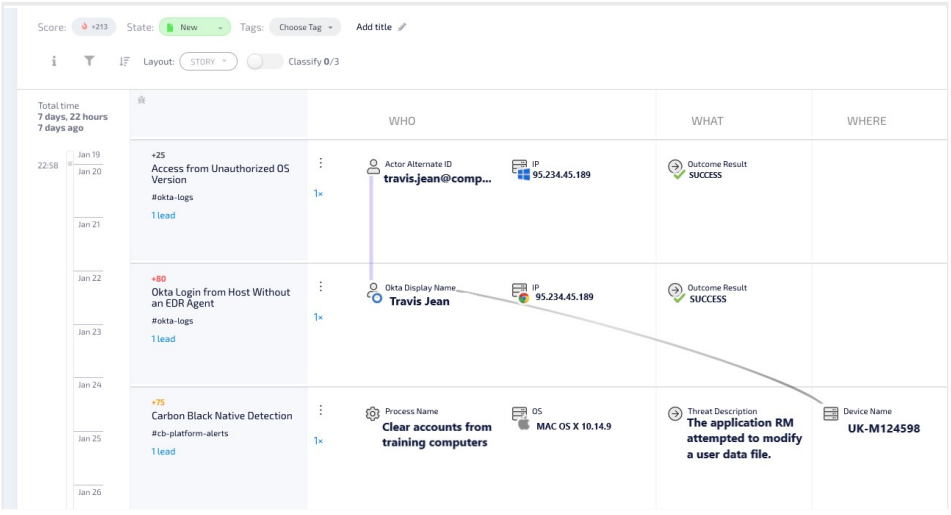
Market-leading solutions like VMware Carbon Black have enabled organizations to monitor and respond to threats thanks to the rich endpoint telemetry generated by the EDR solutions. Using Hunters' open XDR platform, customers can now scale their security operations with high-fidelity Attack Stories across surfaces, automation of repetitive tasks like cross-product investigations and looking at one single interface that connects data from EDR with other existing security and organizational tools, eventually making it safer to navigate the threat landscape and close the gaps with the attackers.

Your security team has invested in the right tools and talent over the years. Now it's time to take those to the next stage of threat detection and response.

THE SOLUTION

Hunters is an open, agile XDR solution that harnesses adversary expertise and machine learning to proactively detect and respond to threats across the entire attack surface - on endpoint, cloud, network, identity, and email. SaaS-delivered, Hunters seamlessly ingests petabytes of organizational data and security telemetry to search for threat signals, and automatically analyze, score and correlate them with existing alerts from Carbon Black. Using a proprietary Knowledge Graph, Hunters XDR provides analysts with detailed attack stories and context for effective investigation and rapid response. It provides rich insights for containment, and streamlines response by integrating with SOAR and workflow tools.

With Hunters XDR, organizations can easily go from EDR to XDR, achieving higher detection efficacy with their existing IT stack while significantly reducing SOC triage and MTTR.



An Attack Story showing a successful Okta login to an employee account and a week later a detection on his personal device. A week later there is an endpoint alert as seen by the Carbon Black detection. After a series of automatic investigations by Hunters, the Okta logs and the Carbon Black alert are connected, indicating a credential theft and an attempt to compromise the endpoint a week later

BENEFITS

Seamlessly transform your existing Carbon Black endpoint telemetry into an XDR

Expedite MTTD and MTTR with data-proof Attack Stories

Detect attacks that bypass existing security controls, with cohesive threat detection across your entire IT environment (cloud, network, endpoint, identity and email)

Deploy Hunters XDR in minutes with just a few clicks, no agents or pre-configuration required

Use Hunters alignment with the MITRE ATT&CK framework to identify your coverage and address blind spots

HOW IT WORKS

1. **22-23.-a**7OEJC ?HKQ@ ?KJJA?PKNO PK LELA EJPK ATEOPEJC OA?QNEPU PKKHOη KN @ENA?PHU ?KJJA?PEJC PK 5+ ' / η * QJPANO : &4 ?KHHA?PO HKCOη ARAJPO =J@ PAHA I APNU BNK I %=N>KJ $H=?G =O SAHH =O KPDAN @KVAJO KB @=P= OKQN?AO KJ LNA I EOAO =J@ EJ PDA ?HKQ@η EJ?HQ@EJC ' &4Oη 0&4Oη ?HKQ@ OANRE?A LNKRE@ANOη BENAS=HHOη +@AJPEPU =J@ #??AOO I =J=CA I AJP PKKHOη =J@ I KNAN

2. &APA?PEKJ ' JCEJAθ * QJPANO : &4 ATPN=?PO PDNA=P OECJ=HO =J@ =HANPO BNK I LAP=>UPAO KB ATEOPEJC OA?QNEPU @=P= QOEJC = OPNA= I LNK?AOOEJC =J=HUPE?O PA?DJKHKCUN +P AJ=>HAO JA=N NA=HBPE I A LNK?AOOEJC =J@ ?K I LHAT =J=HUPE?ON 6DNA=P OECJ=H ATPN=?PEKJ EO CQE@A@ >U * QJPANOų 6625>=OA@ =PP=?G EJPAH SDE?D EO =HOK I =LLA@ KJPK = / +64 ' #66 I· % - PA?DJEMQAN

3. &=P= 4ALNAOAJP=PEKJ KJ = / QHPEБ&E I AJOEKJ=H) N=LDθ 6DA PAHA I APNU ?KHA?PA@ BNK I R=NEKQO +6 =J@ OA?QNEPU PKKHO EO ABBA?PERAHU ?KJJA?PA@ PKCAPDAN KJ = LNKLNEAP=NU - JKSHA@CA) N=LDη = OPNQ?PQNA@ NALNAOAJP=PEKJ KB =HH PDA OQOLE?EKQO >AD=REKQNOη =HH PDA AJPEPEAO EJ PDA JAPSKNGη =J@ PDA NAH=PEKJODELO >APSAAJ PDA I N

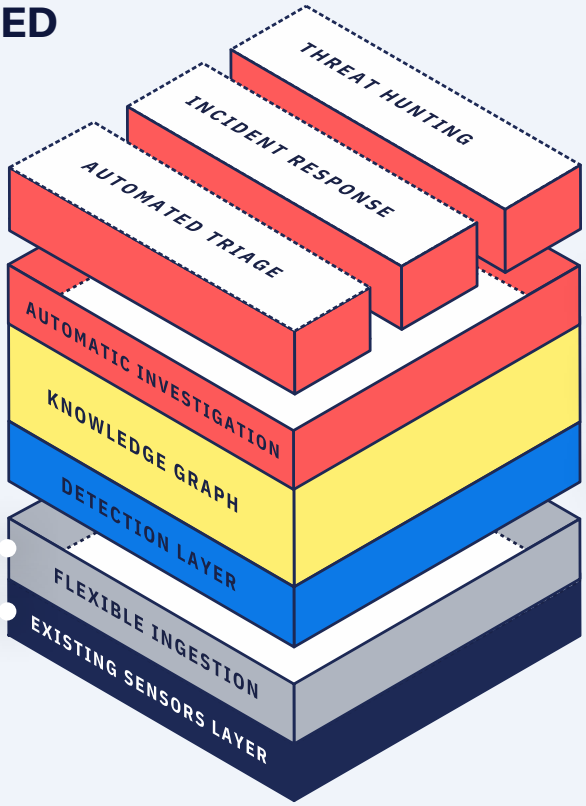
4. #QP K I =PE? +JRAOPEC=PEKJθ +J KN@AN PK QJ@ANOP=J@ SA=G PDNA=P OECJ=HO =J@ =H ANPOη * QJPANO NQJO =QPK I =PE? EJRAOPEC=PEKJON +P BAP?DAO =HH NAHAR=JP EJBKN I =PEKJ =OOK?E=PA@ SEPD PDKOAη EJ?HQ@EJC BA=PQNAO =J@ AJPEPEAO PD=P SANA EJRKHRA@ EJ = OLA?EBE? OQOLE?EKQO =?PEREPUη =J@ =QPK I =PE?=HHU AJNE?DAO PDA I SEPD BQNPDAN ?KJPATPN

5. 5?KNEJC =J@ 2NEKNEPEV=PEKJθ 1 J?A PDANA EO AJKQCD ?KJPATP =NKQJ@ PDNA=P OECJ=HO =J@ =HANPOη * QJPANO : &4 HARAN=CAO / . PK O?KNA PDA I BNK I ň PK ˈnňňη =HHKSEJC BKN =J A=OU LNEKNEPEV=PEKJ =J@ MQE?G PNE=CAN

6. %NKOOБ5QNB=?A %KNNAH=PEKJθ * QJPANO QOAO QJOQLANREOA@ HA=NJEJC PK ?KNNAH=PA OECJ= HO =J@ =HANPO =?NKOO @EOL=N=PA =NA=O KB OQOLE?EKQO =?PEREPU EJ PDA) N=LD ŤAŅCŅη OQOLA?PA@ LDEODEJC A I =EH BKHHKSA@ >U I =HS=NA @KSJHK=@O KJ C=PAS=U =J@ ' &4ťη =J@ OQNB=?A =?PEKJ=>HA #PP=?G 5PKNEAO SDE?D EJ?HQ@A BQHH =PP=?G OQ I I =NU =J@ KQPHEJAN

7. **Response and Remediation:** 5PNA= I HEJA @APA?PEKJ =J@ NAOLKJOA >U AO?=H=PEJC #PP=?G 5PKNEAO EJPK 5 1 #4 PKKHO =J@ KPDAN ATEOPEJC SKNGBHKSOη AJ=>HEJC NAOLKJOA =QPK I =PEKJ =J@ NA@Q?EJC =PP=?GANOų @SAHH PE I AN

KNOWLEDGE - POWERED XDR



Security Data Lake
Cloud Storage, SIEM, Cloud Connectors

Cb

EDR, Identity, Email, Cloud, Network and more

API Access

Hunters Portal

Watch a Hunters XDR demo

Hunters