Palo Alto Networks Cortex XSOAR Sales Playbook

March 2020

paloalto® NETWORKS

CORTEX™ XSOAR BY PALO ALTO NETWORKS

Westcon

Contents

SOC challenges

The solution – SOAR

SOAR benefits

SOAR market opportunity

Cortex XSOAR – the perfect SOAR match

How does Cortex XSOAR work?

Benefits of Cortex XSOAR

SOAR target market and identifiers

Why sell Cortex XSOAR?

How can Westcon help you grow your Cortex XSOAR business?

Resources & further info

How to get started

SOC challenges

Growing alerts

12k alerts per week

Lack of skilled analysts

2 million analysts shortage.
SOC analysts take 6 months to train and only stay for 18 months

No consistent process

No metrics, fragmented documentation

Limited visibility

Expanded threat surface

Disparate infrastructures

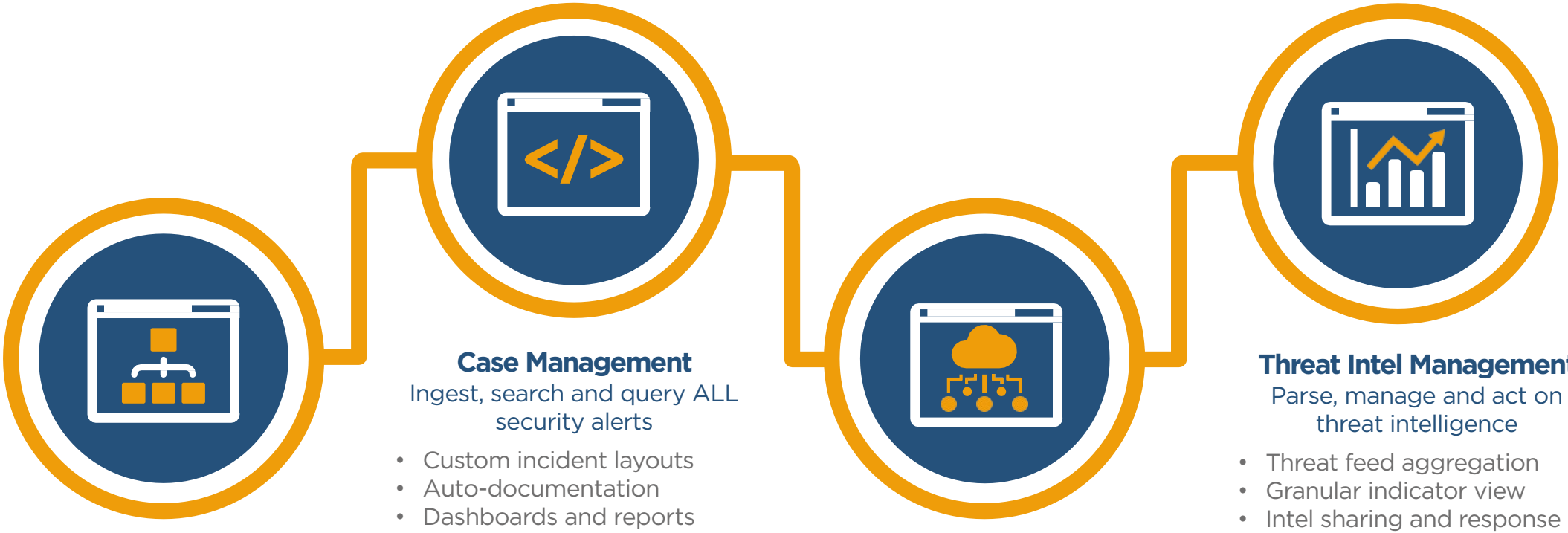
Coordination challenge across product consoles

Long MTTR

Increased business risk: weeks to resolve incidents

The solution - SOAR

Security Orchestration, Automation, and Response



Security Orchestration

Respond to incidents with speed & scale

- Hundreds of integrations
- Thousands of automatable actions
- Visual playbook editor

Case Management

Ingest, search and query ALL security alerts

- Custom incident layouts
- Auto-documentation
- Dashboards and reports

Collaboration & Learning

Improve investigation quality by working together

- Virtual war room
- Auto-Investigation canvas
- Machine learning

Threat Intel Management

Parse, manage and act on threat intelligence

- Threat feed aggregation
- Granular indicator view
- Intel sharing and response

SOAR benefits

Unify security infrastructures

Coordinate enrichment and response by gathering intelligence from multiple products on a single console.

Accelerate incident response

By automating low-level manual tasks, SOAR can reduce incident response times and improve accuracy.

Standardise and scale processes

Through playbooks, SOAR standardises incident enrichment and response processes to increases the baseline quality and scalability of response.

Increase analyst productivity

SOAR frees up analysts' time for more important decision-making, and proactive tasks rather than getting mired in grunt-work.

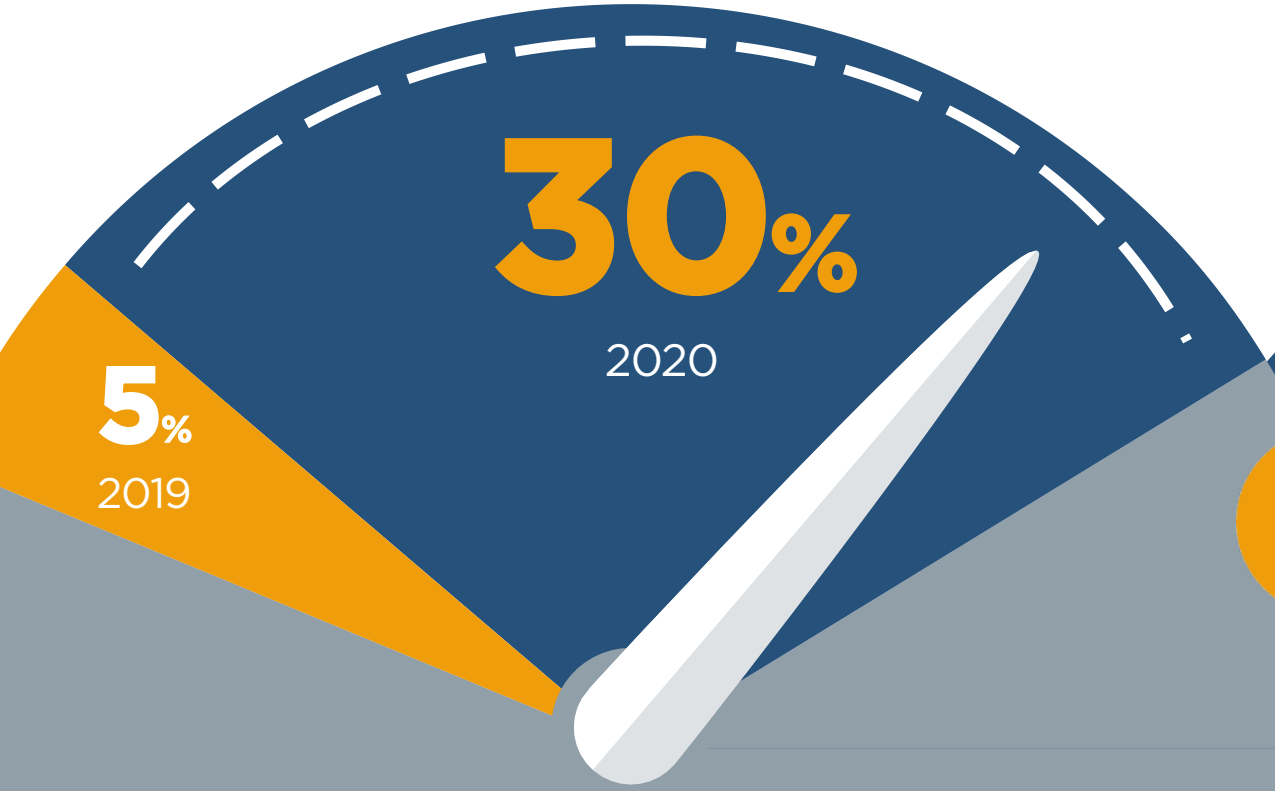
Leverage existing investments

Through automation and minimised console-switching, SOAR enables coordination across multiple products and greater value from existing security investments.

Improve overall security posture

The sum of all aforementioned benefits is an overall improvement of the organisation's security posture and a corresponding reduction in security and business risk.

SOAR market opportunity



Increased Adoption

Organisations leveraging SOAR (Security Orchestration, Automation, and Response) solutions will rise from 5% now to 30% by 2022.

Technology Convergence

The ideal SOAR solution is a convergence of three previously distinct technology markets

- **Security Ochestration and Automation**
- **Security Incident Response Platforms**
- **Threat Intelligence Platforms**

Cortex XSOAR - the perfect SOAR match

Cortex XSOAR is a game-changer for security operations. A significant evolution of the well-known Demisto® platform, Cortex XSOAR integrates threat intelligence management with playbook-driven enforcement across your enterprise so that customers can act on threat feeds with speed and confidence.

SOAR

Automation:

How to make machines do task-orientated "human work"

Incident management and collaboration:

End-to-end management of an incident by people

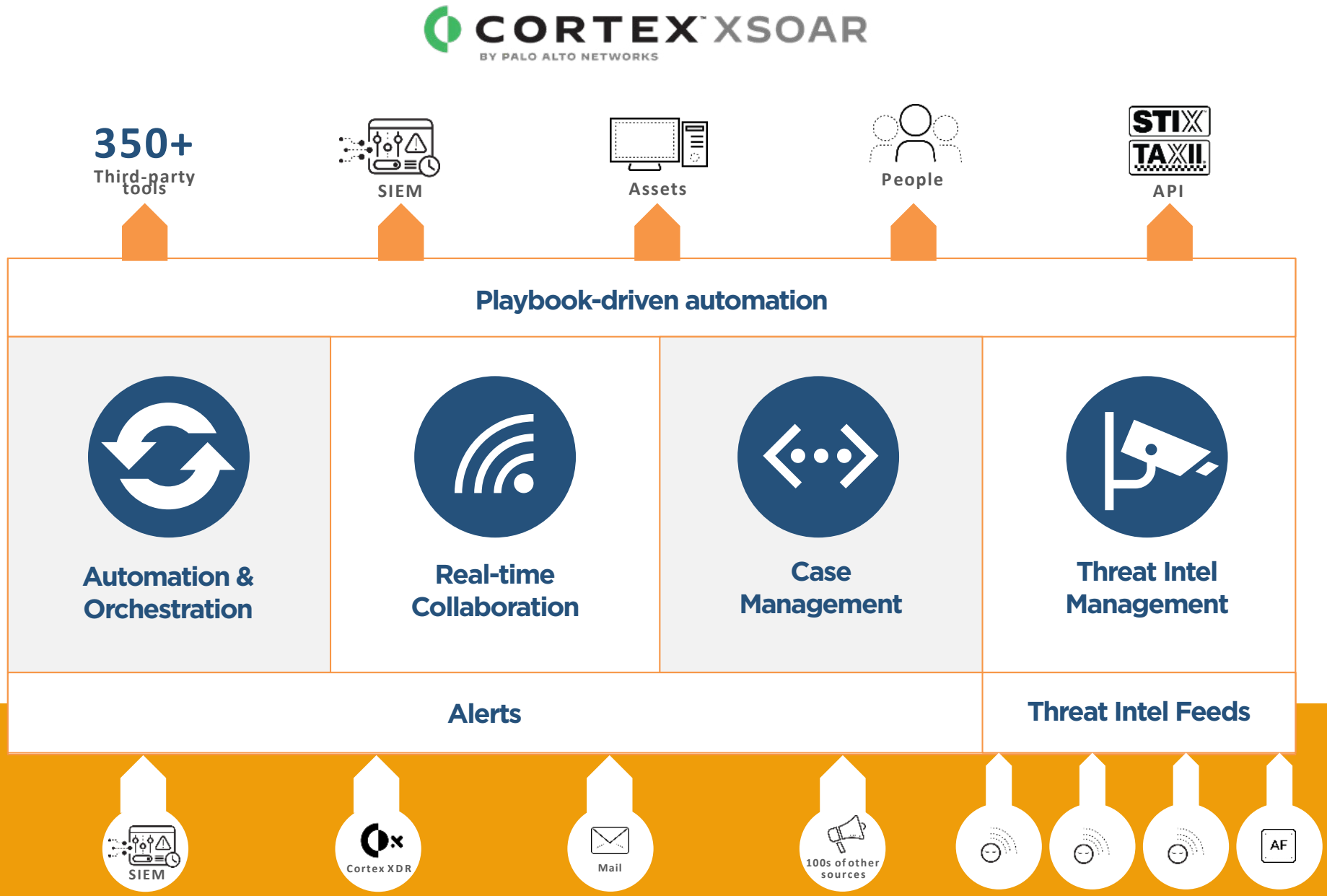
Orchestration:

How different technologies (both security-specific and non-security-specific) are integrated to work together

Dashboards and reporting:

Visualisations and capabilities for collecting and reporting on metrics and other information

How does Cortex XSOAR work?



Benefits of Cortex XSOAR

Accelerate Response

Respond to incidents with speed and scale

- Hundreds of integrations
- Thousands of security actions
- Cross correlations

Standardise Process

Respond to incidents the same way every time

- Task-based workflows
- Visual playbook editor
- SLA and metric tracking

Collaborate and Learn

Improve investigation quality by working together

- Virtual war room
- Investigation canvas
- Machine learning

Reduce Risk

Reduce business and security risk

- Dashboards and reports
- Auto documentation
- Improved ROI

Reduced weekly alerts from 10,000 to 500

Reduced response times from 3 days to 25 minutes

Automated 30% of incidents for 1FTE time saved

SOAR target market & identifiers

Anyone with a SOC!

SOC identifiers:

- 500+ employee size companies
- They will be SIEM users
- They will also be using EDR
- They may have a SOC Analyst or SecOps lead listed on LinkedIn

A number of your existing customers may already have SOCs and are prime targets!!

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (December 2018)

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (August 2019)

Why sell Cortex XSOAR?

What's in it for you?

SOAR is in demand and a growth market

You'll be pushing on open doors and your sales team will want to sell it

Fast sales cycle, typically 3-6 months

Annual license recurring revenue

25-35% margin (subject to a valid deal reg)

Lock out your competitors

Average deal is $150k

Vendor agnostic so you can cross and upsell with nearly all customers

How can Westcon help you grow your Cortex XSOAR business?

Westcon value added services

Trained sales and technical team with a deep knowledge of SOAR and Cortex XSOAR (in addition to the full Palo Alto Networks product portfolio)

Sales and technical training to skill up your team

Data profiling to help you identify target companies within your existing customer base

Marketing support to help you roll out a campaign to generate opportunities

Pre sales and BDM support to help you close opportunities

Dedicated Palo Alto Networks team to help you with deal regs and quotes

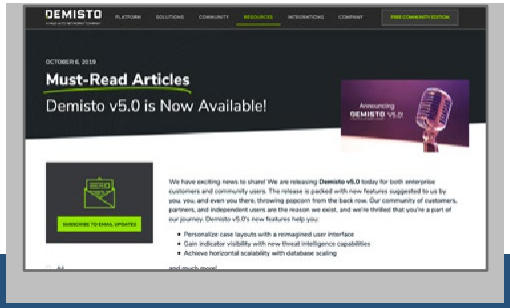
Full range of services including finance to support your deals

Palo Alto Networks Authorized Global Training Partner offering extensive training for your team and your end users

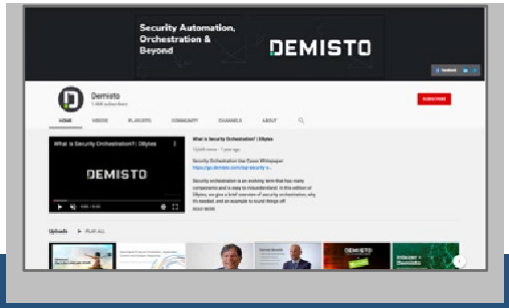
Dedicated Palo Alto Networks Elite Authorised Support Center offering best in class L1/L2 multi lingual support

Resources & further info

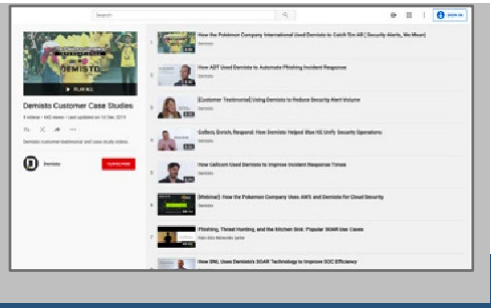
The following resources are available to help you:



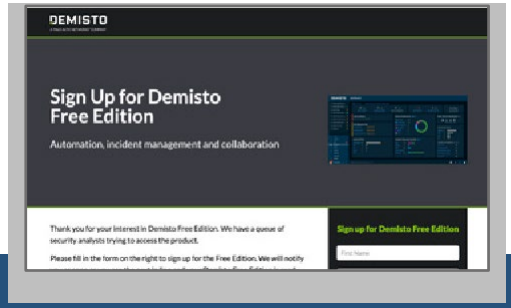
Demisto blog



Demisto YouTube channel

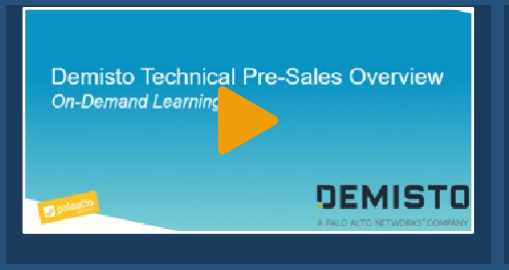


Demisto video case studies



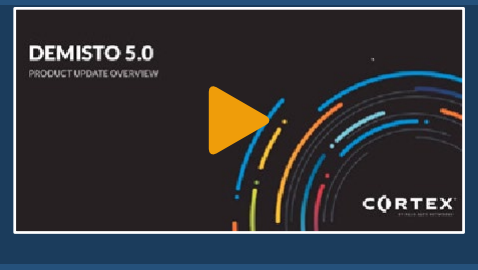
Demisto 30 day free trial

Technical course
5 hours 10 minutes



Pre-sales
2 hours

Sales - Cortex + Demisto
1 hour



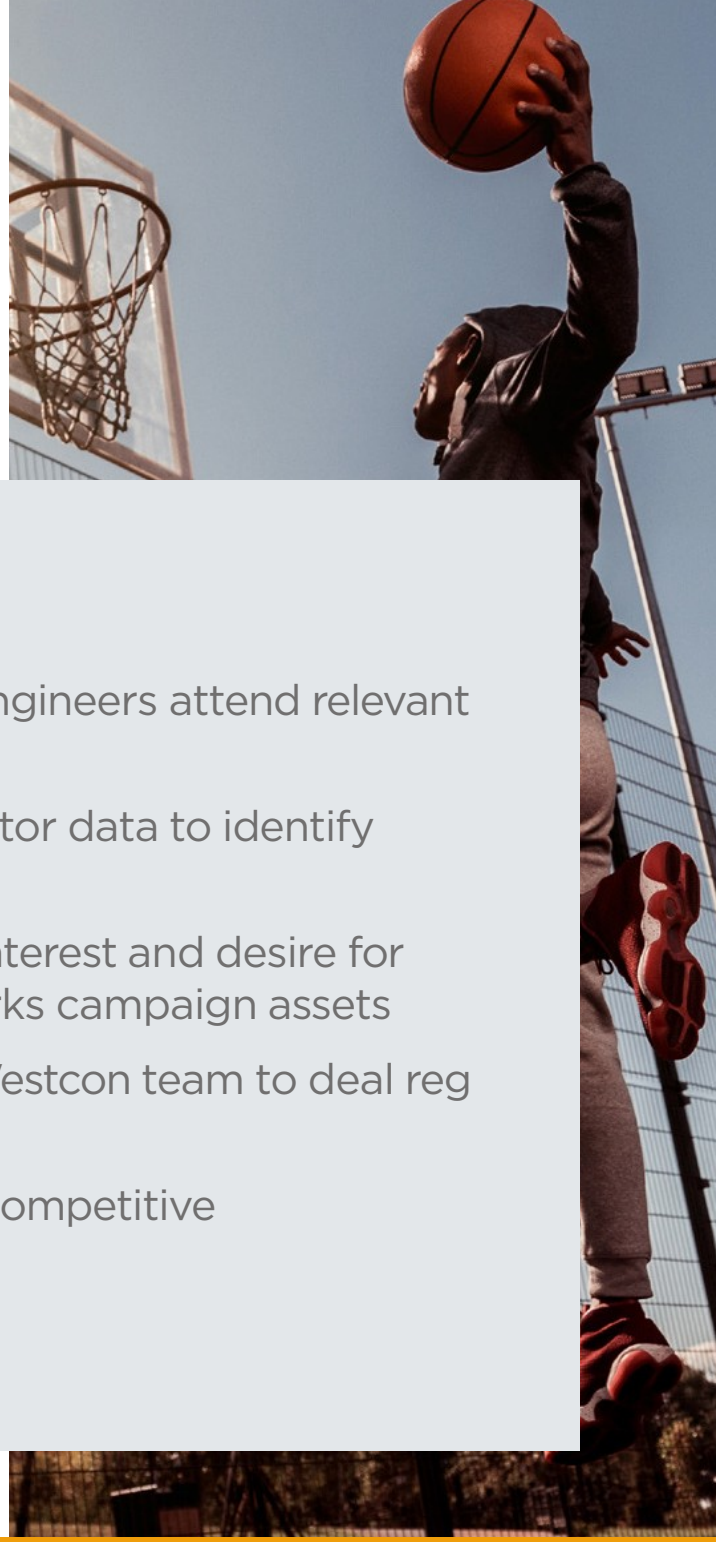
Demisto 5.0
5 minutes

Demisto sales, marketing & technical content on the Partner Portal

Demisto 'Journey to the Center of the SOC' campaign assets

How to get started

Westcon is looking to work with a small number of focus partners to help them establish and grow their SOAR business with Palo Alto Networks.



To get started partners will need to:

- Have a valid Palo Alto Networks partner certification
- Demonstrate a commitment to ensure their sales and pre sales engineers attend relevant training organised for them by Westcon
- Supply current customer list so that Westcon can pull SOC indicator data to identify companies likely to have a SOC that can be targeted
- Jointly fund an initial marketing campaign to create awareness, interest and desire for Demisto within the target customers leveraging Palo Alto Networks campaign assets
- Provide regular updates on leads generated and work with the Westcon team to deal reg these as soon as possible
- Ask Westcon for support if opportunities get stalled or become competitive
- Put all of the above into their Palo Alto Networks business plan

To get started please contact your BDM

Westcon

CORTEX XSOAR
BY PALO ALTO NETWORKS

Start to explore the SOAR opportunity now and contact your Westcon Account Manager

Or contact the EMEA team
PANWSupportCentral.emea@westcon.com

About Westcon-Comstor

Westcon-Comstor (Westcon International) has been a leading global technology distributor for over 30 years. Today, we continue to lead the market through unrivalled channel support and expertise in global deployment, digital distribution and services. Deep market insight and vendor relationships coupled with a uniquely collaborative approach enables our partners across the supply chain to deliver the solutions they need to grow and thrive in today's digital world.