Sommario: Documenti TAC su FirePOWER Service, FireSIGHT System e AMP

Sommario

Documenti TAC sul sistema FireSIGHT e Firepower

Aggiornamento software e sicurezza, re-imaging, migrazione e installazione

- Tipi di file di aggiornamento che possono essere installati su un sistema FireSIGHT
- Comprendere le nuove terminologie dei sistemi FireSIGHT dopo una migrazione e un aggiornamento dalla versione 4.10.x alla 5.x
- Installazione e configurazione di un modulo servizi FirePOWER su una piattaforma ASA
- Installazione dei servizi FirePOWER (SFR) sull'appliance ASA 5585-X Modulo hardware
- Installazione di FireSIGHT Management Center su VMware ESXi
- Ricreare un'immagine di Sourcefire Defense Center e di un'appliance FirePOWER
- Errore di aggiornamento download automatico su un centro di gestione FireSIGHT
- Linee guida per il download dei dati da Firepower Management Center ai dispositivi gestiti
- Configurazione dei servizi Firepower su un dispositivo ISR con un blade UCS-E

Licenza e configurazione iniziale di base

- Confronto delle licenze per le funzionalità sui sistemi FireSIGHT
- Caratteristiche e capacità supportate di vari modelli hardware del sistema FireSIGHT
- Fasi di configurazione iniziale dei sistemi FireSIGHT
- Registrazione di un dispositivo con un centro di gestione FireSIGHT
- Configurazione di un router virtuale su un sistema FireSIGHT
- Gestione del modulo SFR su tunnel VPN senza switch LAN
- Ottenere la chiave di licenza per un dispositivo Firepower e un modulo di servizio Firepower

Vulnerabilità e copertura delle regole, analisi di eventi e file

- Scarica dati pacchetto (file PCAP) tramite interfaccia utente Web
- Procedure di acquisizione dei pacchetti su appliance Sourcefire FirePOWER e NGIPS Virtual Appliance
- Opzioni per ridurre gli eventi di intrusione falsi positivi
- Regole personalizzate di snort locale su un sistema FireSIGHT

Rilevamento e prevenzione delle intrusioni (IDS/IPS), motore ad immersione

- Determinazione dello stato predefinito per una regola di Sourcefire fornita in un criterio di intrusione
- Metriche utilizzate per determinare le regole predefinite in un criterio di base
- Configurazione della variabile SNORT_BPF su un centro difesa
- Ispezione del traffico aggregato di collegamento da parte di Sourcefire FirePOWER e appliance virtuali
- Abilitare il preprocessore di normalizzazione in linea e comprendere l'ispezione pre-ACK e

post-ACK
- Raccolta dei file principali da un'appliance FirePOWER
- Configurazione di una regola di accettazione su un sistema FireSIGHT
- Esclusione dei messaggi EIGRP, OSPF e BGP dalla funzione Firepower Intrusion Inspection
- Elaborazione di una sessione di grandi dimensioni a flusso singolo (flusso elefante) da parte dei servizi Firepower

Security Intelligence, geolocalizzazione e filtro URL

- Esempio di configurazione del filtro URL su un sistema FireSIGHT
- Impossibile scaricare o aggiornare il feed di Security Intelligence
- L'indirizzo IP è bloccato o inserito nella blacklist dall'intelligence di sicurezza di un sistema FireSIGHT
- Risoluzione dei problemi relativi al filtro URL su un sistema FireSIGHT

Controllo delle applicazioni, VDB, individuazione della rete

- FireSIGHT può identificare un host in modo errato o contrassegnare un evento come in sospeso o sconosciuto

Regola di controllo di accesso/firewall

- Gli eventi di connessione sembrano scomparire dal centro di gestione FireSIGHT

Interfaccia utente (GUI/CLI), accesso utente e autenticazione

- Integrazione del sistema FireSIGHT con ISE per l'autenticazione utente RADIUS
- Integrazione del sistema FireSIGHT con ACS 5.x per l'autenticazione utente RADIUS
- Reimpostazione della password dell'utente amministratore sui sistemi FireSIGHT
- Verifica dell'oggetto di autenticazione sul sistema FireSIGHT per l'autenticazione AD Microsoft su SSL/TLS
- Identificare gli attributi dell'oggetto LDAP di Active Directory per la configurazione dell'oggetto di autenticazione
- Configurazione dell'oggetto di autenticazione LDAP sul sistema FireSIGHT
- Verificare LDAP su SSL/TLS (LDAPS) e certificato CA utilizzando Ldp.exe

Utilizzo di CPU e memoria, prestazioni di rete e di sistema

- Istruzioni per la profilatura delle regole sul sistema FireSIGHT
- Raccolta delle statistiche delle prestazioni mediante l'opzione "Performance Monitor" (Monitor delle prestazioni) da 1 secondo
- Raccolta di dati da un sistema FireSIGHT quando una rete incontra problemi di latenza
- Risoluzione dei problemi di eliminazione dei pacchetti a causa di MTU più alta (pacchetto di sovradimensionamento)

Amministrazione e manutenzione del sistema

- Riavviare i processi su un sistema FireSIGHT e un servizio FirePOWER senza riavviare
- Procedure di generazione file di Sourcefire Appliance
- Risoluzione dei problemi con Network Time Protocol (NTP) sui sistemi FireSIGHT
- Risoluzione dei problemi di utilizzo eccessivo del disco sull'appliance Sourcefire
- Configurazione dello stack sui dispositivi Cisco Firepower serie 8000
- Configurazione del clustering sui dispositivi Cisco FirePOWER serie 7000 e 8000

Funzionamento hardware

- Avvisi di stato dall'unità di alimentazione del sistema FireSIGHT
- Risoluzione di un problema con la gestione Lights-Out (LOM) su un centro di gestione

FireSIGHT o un'appliance FirePOWER
- Il sistema FireSIGHT restituisce il messaggio "Errore di input/output"
- Un accessorio FirePOWER si blocca dopo un tentativo di avvio in modalità utente singolo
- Risoluzione dei problemi relativi alle ventole su un sistema FireSIGHT
- Eseguire test diagnostici dal pannello LCD di un accessorio FirePOWER
- Inserire e rimuovere un modulo di rete (NetMod) su un'appliance FirePOWER serie 8000
- Identificazione dei problemi delle schede Network Flow Engine negli accessori Sourcefire FirePOWER serie 7000 e 8000
- Problemi comuni relativi al kit rail per appliance FirePOWER serie 8000
- Istruzioni per l'installazione del kit di guide dell'appliance Firepower serie 7000
- Un modello FireSIGHT Management Center FS4000 può attivare un avviso di stato "Danneggiato dal disco"
- Procedure di riconfigurazione SSD/RAID per FireSIGHT Management Center modelli FS2000 e FS4000

Decrittografia SSL

- Ricreare un'immagine di un'appliance Sourcefire SSL 1500/2000 alla versione 3.6 o successive
- Ottenere una password BIOS per un accessorio SSL
- Procedure di acquisizione dei pacchetti su un accessorio SSL
- Configurazione di SNMP su un accessorio SSL
- Configurazione del set di regole di base su un accessorio SSL
- Configurazione di un criterio di ispezione SSL sul sistema Cisco FireSIGHT

Integrazione con ISE, Estreamer, SIEM, User Agent, API e Connector

- L'accesso a un desktop remoto tramite RDP comporta la modifica dell'utente associato a un indirizzo IP
- Risoluzione dei problemi tra FireSIGHT System e eStreamer Client (SIEM)
- Installazione e disinstallazione di Sourcefire User Agent
- Risoluzione dei problemi di connettività con Sourcefire User Agent
- Configurazione di un sistema FireSIGHT per l'invio di avvisi a un server Syslog esterno
- Concedere autorizzazioni minime a un account utente di Active Directory utilizzato dall'agente utente Sourcefire
- Lo stato in tempo reale dell'agente utente è indicato come Sconosciuto
- Generazione di dati per la risoluzione dei problemi per il software Sourcefire in esecuzione su piattaforma BlueCoat serie X
- Informazioni sul controllo degli accessi basato su TrustSec con Firepower e ISE
- Il servizio del database Cisco Firepower User Agent non si riavvia dopo un arresto

Documenti TAC su Advanced Malware Protection

AMP For Endpoints, connettore FireAMP

- Raccolta di dati diagnostici da un connettore FireAMP in esecuzione su Windows
- Raccolta di dati diagnostici da un connettore FireAMP in esecuzione su Mac OSX
- Raccolta di dati diagnostici da un connettore FireAMP in esecuzione su Linux
- Immagine o clonazione di un computer con il connettore FireAMP installato
- Configurazione e gestione delle esclusioni in FireAMP

- Rimozione della cache e dei file di cronologia di FireAMP in Windows
- Switch della riga di comando per il programma di installazione del connettore FireAMP
- Disabilitare e abilitare il servizio client del connettore FireAMP
- Esecuzione in background del servizio client FireAMP Connector e disattivazione dell'interfaccia utente
- Aggiornamento di un connettore FireAMP su sistemi operativi Windows
- Impossibile arrestare il servizio connettore FireAMP a causa della protezione del connettore
- Tipi di file analizzati dal connettore FireAMP
- Guida alle esclusioni di FireAMP su Windows
- Ottenere informazioni sulla risoluzione dei problemi relativi ai dati su un dispositivo Android per FireAMP Mobile Connector
- Avvia analisi pianificate su FireAMP/AMP for Endpoints
- Esegui analisi IOC (Endpoint Indication of Compromise) con AMP per endpoint o FireAMP
- Installazione e configurazione del modulo AMP con AnyConnect 4.x e AMP Enabler
- Implementazione di Cisco AMP for Endpoints con Identity Persistence
- Utilizzare Advanced Malware Protection (AMP) con falsi eventi positivi o falsi negativi
- Panoramica dell'API Cisco AMP for Endpoint

AMP for Network

- Server necessari per le operazioni Advanced Malware Protection (AMP)
- Risoluzione dei problemi di connettività e registrazione con AMP su FireSIGHT Management Center
- Processo di rimozione delle connessioni tra un centro di gestione FireSIGHT e una console cloud FireAMP

Cloud

- Installazione e configurazione di FireAMP Private Cloud
- Generazione di un file snapshot di supporto su un cloud privato FireAMP
- Caricamento di un file nella console cloud FireAMP per visualizzare l'analisi dei file recenti

Threat Grid

- Generazione di uno snapshot di supporto su un'appliance AMP Threat Grid