TRAINING

by

What is SOAR?

Why SOAR?

Pain points of current SOC Teams

- Too many alerts — Alert Fatigue
- Way too many tools working in silos
- Slow — 40 minutes – 2 hours
- No standardization in Analysis and Investigation
- Human Error
- Skill shortage — Retaining talent is a huge challenge

SOAR can help SOC teams in reducing these pain points significantly.

What could be automated?

Assignment of alerts to analyst

- Who will pick up the alert?

What could be automated?

Assignment of alerts to analyst

Information gathering

- Picking up the important information from the triggered alert.
- Usually the information in the important fields
- Often acts as a starting point for investigation

What could be automated?

Assignment of alerts to analyst

Information gathering

Enrichment of information

- Connect with AD to get the more details of a user
- Connect to VA report and get the list of vulnerabilities on a machine of interest
- Connect with TI and check the reputation of File/URL/IP

What could be automated?

SOC EXPERTS

Assignment of alerts to analyst | Information gathering | Enrichment of information | **Analysis / Investigation**

- Get the file from a end user machine and submit it to Sandbox for analysis
- Check if an IP has ever communicated to our network in the past.
- Has any other user received an email from the same sender?

What could be automated?

Assignment of alerts to analyst | Information gathering | Enrichment of information | Analysis / Investigation | **User Interactions**

- Are you trying to log in to the server?
- We are analyzing the email you have reported.
- The email you have reported is a legitimate email and is safe to open.
- Permission to search all the mailboxes for mail with same subject line.

What could be automated?

SOC EXPERTS

Assignment of alerts to analyst | Information gathering | Enrichment of information | Analysis / Investigation | User Interactions | **Respond**

- Creating a ticket
- Initiate a scan on VA Scanner
- Initiate a AV Scan
- Blocking IP on Firewall
- Blocking URLs on Web Gateway

What could be automated?

SOC EXPERTS

Assignment of alerts to analyst | Information gathering | Enrichment of information | Analysis / Investigation | User Interactions | Respond | **Enhancement / Lessons Learned**

- Adding the newly detected malware hash to local threat intel
- Sending organization wide email about the new targeted phishing technique.

What could be automated?

SOC EXPERTS

- Assignment of alerts to analyst
- Information gathering
- Enrichment of information
- Analysis / Investigation
- User Interactions
- Respond
- Enhancement / Lessons Learned

Any and all of these can be automated

Where does SOAR fit in?

Typical SOC Workflow

SOC Workflow with SOAR

Will SOAR replace Analyst Jobs?

Bad News Yes

Good News

- Its a new technology (SOAR is in Infant stage)
- <15% of SOC teams are using SOAR
- Wide-spread adoption will take 2 – 5 years
- Not every SOC can use SOAR right away (even if they want to)
- You are learning SOAR

What does it take to be good at SOAR?

- Good understanding of SOC Processes in an organization
- Basic working knowledge of different tools/technologies
- Basic of scripting (python)

Can I be a SOAR engineer without scripting?

- You can survive, but cant excel.

Will SOAR replace SIEM?

- SOAR acts as a complimentary solution to SIEM (and not a competitive solution.)
- SIEM does the heavy lifting of processing millions of logs and generating few 100 alerts.
- SOAR starts with these alerts and handles the analysis and incident response.

- SOAR can be combined with SIEM solution.

SOAR Vendors.

IBM Resilient

splunk> phantom

Siemplify

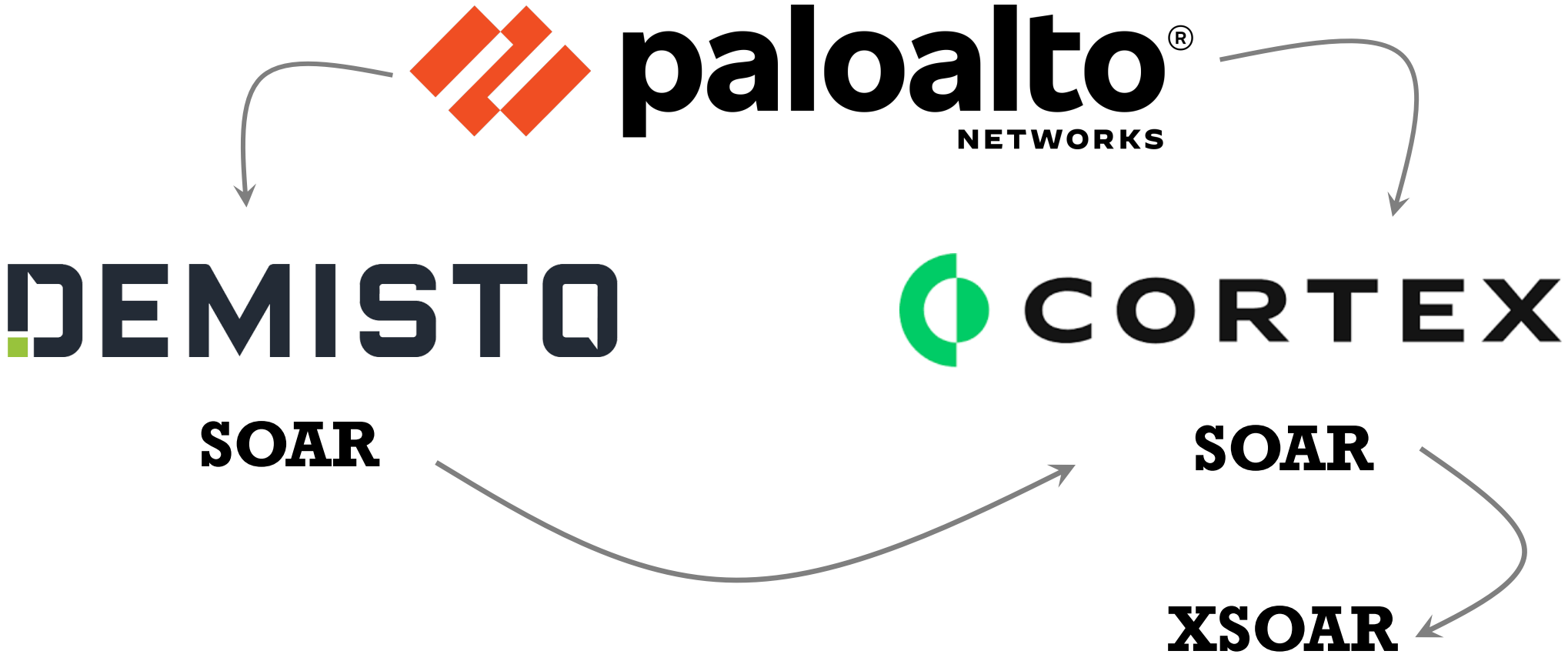
RAPID7 Insight connect

SWIMLANE

ThreatConnect

CORTEX XSOAR BY PALO ALTO NETWORKS

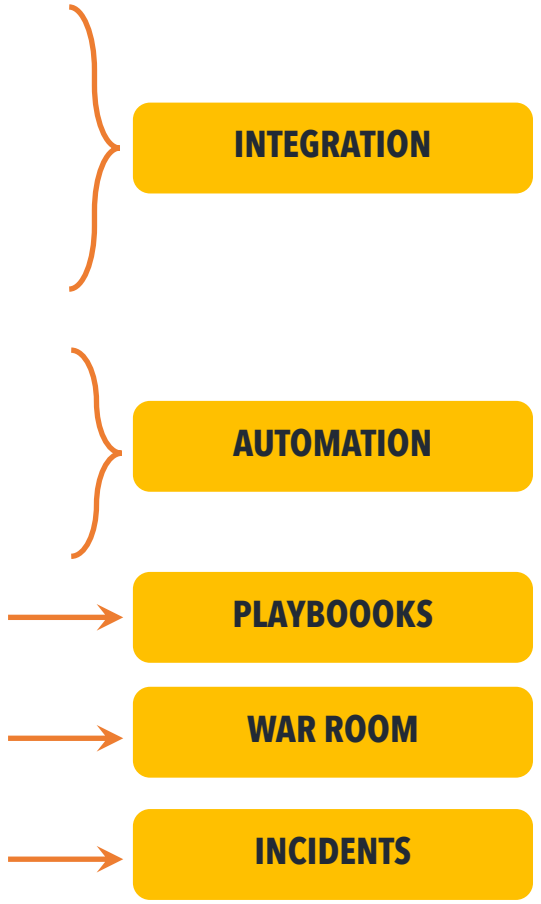
CORTEX XSOAR - History



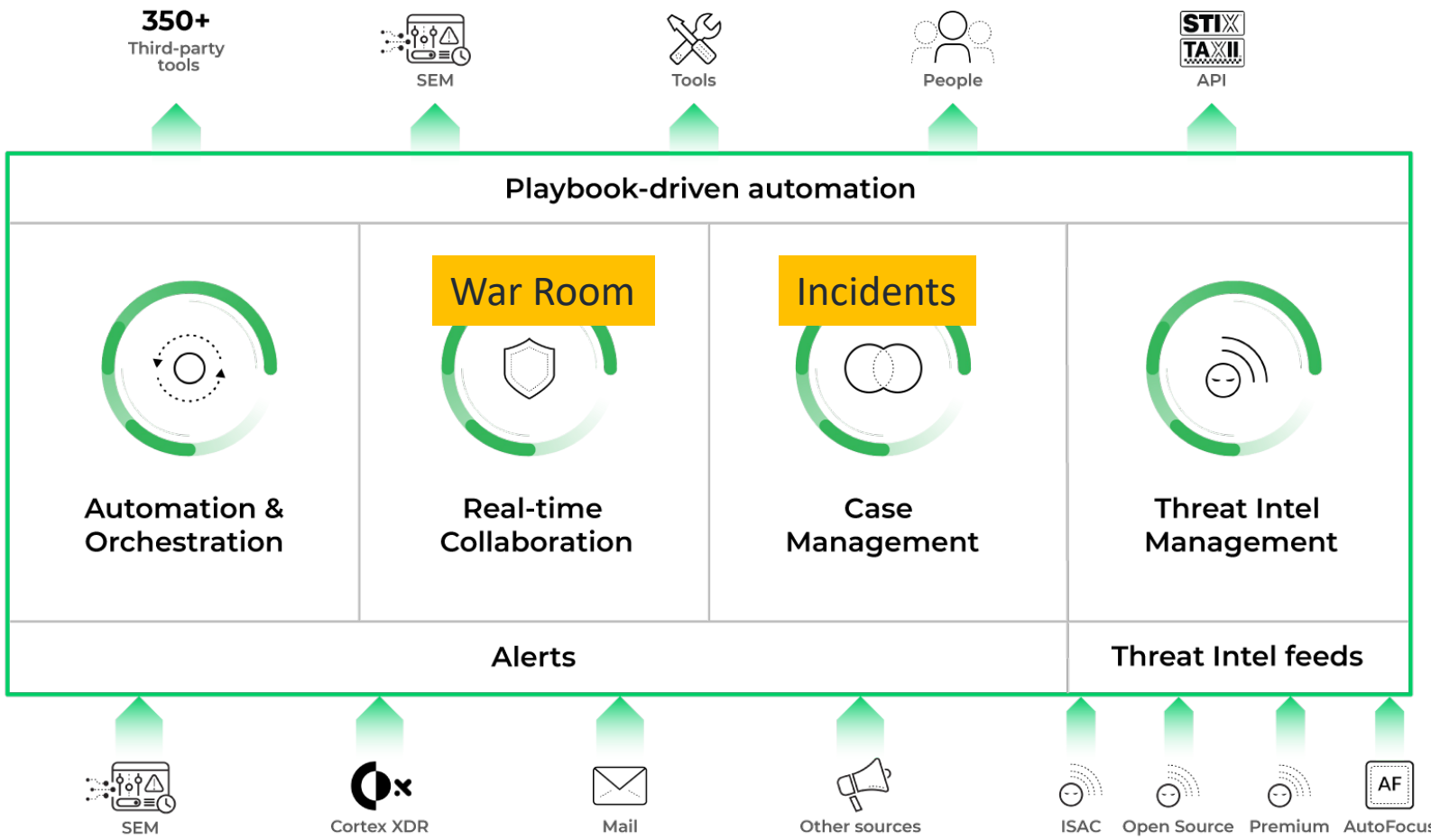
CORTEX XSOAR
BY PALO ALTO NETWORKS

CORTEX XSOAR - Features

- Should be able to pick up alerts
- Should work with multiple technologies
- Work with Threat Intelligence
- Able to query various technologies
- Able to make configuration changes
- Able to follow step-by-step instructions
- Document incident & Collaborate with peers
- Able to track progress of investigation



CORTEX XSOAR - Features



ASSIGNMENT

PALO ALTO BEACON

https://beacon.paloaltonetworks.com/student/catalog

Once you register and login:
https://beacon.paloaltonetworks.com/student/collection/666206-cortex-xsoar?sid=899781e6-c5fa-4a4b-9ba5-abe53127312e&sid_i=2