Security Automation

Reduce workload und speed
up your incident response

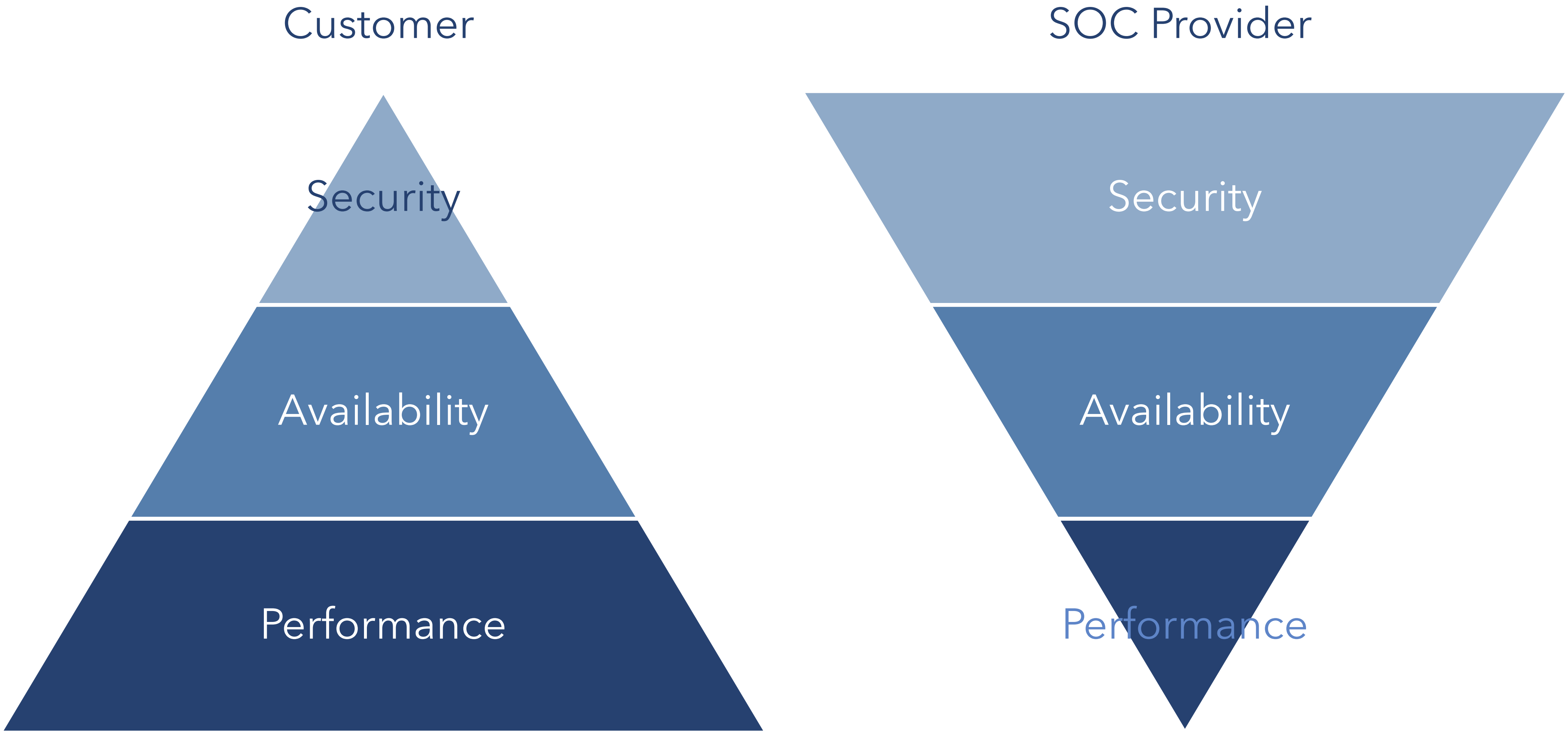
SOAR Service

What does a CISO think about it?

> “SOAR is powerful but dangerous !”

SOAR Service

Different Focus within IT-Organizations



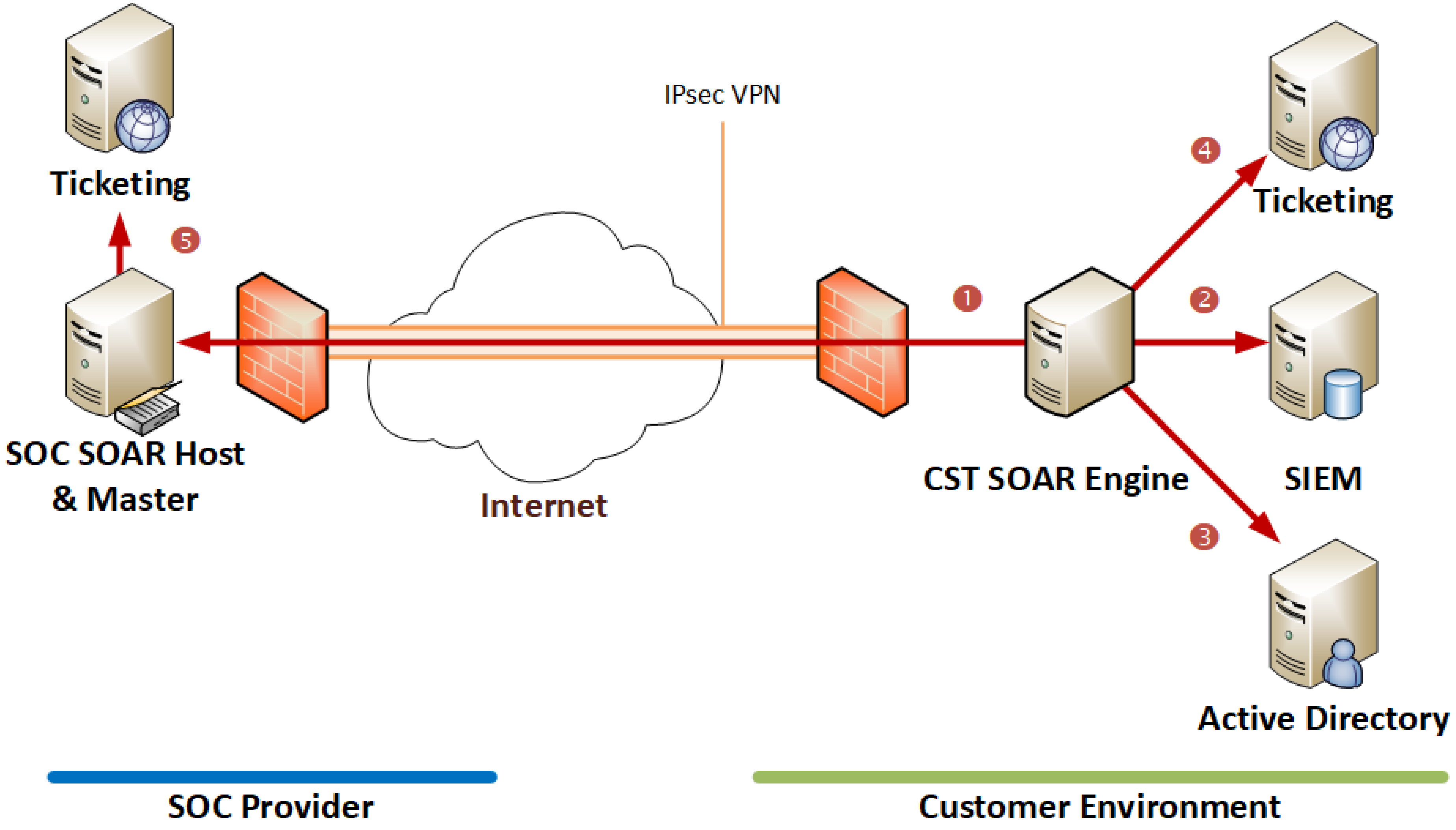
SOAR Service

How we prevent Supply Chain Attacks?

- Identify:
  - Understand the dependencies from your vendor in the details and document it
  - Practice attack scenarios frequently
  - We always try to prevent any flow of customer data to our premises and know exactly what we need, to deliver our service
  - Tailored monitoring of all communication of the SOAR system
- Protection:
  - Our SOAR solution is multi-tenant and all data is encrypted, if needed the customer can have his own Host and customer data stays at his premises (see architecture slides)
  - Our self developed tA SOC Management Framework helps to reduce the risks
- Detection:
  - terreActive SOC Management Framework includes among other things different detection tools
- Response:
  - terreActive SOC is build to protect our clients and ourselves

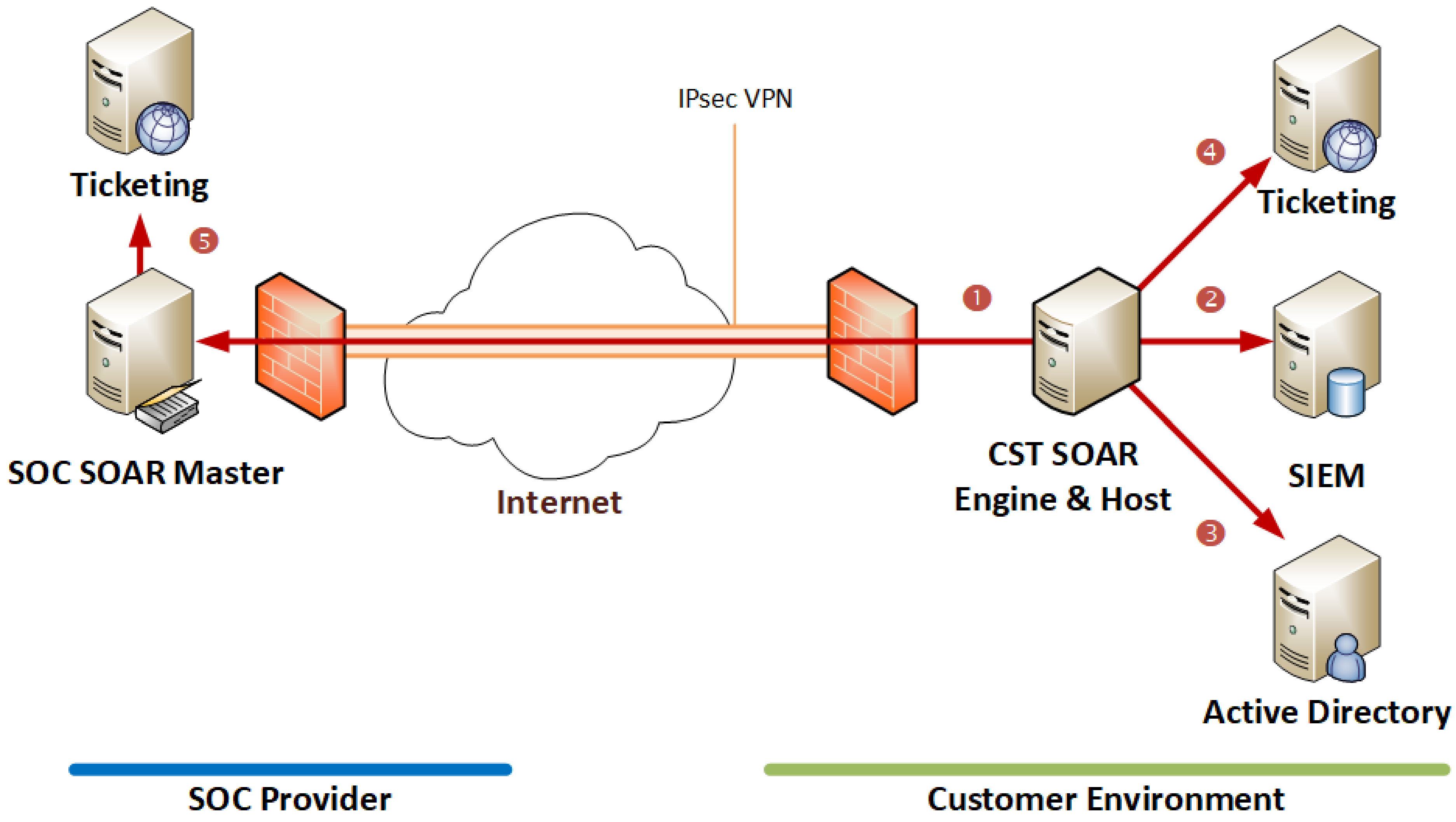
SOAR Service

Architecture Standard



SOAR Service

Architecture On Prem Host



SOAR Service

What does a Analyst think about it?

> “Let’s get rid of the boring stuff!”

SOAR Service

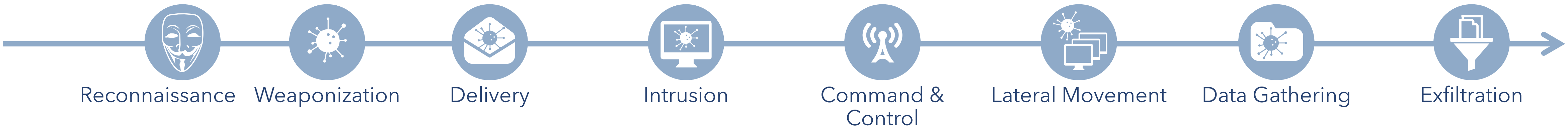
Why a SOC Analyst wants to use it?

- **Reduce manual work like:**
  - Close Use Cases that trigger more than once
  - Verify certain information
  - Enrichment of incident information
- **Exchange Information between the partners and teams**
  - Automated reporting about certain changes or findings
- **Automated response triggers some steps or a whole process**
  - Predefined analysis or actions as runbooks to perform individual tasks or automated response end-to-end
    - Isolate a certain host
    - Alarm our SOC if a certain SIEM alert triggers and another indicator was found.

SOAR Service

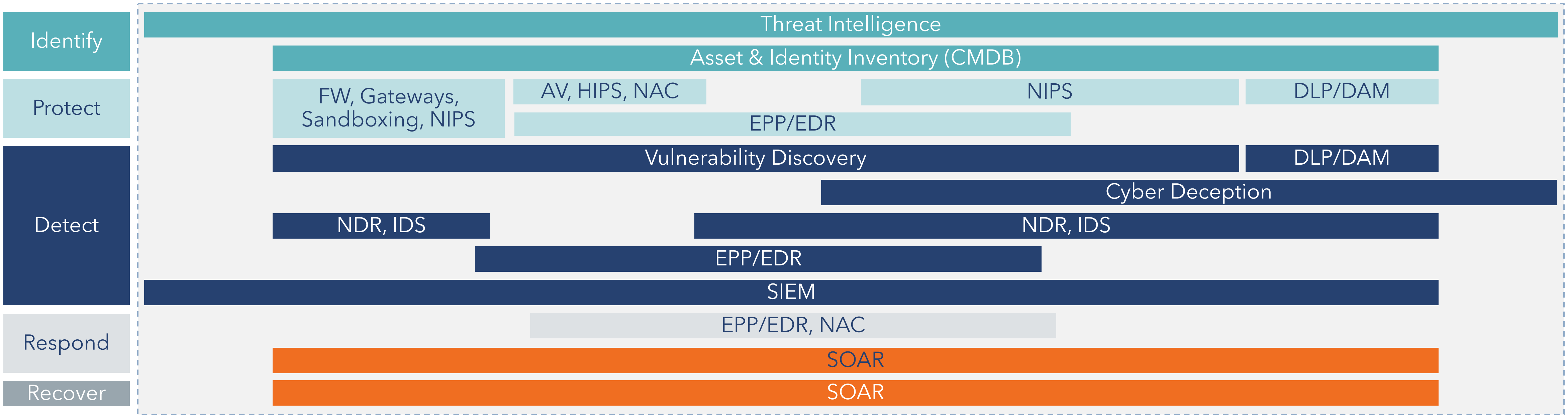
Within a Cyber Defense Platform

Attack Phases (Cyber Kill Chain)



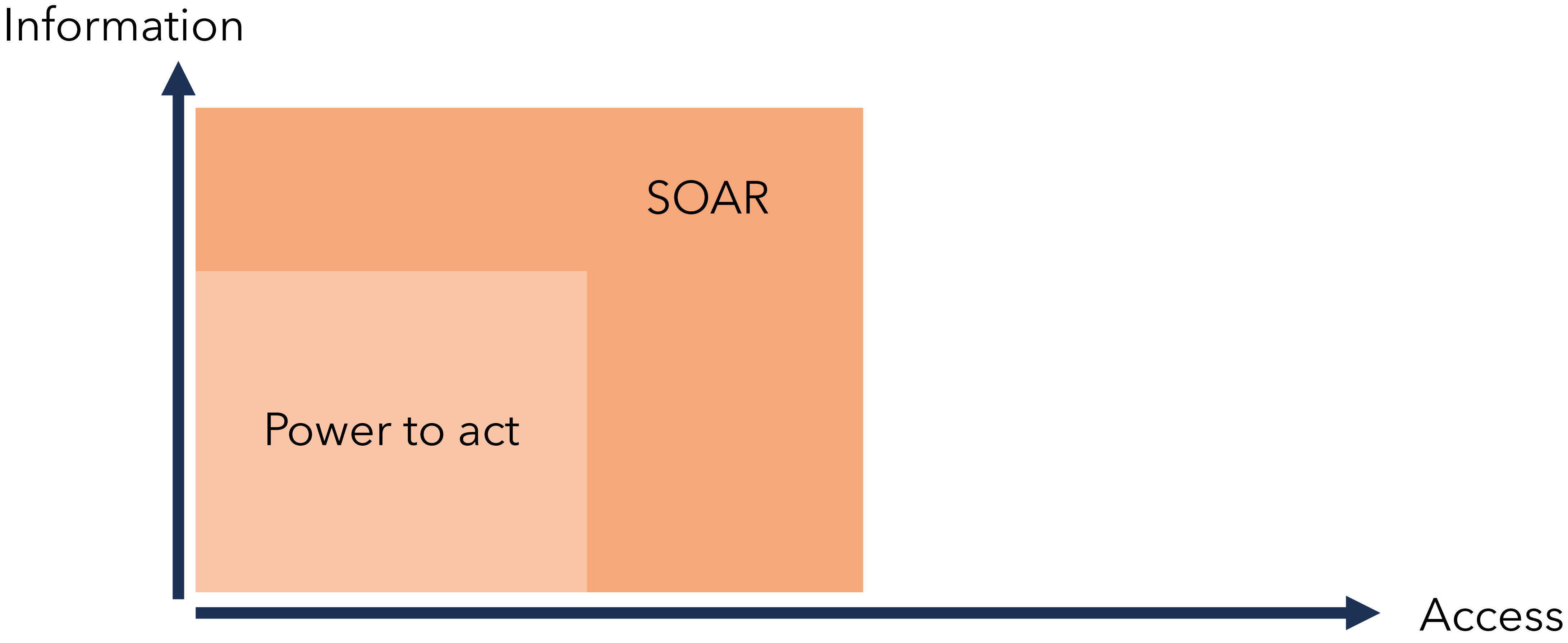
NIST

TOOLS FOR CYBER DEFENSE PLATFORM



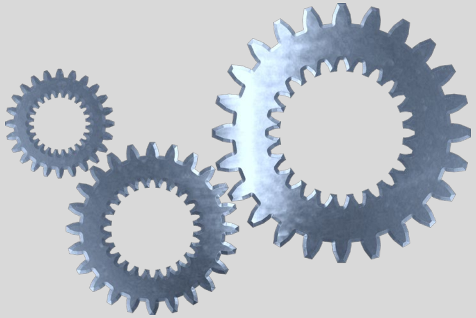
SOAR Service

Extension of SOC scope



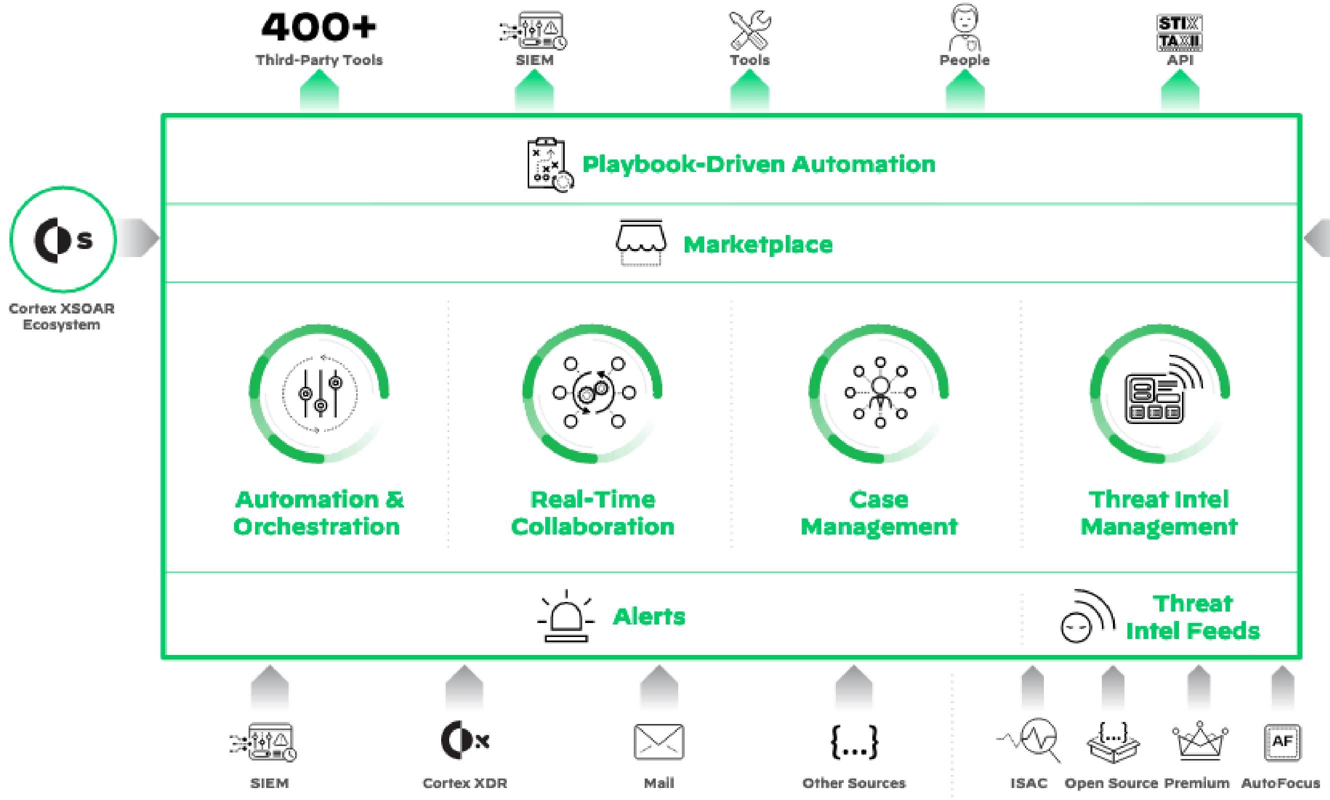
SOAR Scenarios

Phishing, Process Automation



SaaS Service: SOAR

XSOAR from Palo Alto



1. **Orchestration** across security product stack
2. **Automation** of tasks and workflows (80% of Tier-1 analyst)
3. **Incident response playbooks** (example phishing)
4. **Collaboration** on analysis and response in virtual War Room
5. **SLA** and performance **metrics**

SaaS Service: SOAR

Cyber Defense Platform Integration (Ticketing, …)

Analytics and SIEM	CORTEX DEVO exabeam FORTINET JASK LogRhythm McAfee MICRO FOCUS Radar splunk sumologic
Threat Intelligence	paloalto ALIEN VAULT ANOMALI COFENSE CYMON.io DOMAINTOOLS FARSIGHT SECURITY OpenPhish Recorded Future VirusTotal
Malware Analysis	paloalto cisco cuckoo FIREEYE INTEZER JOESecurity KOODOUS REVERSING LABS SNDBOX
Endpoint	CORTEX Carbon Black. CounterTack CROWDSTRIKE cybereason CYLANCE SentinelOne Symantec. TANIUM
Network Security	paloalto Check Point f5 PROTECTWISE Signal Sciences zscaler VECTRA tufin
Authentication	CYBERARK DUO Active Directory okta
Email Gateway	BitDam mimecast proofpoint. Symantec.
Ticketing	cherwell easyVISTA freshdesk Jira Software salesforce zendesk
Messaging	Exchange pagerduty slack twilio zoom
Cloud	CORTEX PRISMA aws Google Cloud Microsoft netskope

…and more!

SaaS Service: SOAR

Phishing attacks

High Alert Volumes

Phishing attacks are frequent, easy to execute, and act as the entry vector for most security attacks

Disjointed Processes

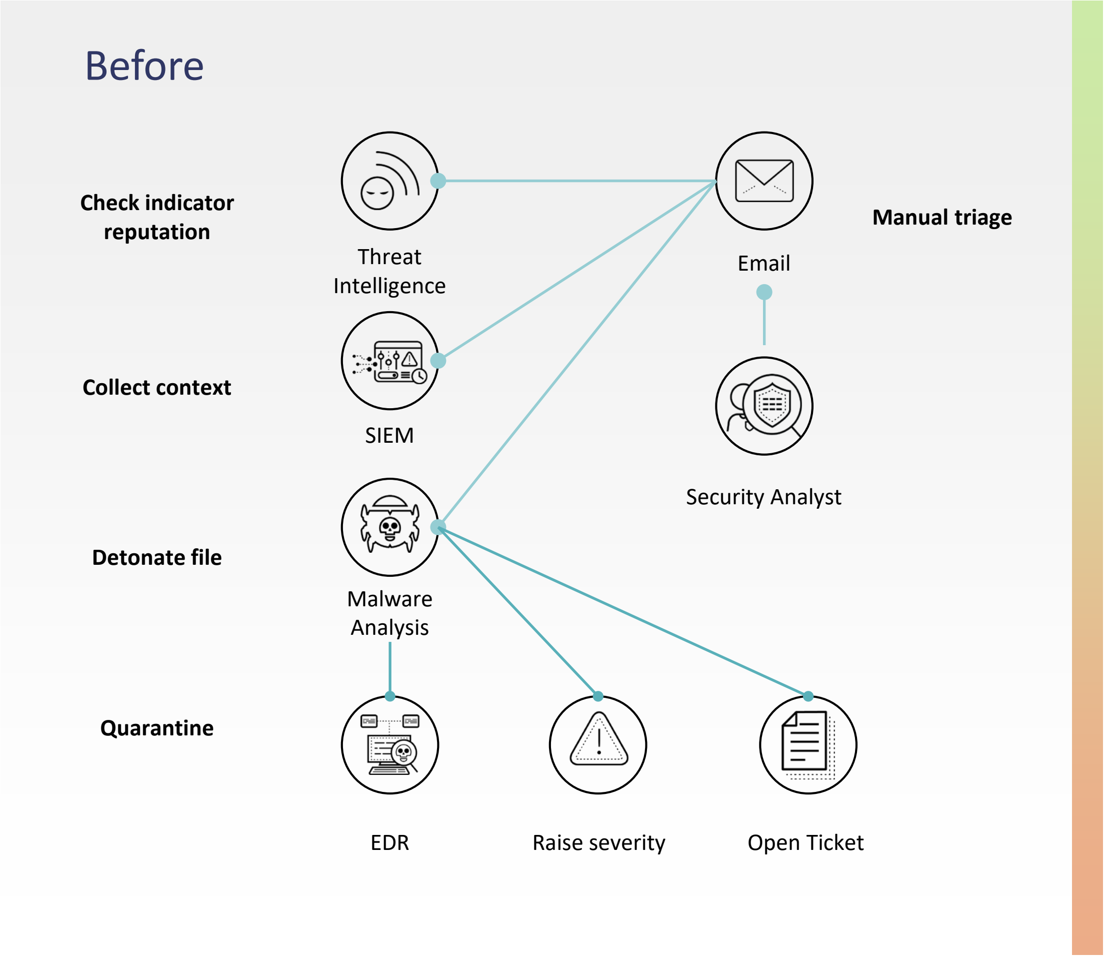
Security teams must coordinate across email inboxes, threat intel, NGFW, ticketing, and other tools for phishing response

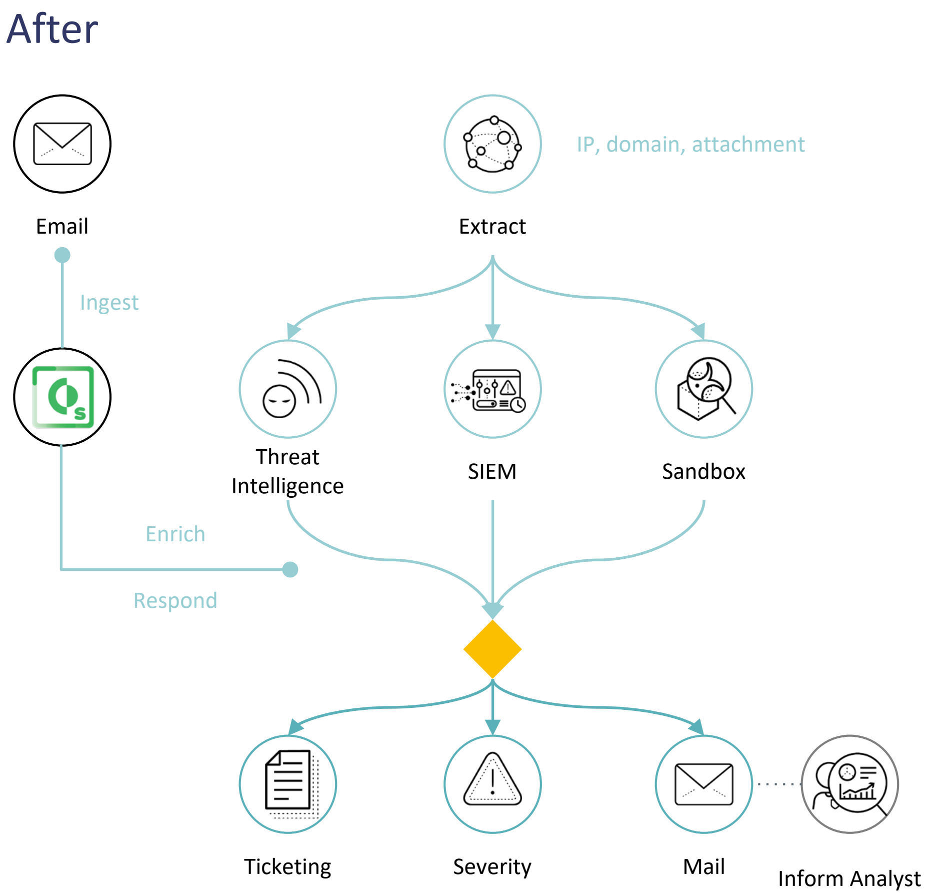
Ever-Present and Growing

95% of all attacks on enterprise networks are a result of spear phishing

SaaS Service: SOAR

Phishing attacks





SaaS Service: SOAR

Phishing attacks

Product Integrations

Cortex XSOAR integrates with all security tools commonly used for phishing enrichment and response

Intuitive Response Playbooks

OOTB and custom task-based workflows enable security teams to coordinate across teams, products, and infrastructures

Automated Actions

1000s of automated actions across security tools make scalable phishing response a reality

SaaS Service: SOAR

SOC process automation

Team Silos

Managing and responding to security incidents involves end users, IT team, NOC team, and other stakeholders

Shifting Context

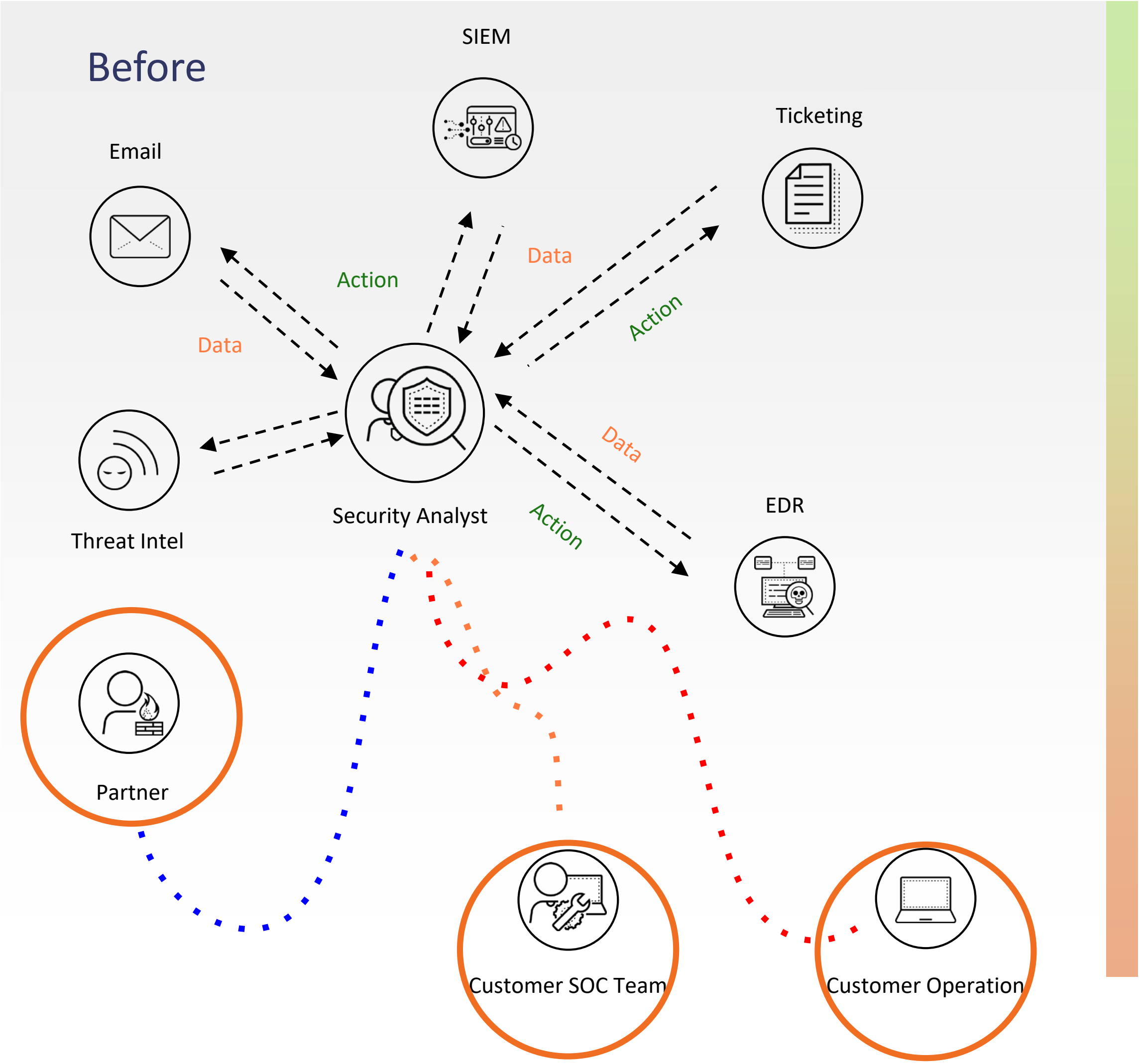
Coordinating across security tools involves shifting context, leading to rework and fragmented documentation

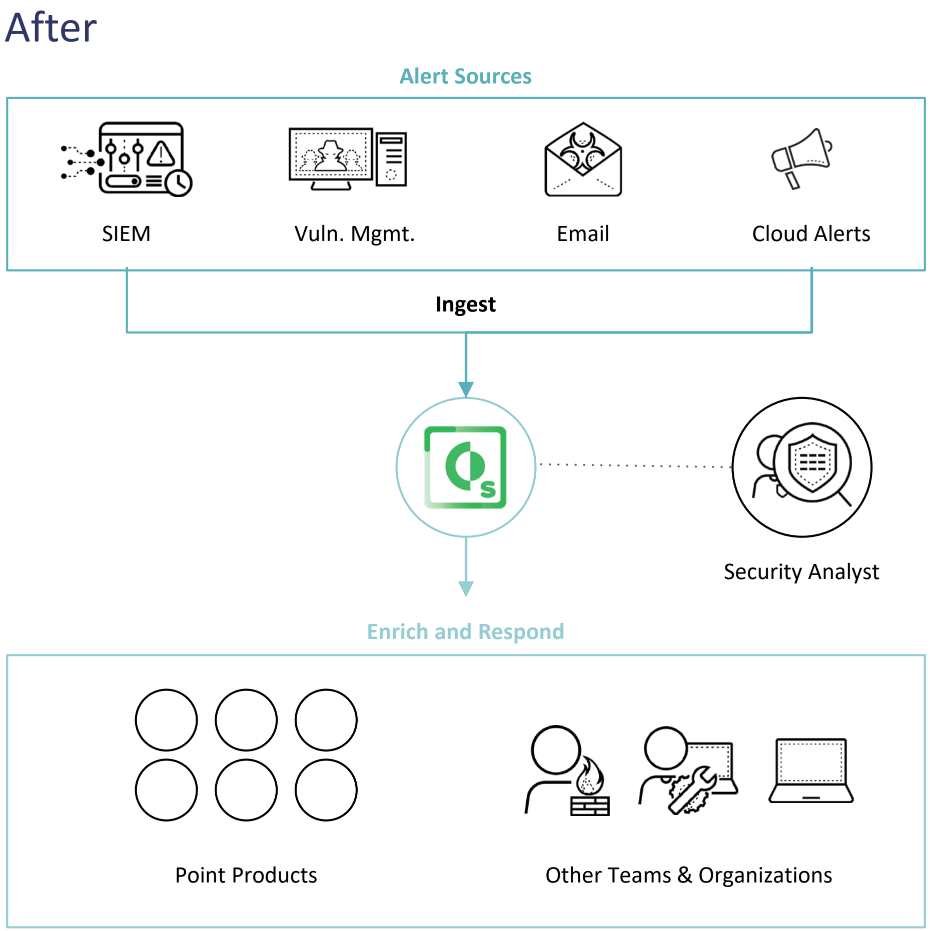
Lack of Metrics

Security teams lack the time, flexibility, and centralized data to visualize relevant metrics and track performance

SaaS Service: SOAR

SOC process automation





SaaS Service: SOAR

SOC process automation

Cross-team Communication

Communicate with end users, security teammates, and other teams, both in real-time and through automated tasks

Security Focused Context

Ingest all security alerts for centralized view and context across the incident response lifecycle

Respond in real-time

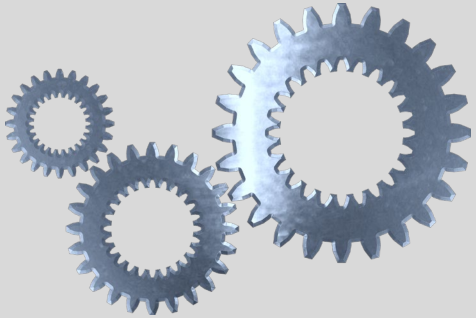
React in real time to new indicators as they are ingested

Cyber Security
since 1996

terreActive
terreActive
terreActive
terreActive

SOC process optimization

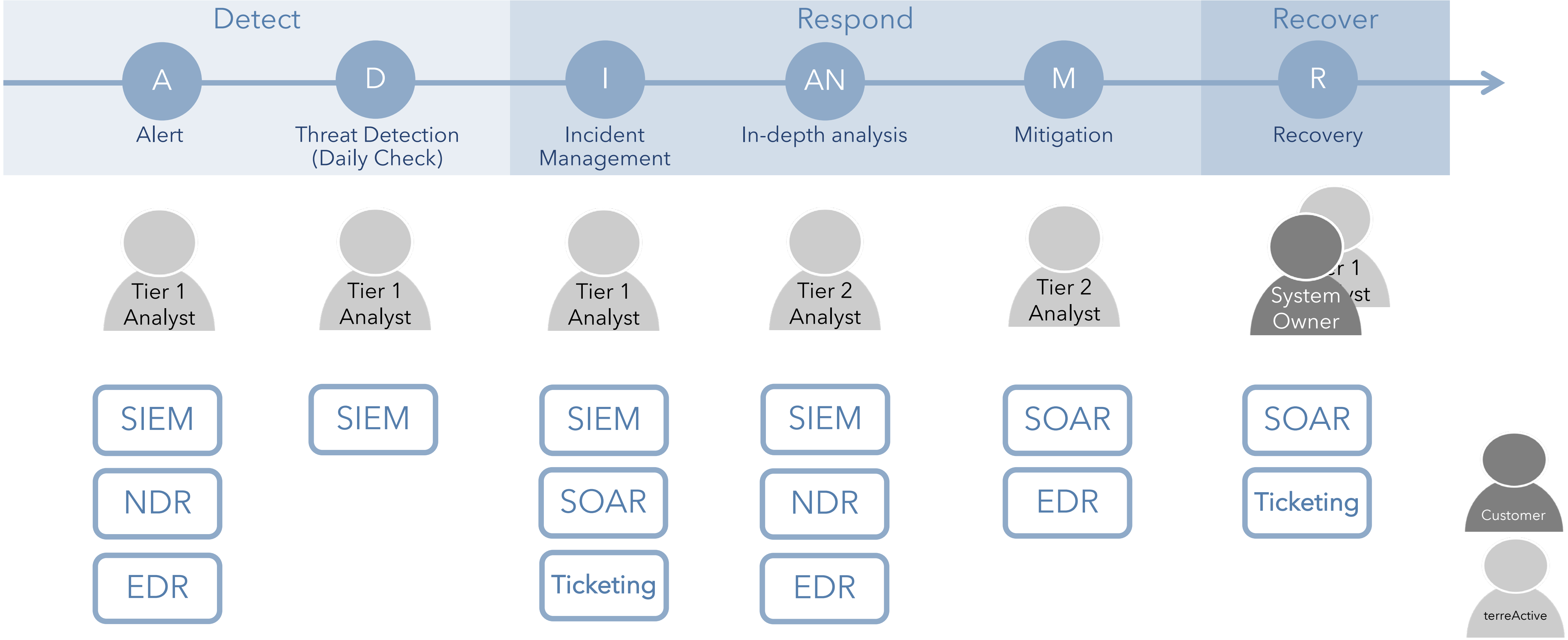
Roles, Steps, Tools



SOAR Service

Which tool is used by which role?

Detect & Response Phases

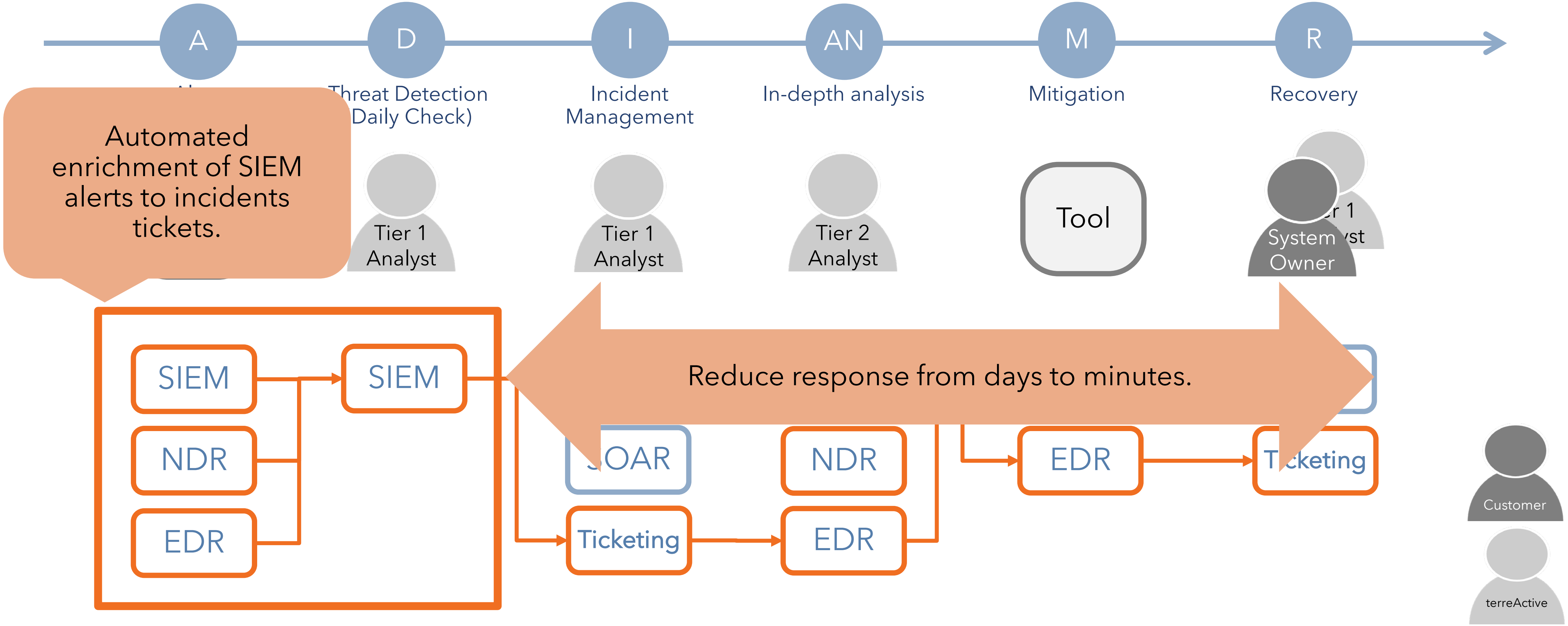


Detect		Respond			Recover
A	D	I	AN	M	R
Alert	Threat Detection (Daily Check)	Incident Management	In-depth analysis	Mitigation	Recovery
Tier 1 Analyst	Tier 1 Analyst	Tier 1 Analyst	Tier 2 Analyst	Tier 2 Analyst	System Owner Tier 1 Analyst
SIEM	SIEM	SIEM	SIEM	SOAR	SOAR
NDR		SOAR	NDR	EDR	Ticketing
EDR		Ticketing	EDR		

SOAR Service

SOC Process optimization

Detect & Response Phases

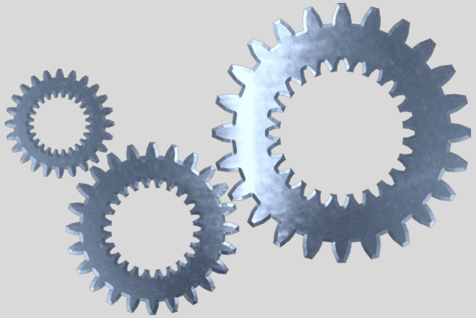


Automated enrichment of SIEM alerts to incidents tickets.

Reduce response from days to minutes.

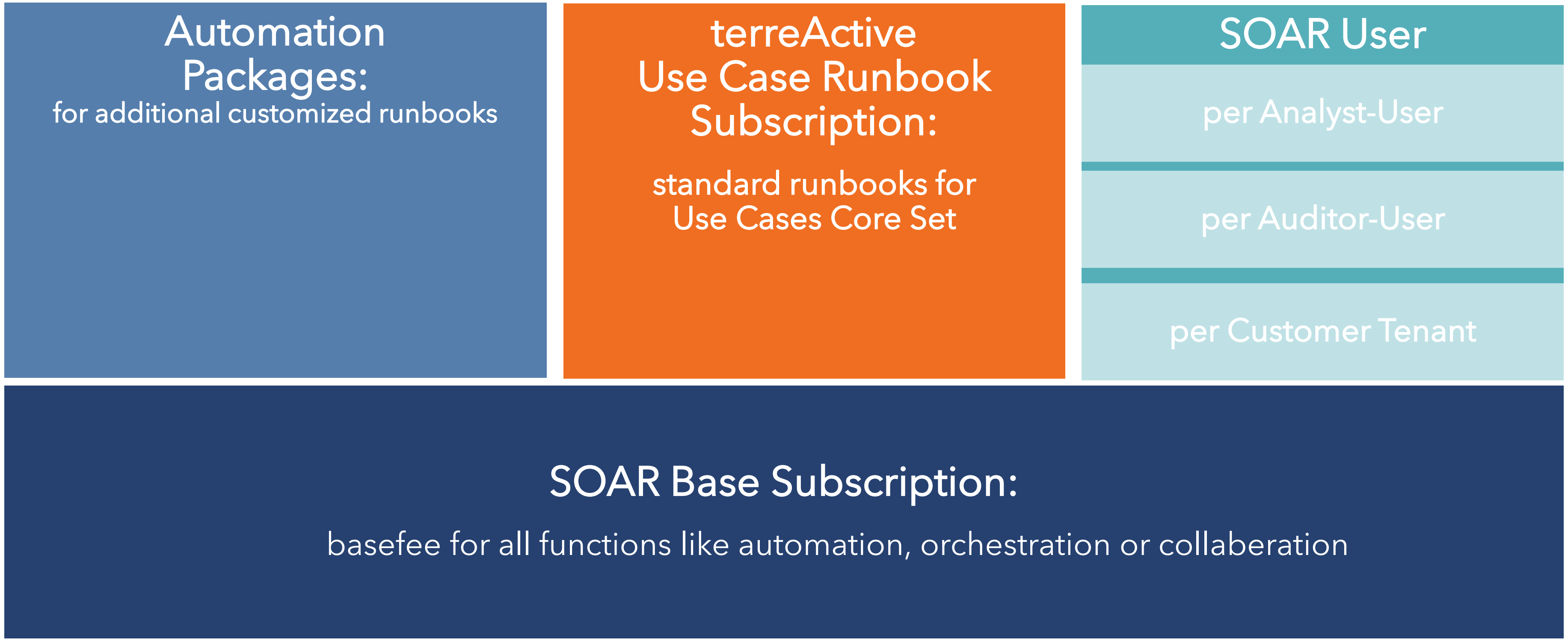
Is SOAR for everyone?

Modules, Deployment, Conclusion



SOAR Service

Service modules



Automation Packages: for additional customized runbooks

terreActive Use Case Runbook Subscription: standard runbooks for Use Cases Core Set

SOAR User

- per Analyst-User
- per Auditor-User
- per Customer Tenant

SOAR Base Subscription: basefee for all functions like automation, orchestration or collaberation

- SOAR as a SaaS service for new customer segments
- SOAR as SaaS service reduces complexity and operation cost
- SOAR service modules allow a individual implementation for each customer

SOAR Service

Customer integration

Customer	Engine	Ticketing	Use Case Playbooks	User	Case Management
A	OK	OK	OK	In Progress	In Progress
B	OK	-	OK	-	-
C	OK	In Progress	OK	-	-
D	In Progress	-	OK	-	-
E	OK	OK	In Progress	-	-

SOAR Service

Why SOAR?

	Goal	Result (real customer data)
Save Resources & reduce Budget	Reduce variable cost and manual work for the SOC and the customer's organization.	9650 automated actions within 3 months 1 minute for each action = 19 days (8.4h/day) saved per quarter **Manual work down by 6 days a month!**
Optimize quality	Integration of all important sources and process design through the experts from customer, partner and SOC.	Direct response through 7x24 organization Response process used by anyone in charge **Quality of experts done by anyone**
Act faster & broader	Extend the scope of action for the SOC and automate information gathering or mitigation tasks.	Fast response to alerts 7x24 with on call organization SOC scope extension **MTTR down by 80%!**

Contact

We secure your success

Cyber Security
since 1996

terreActive
terreActive
terreActive
terreActive

Rolf Hefti

rolf.hefti@terreActive.ch

terreActive AG
Kasinostrasse 30
CH-5001 Aarau

www.security.ch

+41 62 834 00 55
info@terreActive.ch