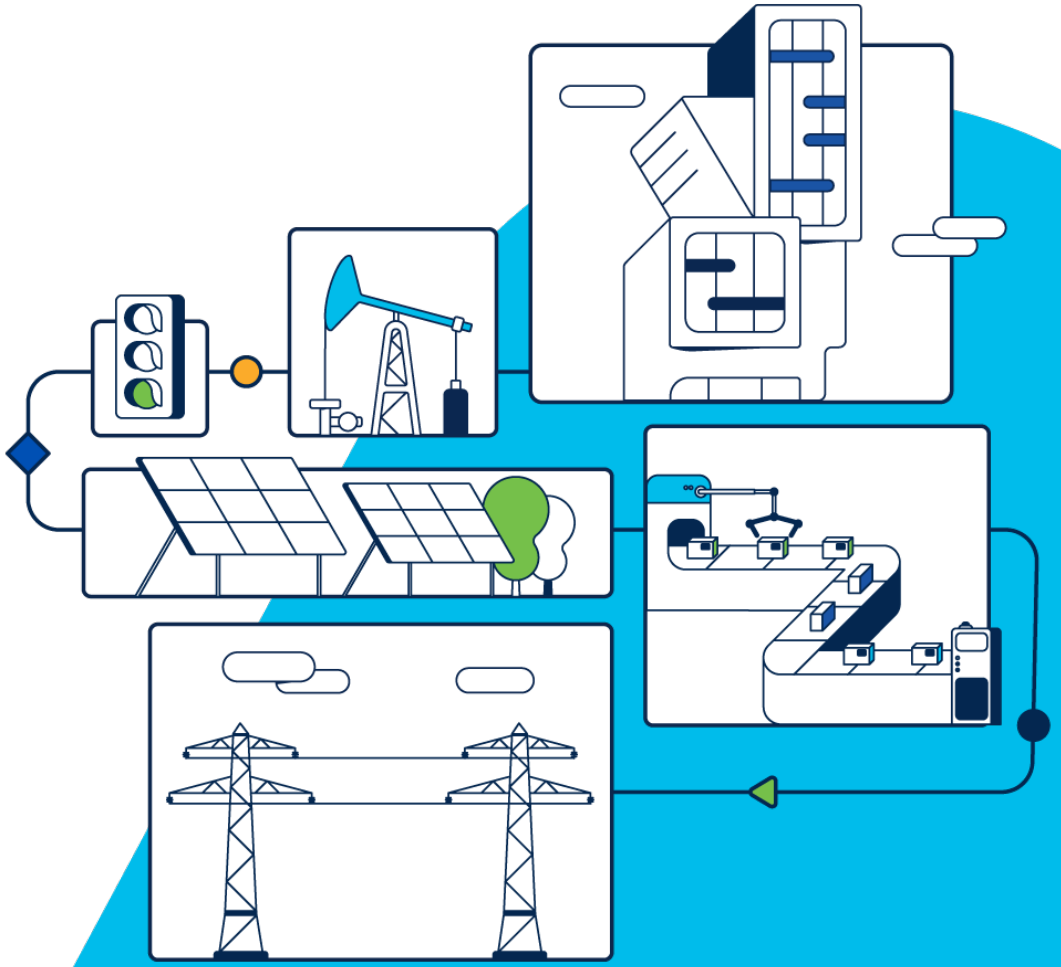
Cisco rešenja bezbednosti u industrijskim IoT mrežama

Radenko Čitaković

Systems Architect, Cisco

rcitakov@cisco.com

Novembar 2023.



Cisco IoT portfolio

Industrijski svičevi
IE1000, IE2000, IE3100, IE3200, IE3300, IE3400, IE3400H, IE4000, IE5000, IE9300

Industrijski ruteri
IR1101, IR1800, IR8100, IR8300

Uređaji za ugradnju
ESS, ESR, ESW, Resilient Mesh

Industrijske bežične mreže
Cisco URWB, IW6300, IW9167E, IR5XX, IXM Gateway

Industrijska sajber bezbednost
Cyber Vision, ISA3000 Firewall

Kontrola i razmena podataka
Edge Intelligence, IOx

Industrijski senzori
Industrial Asset Vision

Upravljanje i Automatizacija
Cisco DNA Center, Cisco SD-WAN, IoT Operations Dashboard

Korišćenje i primena

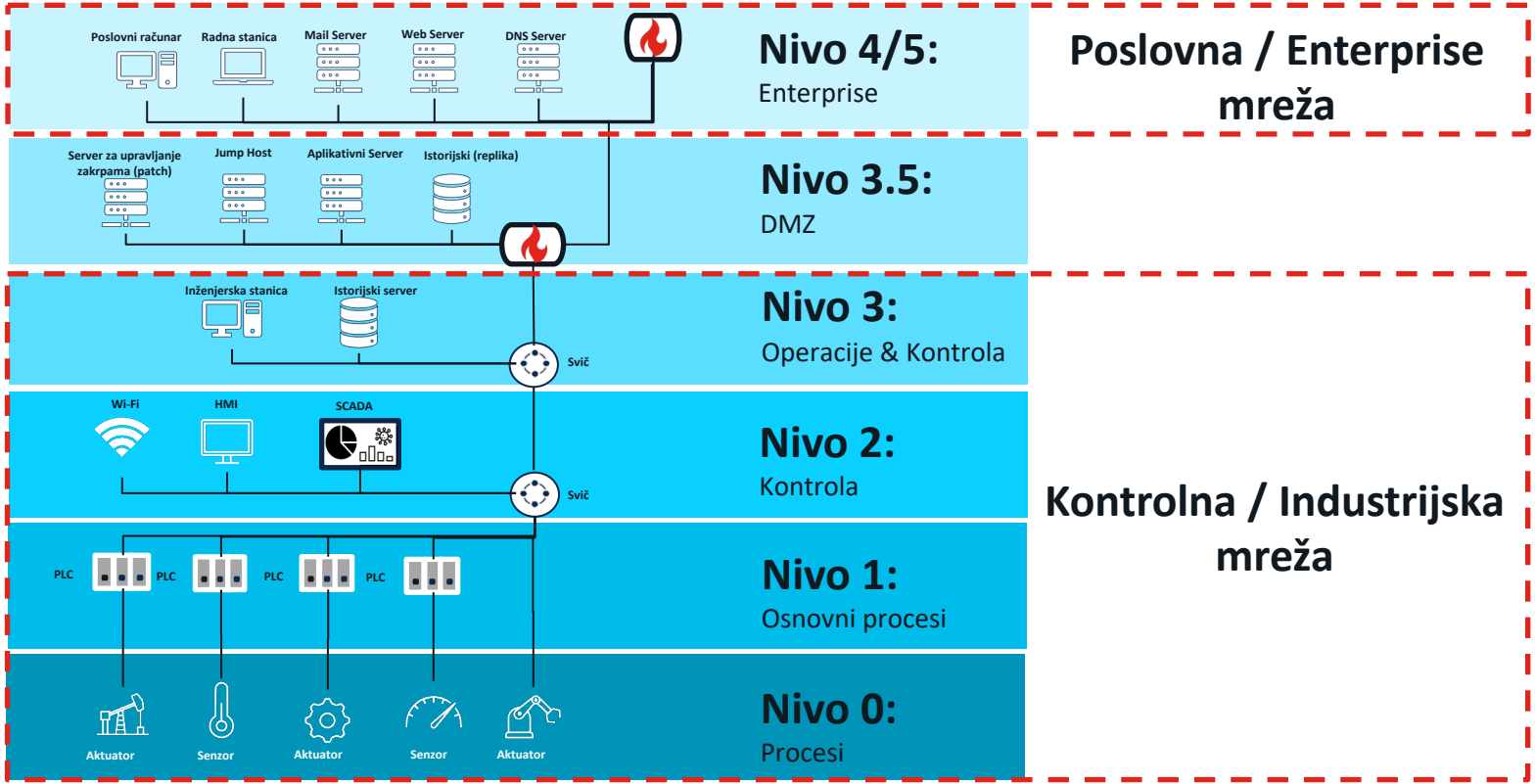
Koraci ka bezbednim industrijskim mrežama

Prioriteti sajber bezbednosti

SANS **5 kritičnih kontrolnih mera**

1. Odgovor na incident u industrijskim sistemima
2. Odbrambena arhitektura
3. Vidljivost i upravljanje u industrijskim mrežama
4. Bezbedan udaljeni pristup
5. Upravljanje ranjivostima zasnovano na riziku

Purdue referentni model arhitekture (PERA)

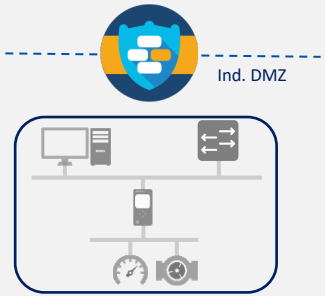


4 koraka do bezbenosti u industrijskim mrežama

1 Izgradite temelj bezbednosti

Definišite IT/OT granicu pomoću Cisco Secure Firewall-a

Cisco Secure Firewall

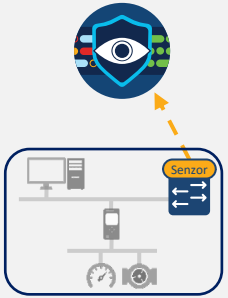


Otkrijte, Zaštitite, Reagujte

2 Dobijte vidljivost i status uređaja

Mreža kao ***senzor*** sa Cisco Ciber Vision

Cisco Cyber Vision

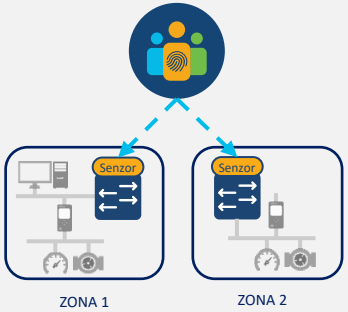


Identifikujte, Detektujte

3 Segmentirajte mrežu u manje zone poverenja

Mreža kao ***izvršilac*** sa Cisco ISE

Cisco Identity Services Engine

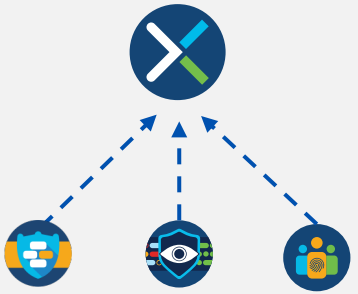


Segmentirajte, Zaštitite, Reagujte

4 Integrišite istragu incidenata

Istražite pretnje i orkestrirajte odgovor pomoću Cisco XDR-a

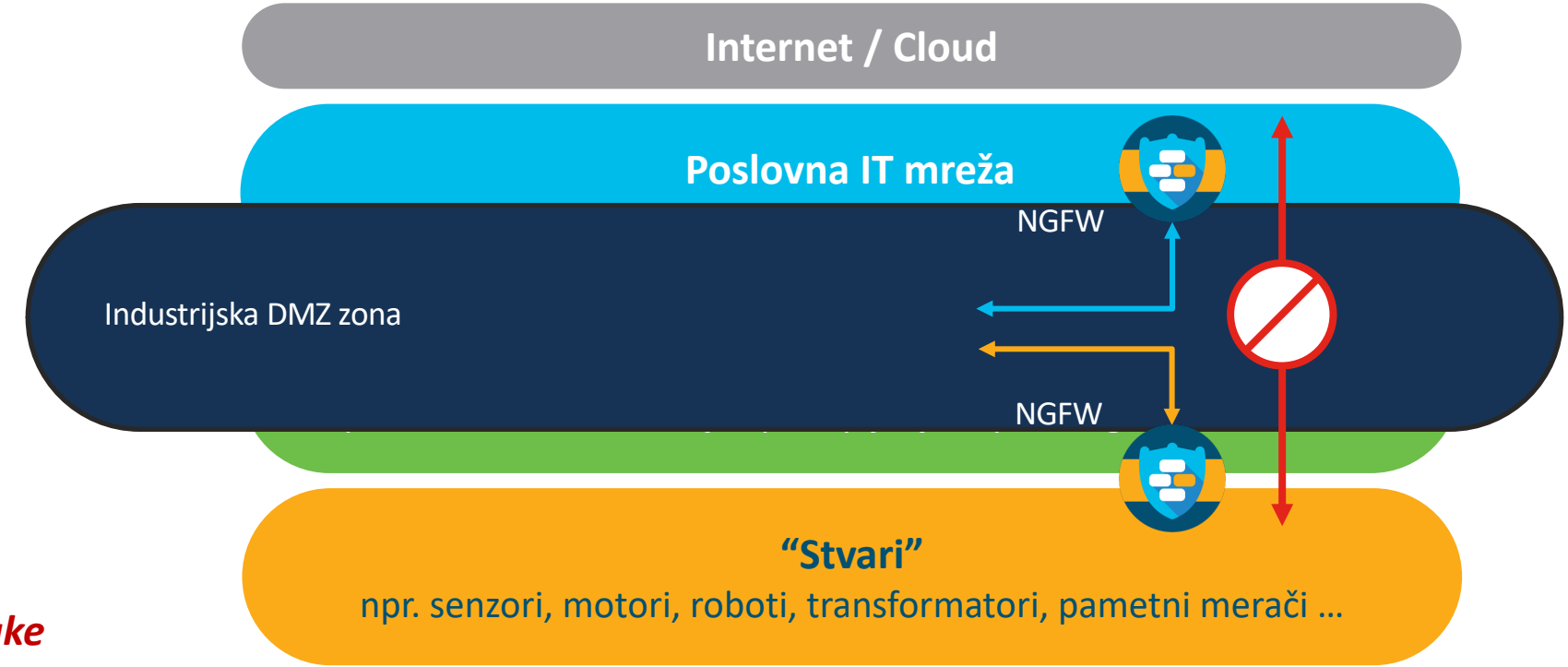
Cisco XDR



Istražite, Reagujte

Industrijska DMZ

Industrijska DMZ



Preporuke

- Eliminišite direktan saobraćaj između poslovne i industrijske zone. Ne treba dozvoliti industrijske protokole između IT i OT mreža
- Koristite VLAN segmentaciju za iDMZ uređaje da forsirate inspekciju
- Osigurajte da OT i IT mreža rade nezavisno jedna od druge da smanjite uticaje “nepovezanosti”

Vidljivost u OT

Kritična potreba za vidljivošću u industrijskim mrežama

Identifikovanje OT imovine i njihove komunikacije

Rešavanje problema sa konfiguracijom

Poboljšanje pouzdanosti i performansi mreže

Otkrivanje upada i zlonamernog saobraćaja

Kontrolisanje daljinskog pristupa inženjerskim stanicama

Vidljivost pomaže u pokretanju IT/OT saradnje tako što deli zajedničko razumevanje situacije

Tipični “problemi” viđeni u industrijskim mrežama

Neovlašćeni daljinski pristup trećih strana

Podrazumevani kredencijali za prijavu na sisteme

IPv6 saobraćaj u IPv4 mrežama

Višestruki Time serveri

Aktivnosti malvera ili virusa

Bezbednosne zakrpe nisu instalirane

Povučena sredstva su i dalje povezana

Nepotrebne mrežne komunikacije

Nepoznati uređaji na mreži

DNS upiti za Amazon

Windows XP SMBv1

Otpremanje programa preko VPN-a tokom noći

Firmver otpremljen preko FTP-a bez potpisa

Loša konfiguracija firewall-a ili sviča

Uređaji u pogrešnom VLAN-u

OT mreža potpuno povezana sa IT mrežom

Izgradnja pouzdane i bezbedne industrijske mreže je ključna za uspešno poslovanje

Cisco Cyber Vision

Platforma za ***Vidljivost*** i ***Bezbednost*** u industrijskom IoT okruženju

Vidljivost

Inventar imovine

”Obrazac” komunikacije

Bezbednosni statusi

Ranjivosti uređaja

Bodovanje rizika

Operativni uvidi

Pratite modifikacije procesa/uređaja

Zabeležite događaje sistema kontrole

Kontekst i uvidi koji su temelj za izgradnju pouzdanih i bezbednih OT mreža

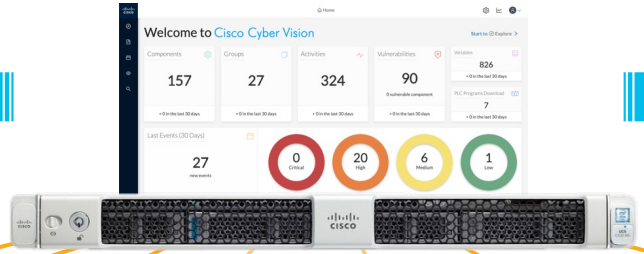
Bezbednost i sigurnost u skali sa infrastrukturom

Vidljivost i detekcija pretnji ugrađena u vašu industrijsku mrežu

Cyber Vision Center

Centralizovana Analitika & Vizuelizacija podataka

Integracije sa Cisco rešenjima



Integracije sa drugim sistemima

Lagani metapodaci

IE3300 i IE3400 svičevi

IE3400HD IP67 svič

IR1101 4G/5G Ruter

IR8300 Multi-servisni Ruter

Catalyst IE9300 Rugged Agregacioni svičevi

Catalyst 9300/9400

IC3000 industrijski računar

Mrežni senzori

Duboka inspekcija paketa ugrađena je u mrežne elemente i eliminiše potrebu za SPAN-om

Hardverski senzor

DPI preko SPAN za podršku braunfild

Uloga ***Cyber Vision*** senzora

Prikuplja saobraćaj industrijske mreže

Snima tokove industrijske mreže (pasivno) i ispituje uređaje (aktivno). Lokalno skladišti podatke u slučaju da Centar nije dostupan

Dekodira industrijske protokole (DPI)

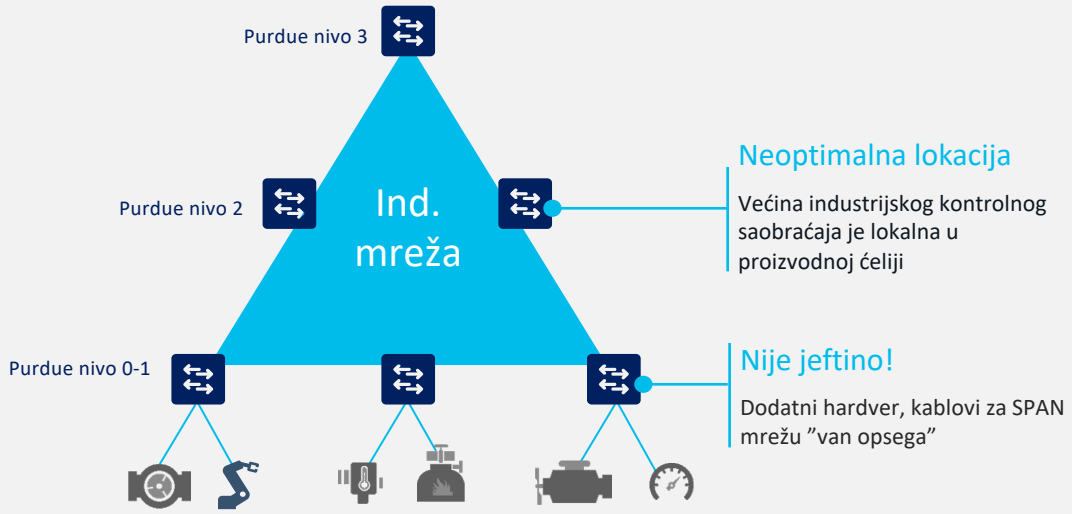
Razume većinu OT i IT komunikacionih protokola za analizu korisnog opterećenja paketa i izdvajanje značajnih informacija

Šalje meta podatke ka Cyber Vision Center

Šalje metapodatke centru za skladištenje, analizu i vizuelizaciju. Ovo dodaje samo 3 do 5% dodatnog saobraćaja na mrežu

Zašto je važan mrežni senzor?

Većina industrijskog mrežnog saobraćaja je **istok-zapad**, a ne **sever-jug**



Važna je lokacija za DPI !

- Preslikavanje saobraćaja na sloju agregacije daje samo vidljivosti saobraćaja sever-jug
- Preslikavanje saobraćaja na sloju ćelije zahteva skupu SPAN mrežu “van opsega”

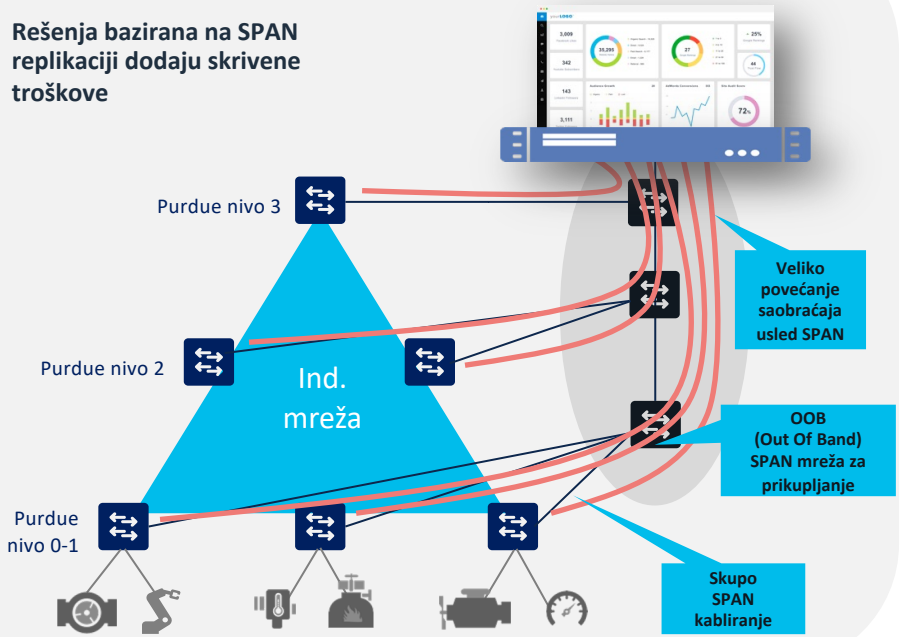
Senzori ugrađeni u mrežu vide sve što je vezano za nju

Zašto je važan mrežni senzor?

Vidljivost koju možete primeniti u velikom obimu bez potrebe za skupim SPAN mrežama

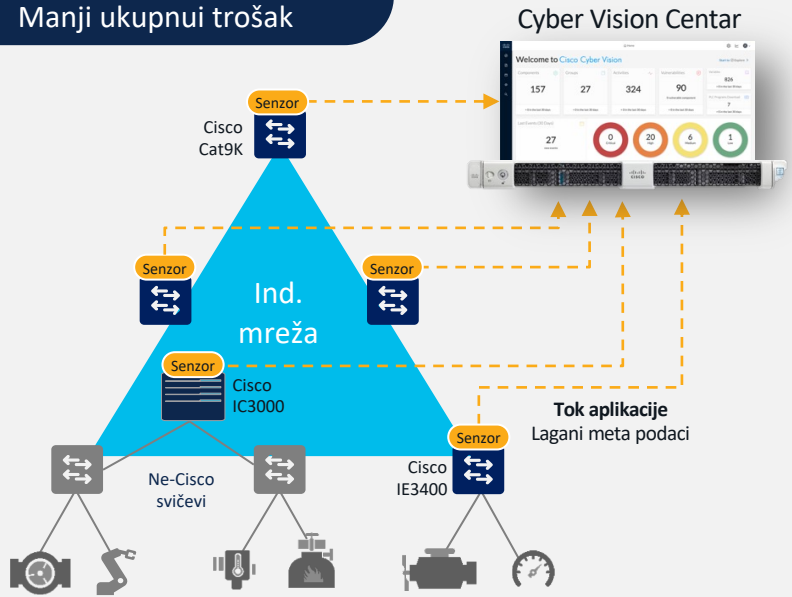
Druga rešenja

Rešenja bazirana na SPAN replikaciji dodaju skrivene troškove



RSPAN donosi kašnjenje i džiter!

Jednostavna implementacija
Manji ukupnui trošak

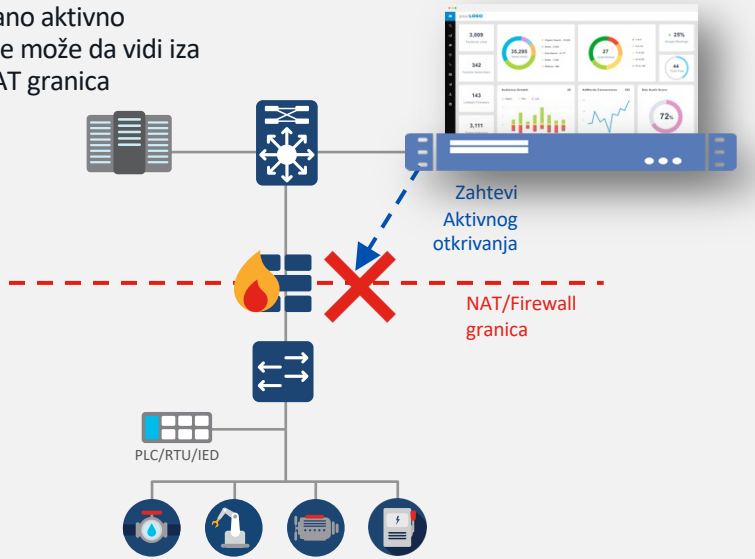


Zašto je važan mrežni senzor?

Distribuirano aktivno otkrivanje na ivici daje 100% vidljivost

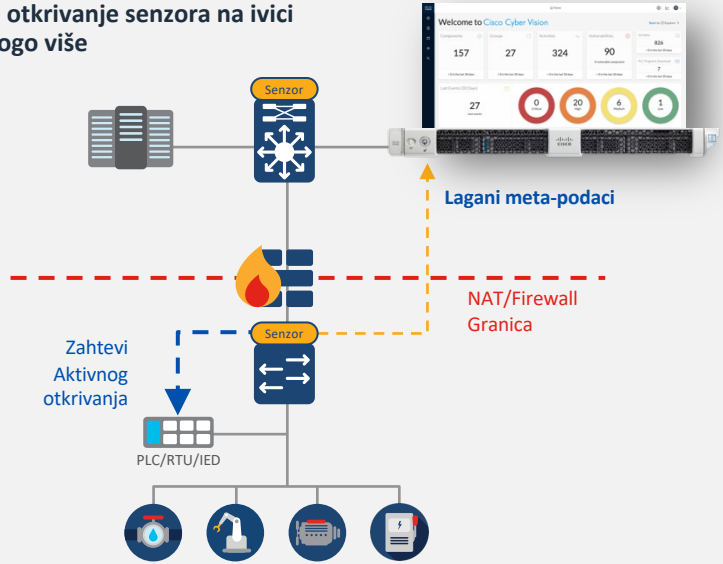
Druga rešenja

Centralizovano aktivno otkrivanje ne može da vidi iza Firewall i NAT granica

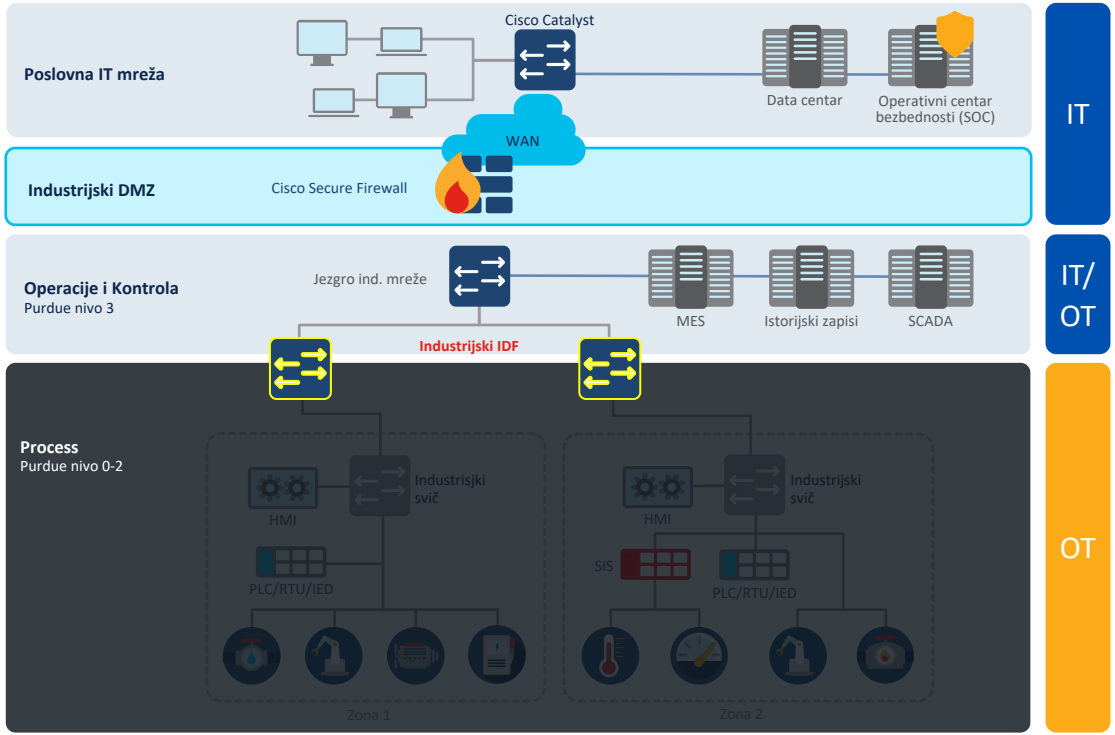


Cisco Cyber Vision

Aktivno otkrivanje senzora na ivici vidi mnogo više

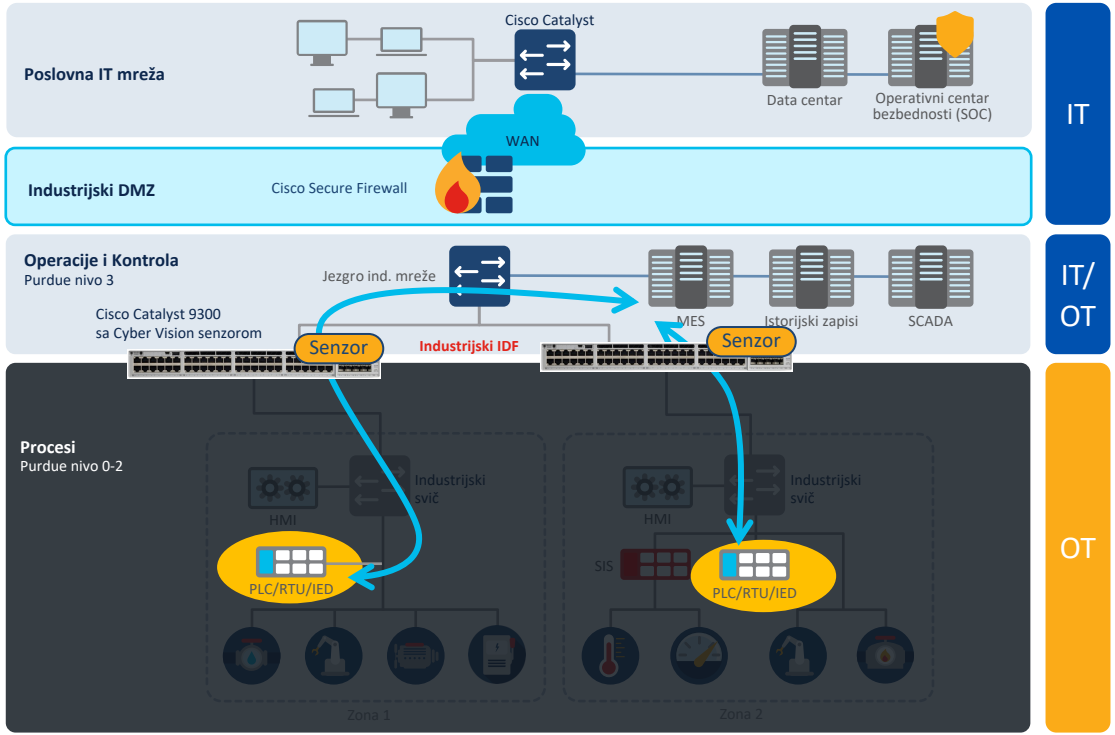


IT nema vidljivost iza industrijskog IDF-a



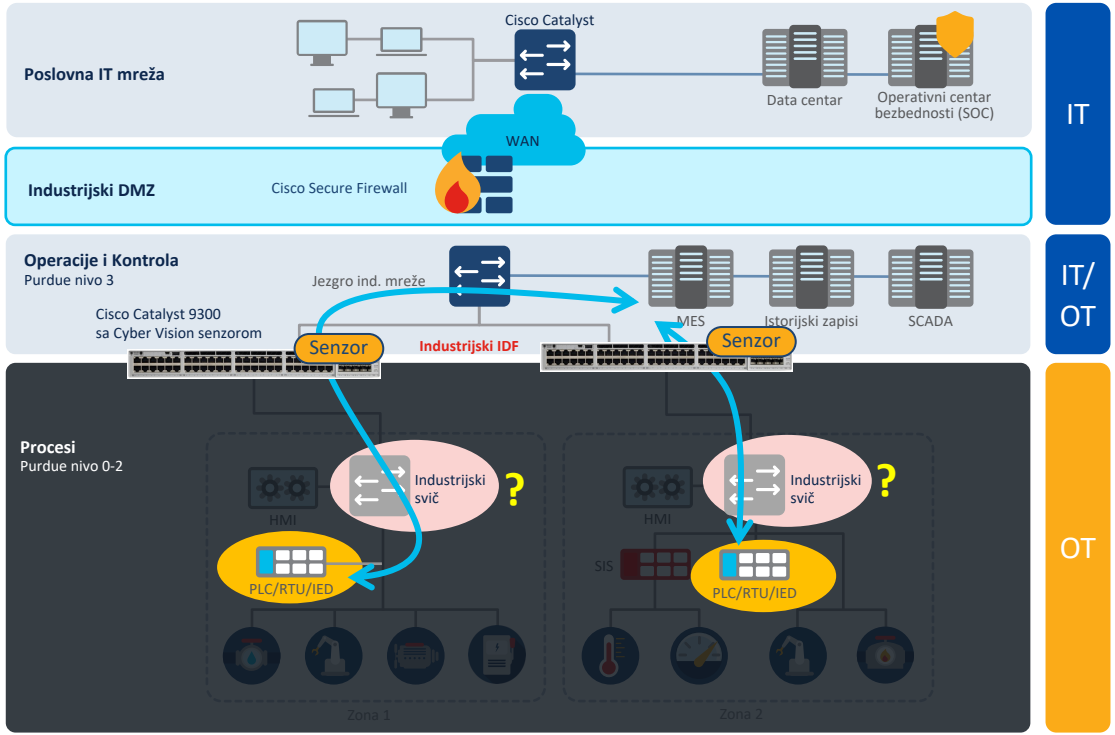
Kako IT može da iskoristi mrežnu opremu koju poseduje da bi stekao vidljivost u OT-u?

Catalyst svičevi “upale svetlo”



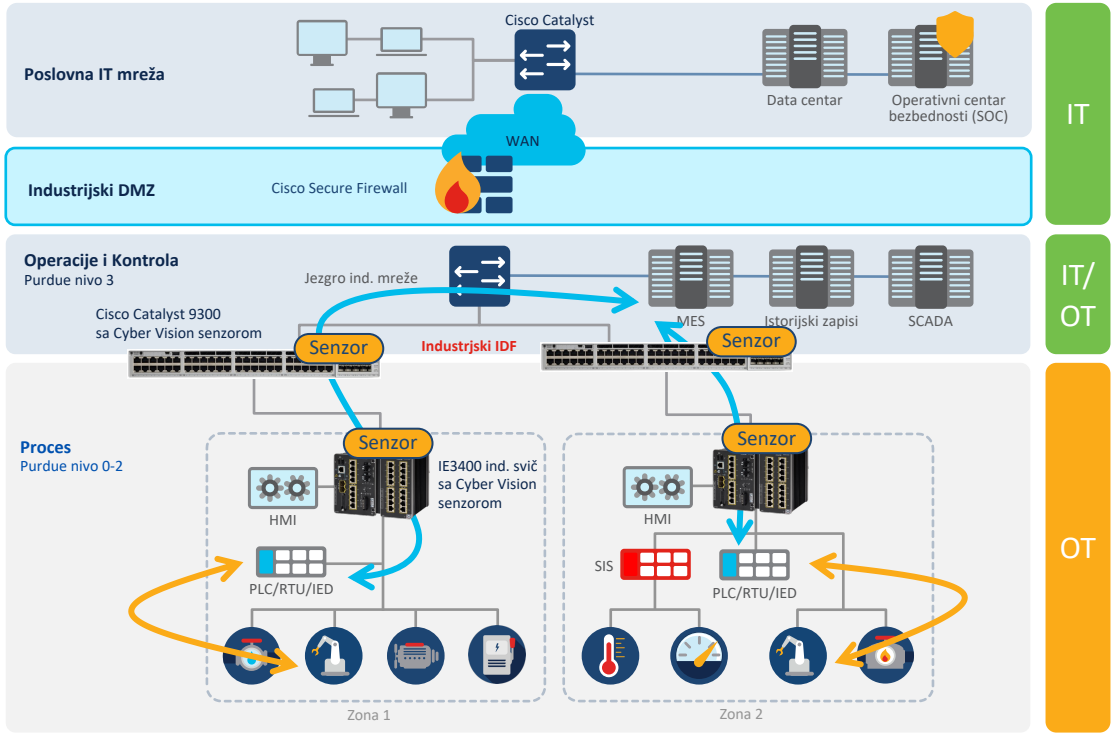
Korak 1: Cyber Vision senzor na Catalyst 9300 svičeveima vam daje vidljivost za Sever-Jug saobraćaj i identifikaciju ključnih uređaja

Pokažite prednosti vidljivosti za OT



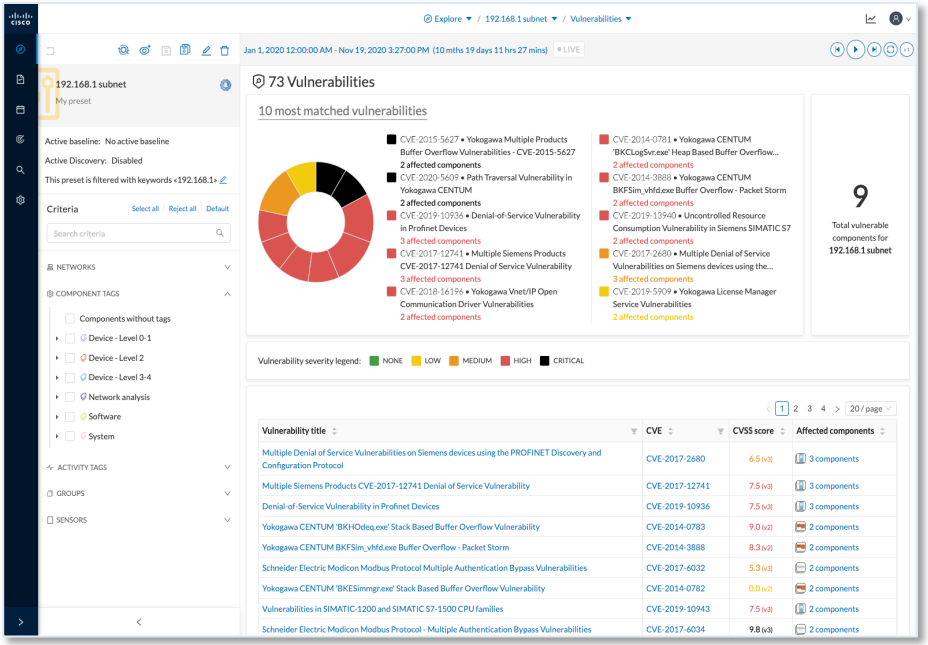
Korak 2: Identifikujte kritične industrijske svičeve koji povezuju ove bitne uređaje

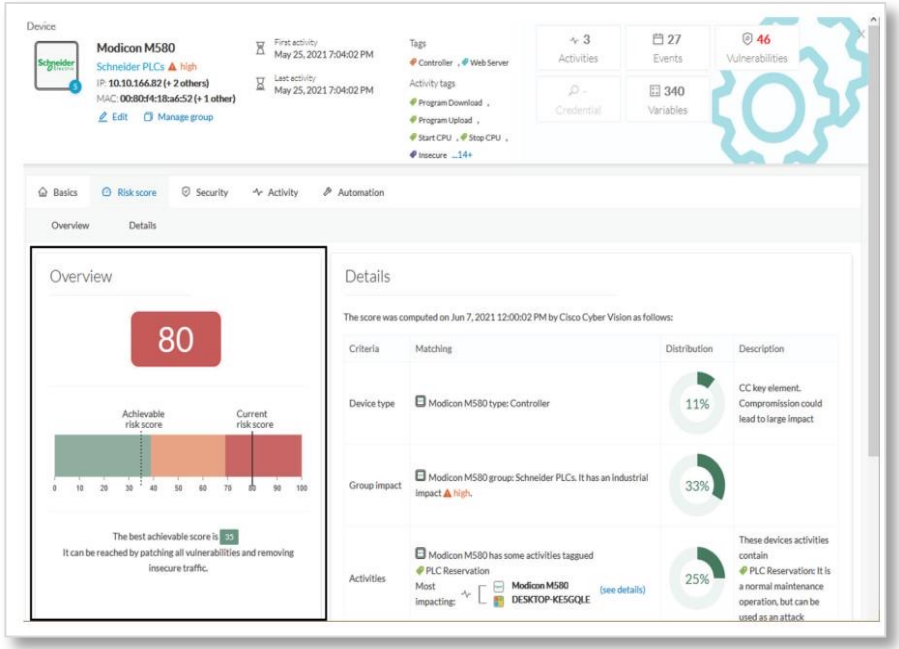
Steknite punu vidljivost - unapredite bezbednosni status



Korak 3: Zamenite te svičeve sa Cisco IE svičevimea na kojima radi Cyber Vision senzor da vidite celu OT mrežu

Automatski identifikujte ranjivosti vaših OT uređaja, procenite rizik



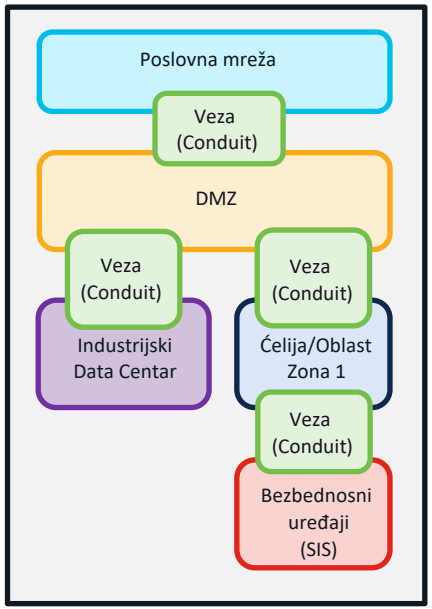


Segmentacija mreže

Segmentacija je ključ zaštite OT imovine

Koristite NIST i/ili IEC 62443 preporuke

IEC 62443



NIST “Zero Trust” vodič

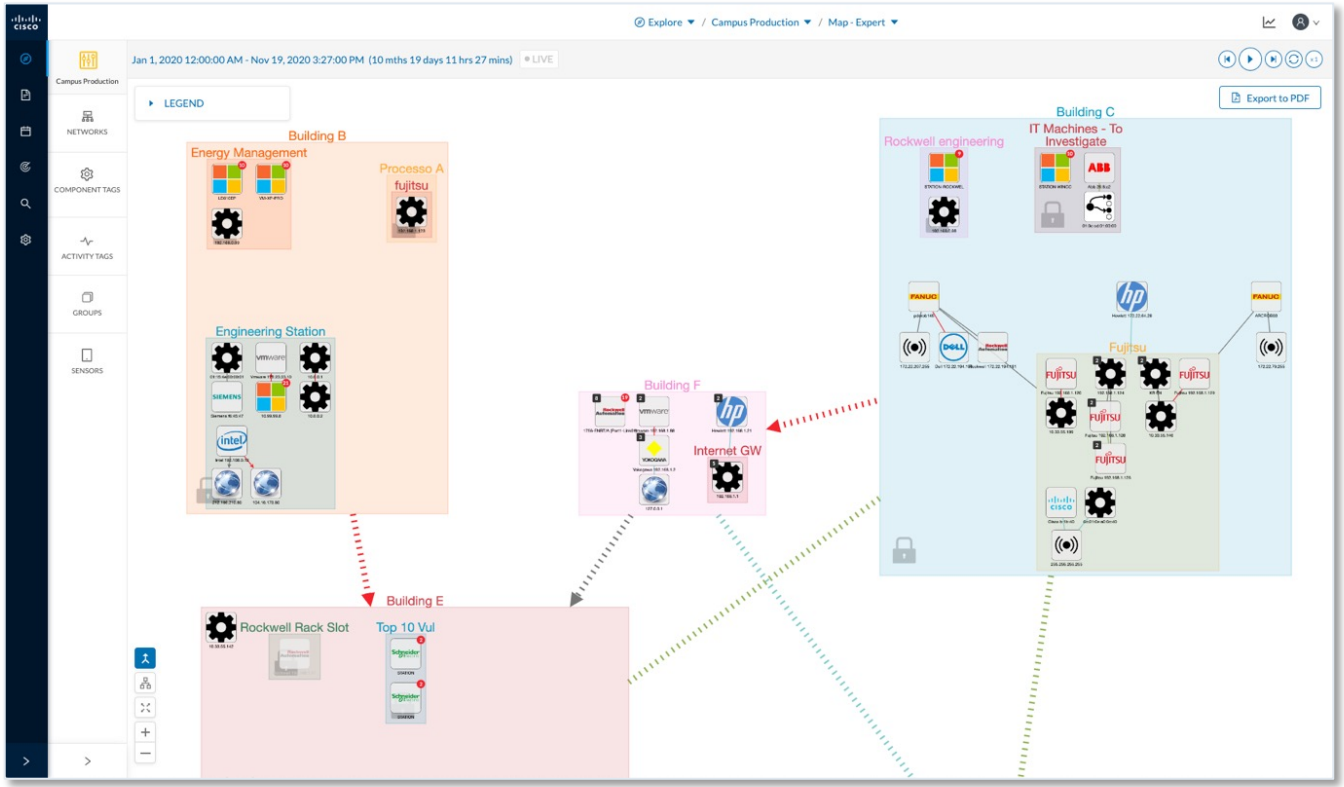
3.1.2 ZTA Using Micro-Segmentation

An enterprise may choose to implement a ZTA based on placing individual or groups of resources on a unique network segment protected by a gateway security component. In this approach, the enterprise places infrastructure devices such as intelligent switches (or routers) or next generation firewalls (NGFWs) or special purpose gateway devices to act as PEPs protecting each resource or small group of related resources. Alternatively (or additionally), the enterprise may choose to implement host-based micro-segmentation using software agents (see Section 3.2.1) or firewalls on the endpoint asset(s), These gateway devices dynamically grant access to individual requests from a client, asset or service. Depending on the model, the gateway may be the sole PEP component or part of a multipart PEP consisting of the gateway and client-side agent (see Section 3.2.1).

This approach applies to a variety of use cases and deployment models as the protecting device acts as the PEP, with management of said devices acting as the PE/PA component. This approach requires an identity governance program (IGP) to fully function but relies on the gateway components to act as the PEP that shields resources from unauthorized access and/or discovery.

The key necessity to this approach is that the PEP components are managed and should be able to react and reconfigure as needed to respond to threats or change in the workflow. It is possible to implement some features of a micro-segmented enterprise by using less advanced gateway devices and even stateless firewalls, but the administration cost and difficulty to quickly adapt to changes make this a very poor choice.

Koristite Cyber Vision za grupisanje OT uređaja u Zone



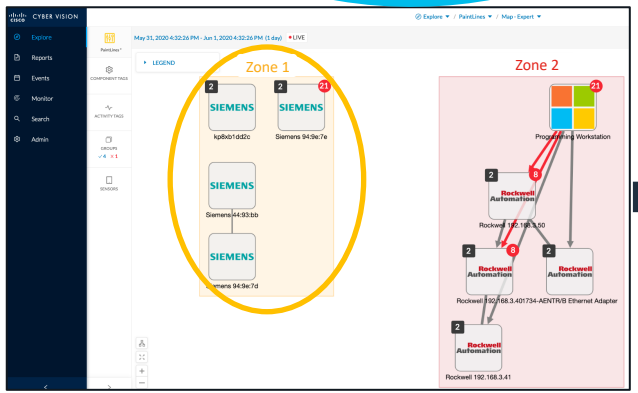
Cyber Vision + ISE pojednostavljuju segmentaciju

OT

Mogu da grupišem sredstva u zone koje odgovaraju mom industrijskom procesu

IT

Mogu da izgradim bezbednosne politike koje neće poremetiti proizvodnju



Cyber Vision mapa

	Zona 1	Zona 2	PLC	MES
Zona 1	✓	✗	✓	✗
Zona 2	✗	✓	✓	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

pxGrid ažuriranje sa identitetima krajnjih tačaka sredstava i grupom ”Ćelija 1” kao prilagođenim atributom

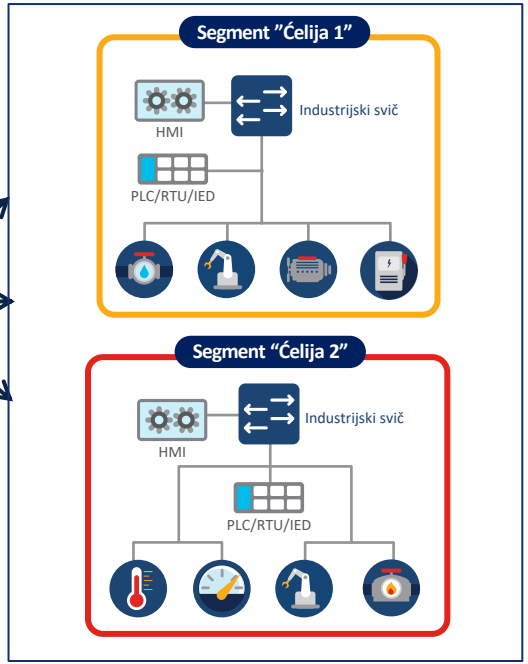
Cisco ISE matrica pravila

dACL

SGT

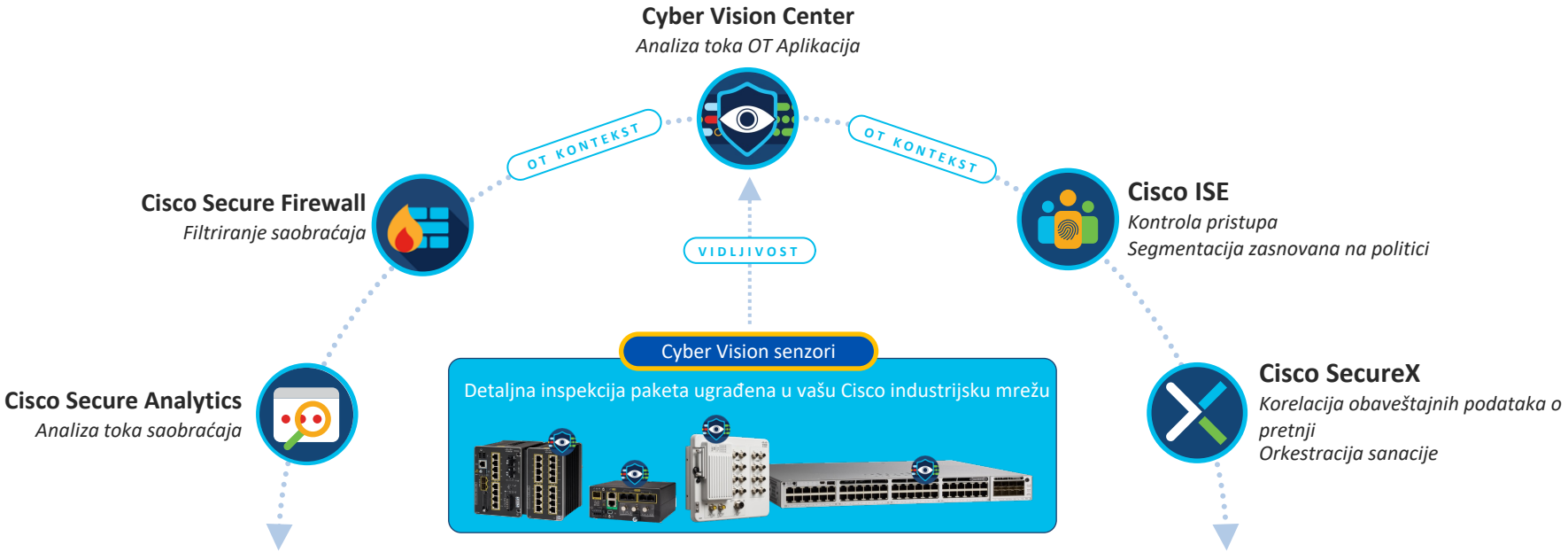
VLAN

Segmentacija industrijske mreže



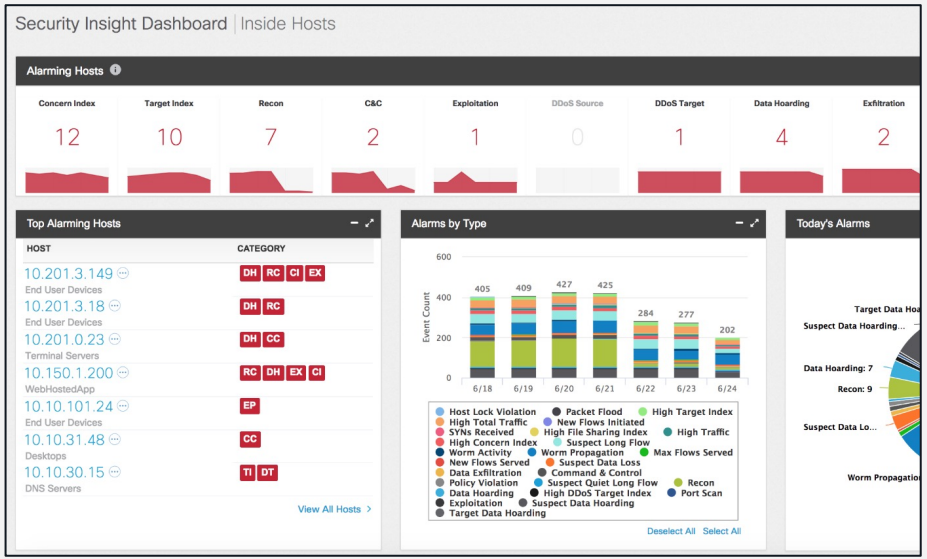
Otklanjanje pretnji

Cyber Vision širi IT bezbednost u OT



Vidljivost OT sredstava i konteksta koji se dele u svim vašim IT bezbednosnim alatima

Cisco Secure Analytics + Cyber Vision



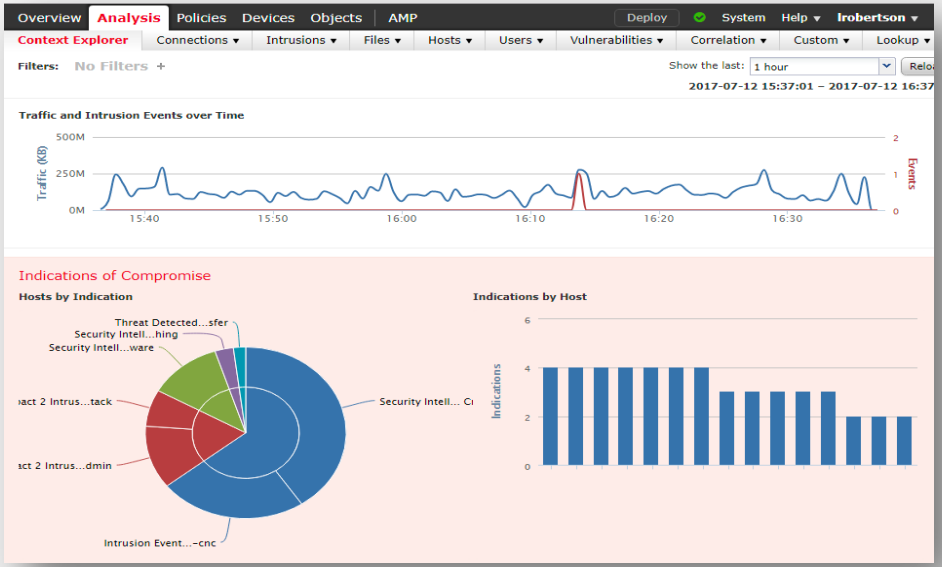
Obogatite informacije o hostovima u Cisco Secure Analitics bogatim kontekstom iz Cyber Vision-a

Lako identifikujte tokove mapirane na industrijske uređaje pomoću atributa host-grupa na osnovu informacija Cyber Vision-a

Kreirajte politike upozorenja da biste identifikovali i upozorili na komunikaciju između zona

Cyber Vision pomaže Secure Analytics-u da istraži i otkrije pretnje u industrijskim mrežama

Cisco Secure FMC + Cyber Vision



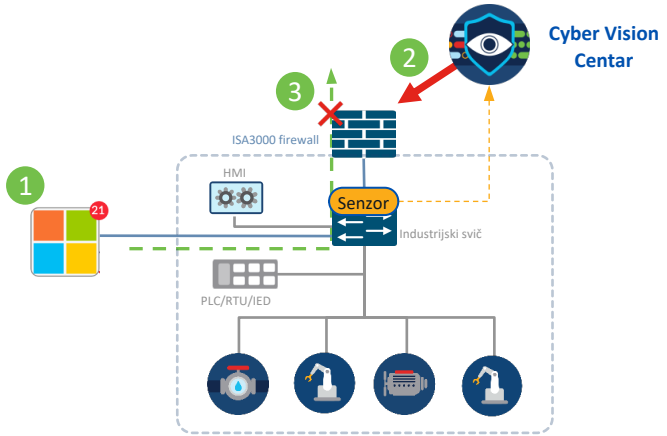
Mapirajte identitet ICS uređaja na Hostove u Firepower-u za korišćenje u politici korelacije bezbednog zaštitnog zida

Identifikujte anomalije i tokove u Cyber Vision-u i prekinite sesije FTD Firewall-a

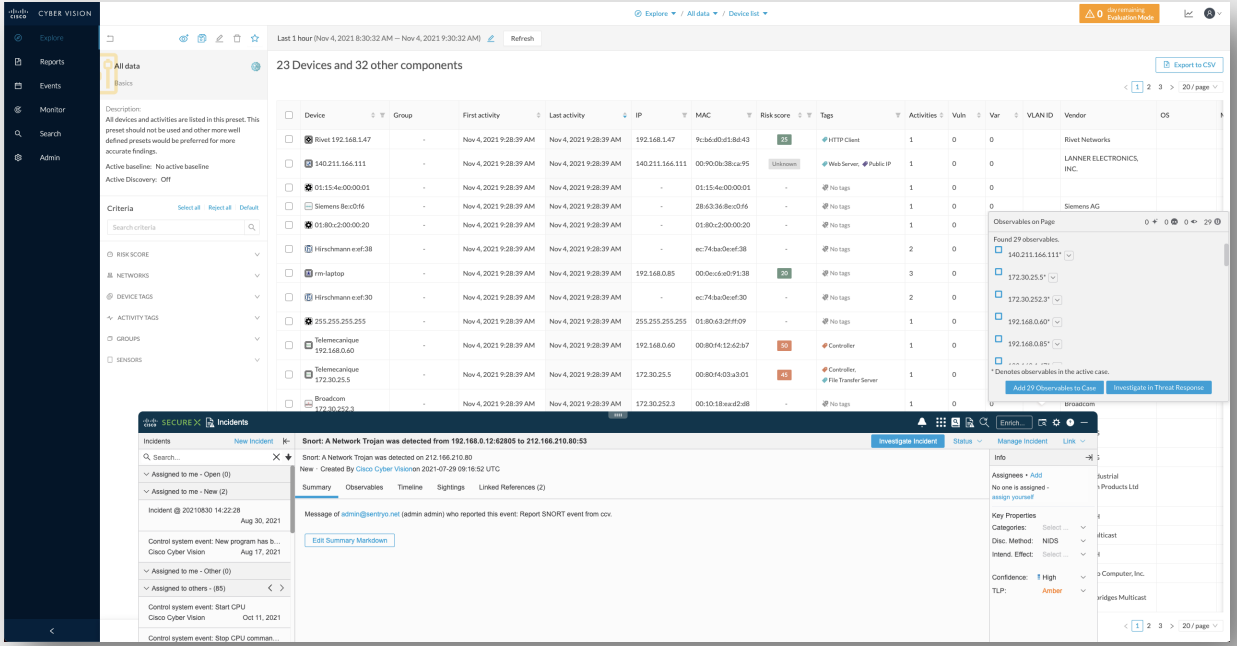
Iskoristite host atribute iz Cyber Vision-a da biste upozorili na neočekivano ponašanje

Odbrana od pretnji Firewall-a (FTD) – Kill Sessions

1. Cyber Vision detektuje događaj
   - Promena ustaljenog ponašanja
     - Nova komponenta
     - Nova aktivnost
     - Nova promenljiva
   - IDS (Snort) uzbuna
2. Cyber Vision šalje komandu Firewall-u da terminira pridruženu sesiju
3. Firewall blokira sesiju



Istraga i Orkestracija sa SecureX



Koristite SecureX za

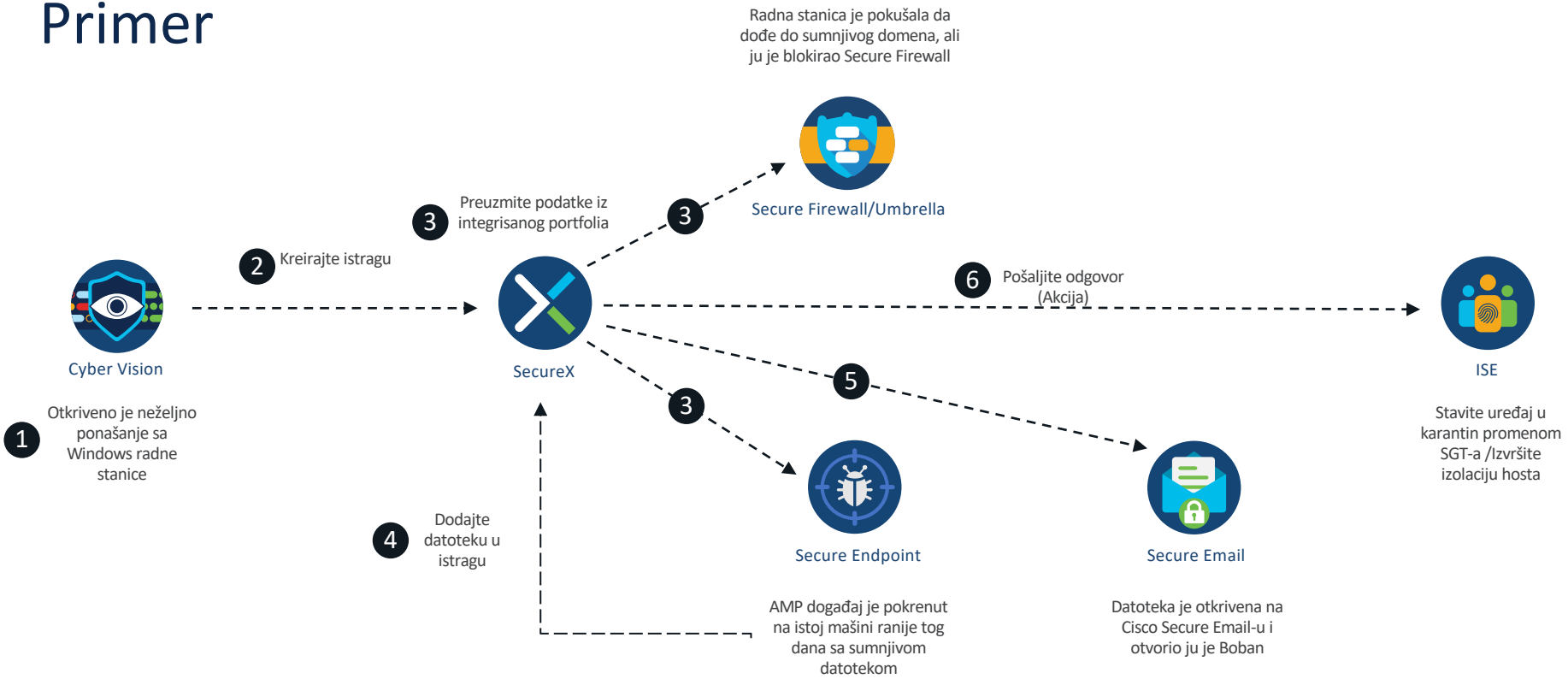
Kreiranje i upravljanje incidentima

Kreiranje i orkestriracija **playbook-ova**

Pokretanje istrage u Talosu, Umbrella, Secure Endpoint, Threat Grid, itd.

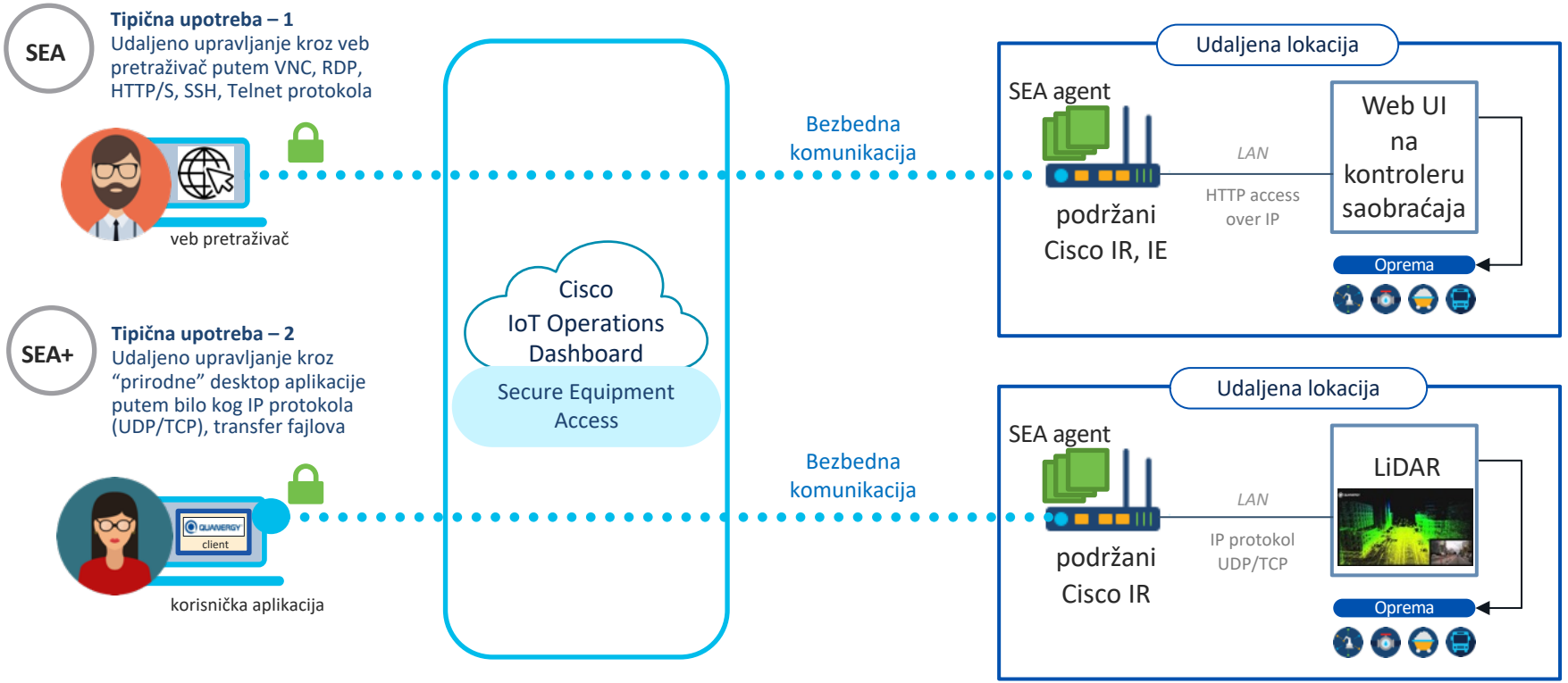
SecureX traka u Cyber Vision za istragu i orkestraciju sanacije, otklanjanje pretnje

Primer


Radna stanica je pokušala da dođe do sumnjivog domena, ali ju je blokirao Secure Firewall
Secure Firewall/Umbrella
3
Preuzmite podatke iz integrisanog portfolia
3
2
Kreirajte istragu
Cyber Vision
SecureX
6
Pošaljite odgovor (Akcija)
ISE
Stavite uređaj u karantin promenom SGT-a /Izvršite izolaciju hosta
1
Otkriveno je neželjno ponašanje sa Windows radne stanice
5
3
Secure Endpoint
Secure Email
4
Dodajte datoteku u istragu
AMP događaj je pokrenut na istoj mašini ranije tog dana sa sumnjivom datotekom
Datoteka je otkrivena na Cisco Secure Email-u i otvorio ju je Boban

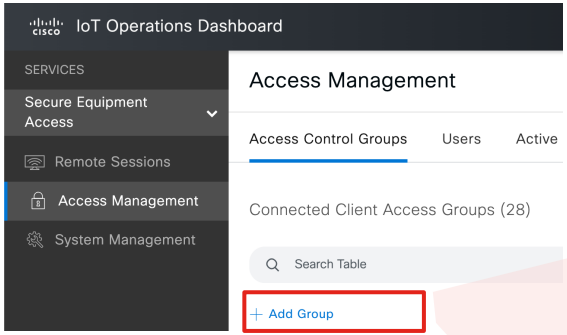
Bezbedan udaljeni pristup

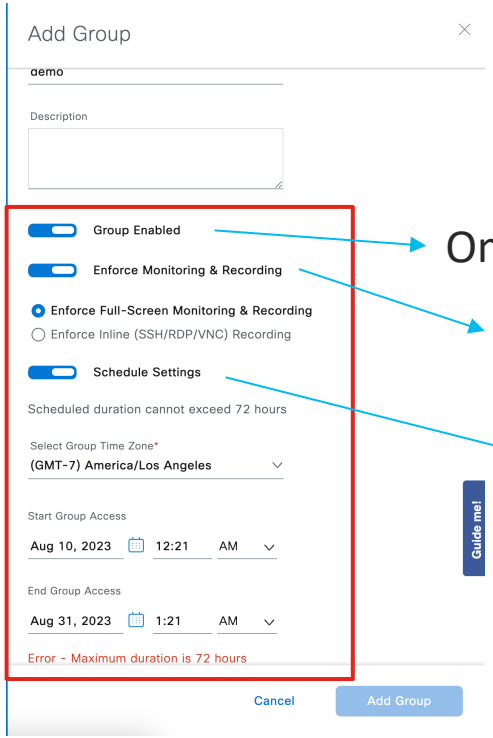
Bezbedan udaljeni pristup opremi – Cisco SEA i SEA+



SEA – opcije kreiranja grupa

Grupe mogu biti aktivne samo u udređenom period i može se forsirati snimanje





Omogući/Onemogući grupu

Primeni snimanje sesije

Omogući zakazan vremenski period

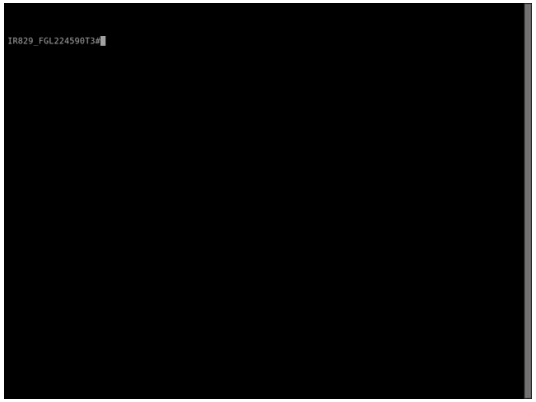
SEA Integracije

Duo

- Primena dodatnih mehanizama bezbednosti za pristup udaljenog korisnika (Autentifikacija, provera statusa,…)
- Primenjuje se na udaljeni računar.
- Samo za SEA+. Nije relevantno za SEA

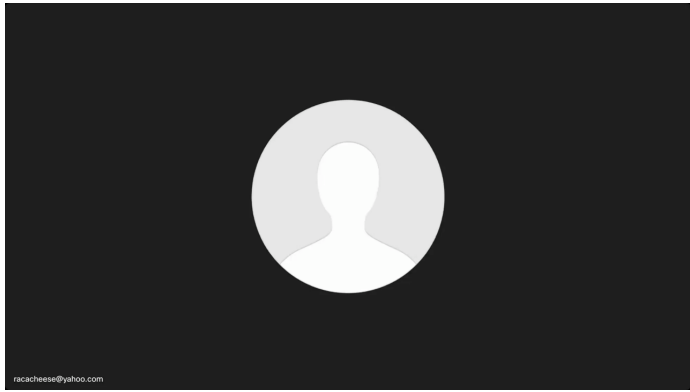
Amazon S3

- Skladište snimljenih ***inline*** sesija SEA agenta
- Telnet, SSH, RDP, VNC, Web



Webex

- Kompletno snimanje celog ekrana
- Snimljen kompletan “podeljen“ ekran u Webex sastanku




CISCO