PREVENT
DETECT
RESPOND
HUNT.

Endpoint Security - Completed.

Weltweit wird mehr Geld mit IT-Kriminalität verdient als mit dem organisierten Drogenhandel!

Zitat: Arne Schönbohm, BSI President (Dezember 2016)

Protection alleine reicht nicht mehr aus!
Wir sollten aktiv nach Bedrohungen auf Endpunkten suchen und diese eleminieren bevor ein Vorfall passiert!

What's key to you?

Increase your level of SECURITY?		What are you doing against file-less Malware?
Increase PERFORMANCE and stability		Can you work productively on your systems?
Improving OPERATIONAL efficiency		How much time do you need to manage and maintain your current solution?
Increase level of AUTOMATION and INTEGRATION		Should your systems collaborate better?
Get complete VISIBILITY		What is really happening on your systems?
What else?		Is there anything we missed?

THE CONCEPT

Managed Detection & Response

SentinelOne

ONE Agent
Working straight at the ENDPOINT

Building the CENTER of your Endpoint Security

Endpoint Security – Completed.

How does it work?

The Workflow

SentinelOne

Endpoint Protection
Pre-Execution
Static AI

PE - PDF - Office Docs

ActiveEDR
Autonomous Behavioral AI
Story Tracking

Lateral Movement - Fileless - Exploits - scripts/macros

Fighting the unknown!
How will the story end?

https://www.theverge.com/2012/6/24/3113237/minority-report-idea-summit-predicted-the-future

Kryptik Ransomware 2.exe

More

ACTIONS

CLASSIFICATION

STATUS

Alert — Kill — Quarantine — Remediate

File Info

File: Kryptik Ransomware 2.exe
Path: \Device\HarddiskVolume2\Users\admin\Desktop\ Copy path

Device: Enterprise-Desktop
Console visible IP: 12.124.76.22
IP Address: 172.16.48.159, 172.16.48.159
Domain: WORKGROUP
Username: ENTERPRISE-DESK\admin
Agent Version: 3.1.1.12
Site: Demo TEST
Group: Default Group

Identified: 05/03/2019 11:02:32
Reported at: 05/03/2019 11:02:33

Seen on network: 3 times

Summary

S1 Risk levels:

SHA1: a56f82902
Recorded Fu

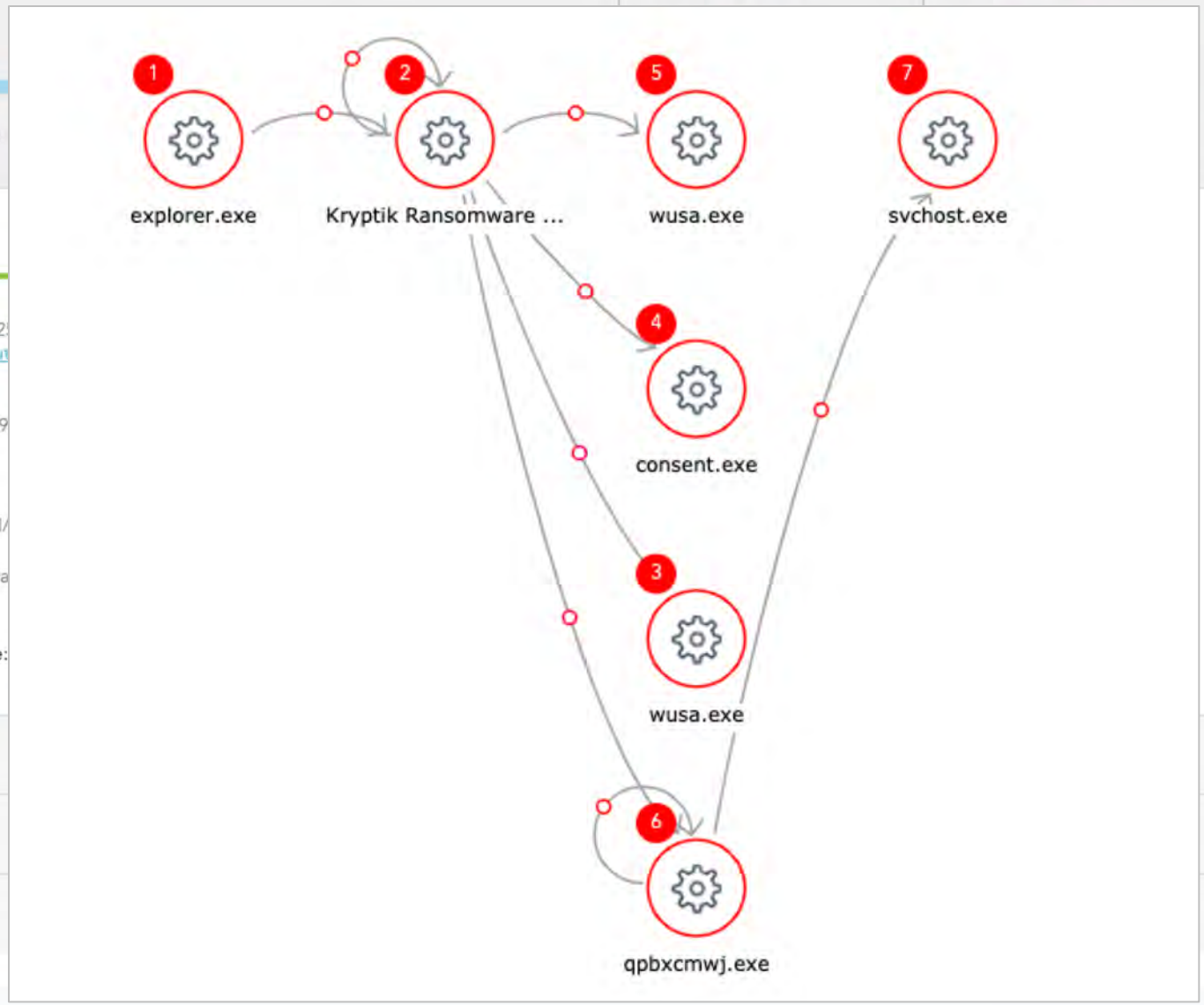
SHA256:
b89442fbf112a2c9

Signer Identity: N/

Kryptik Ransomwa
Ver: N/A

Detecting engine:

Download threat file



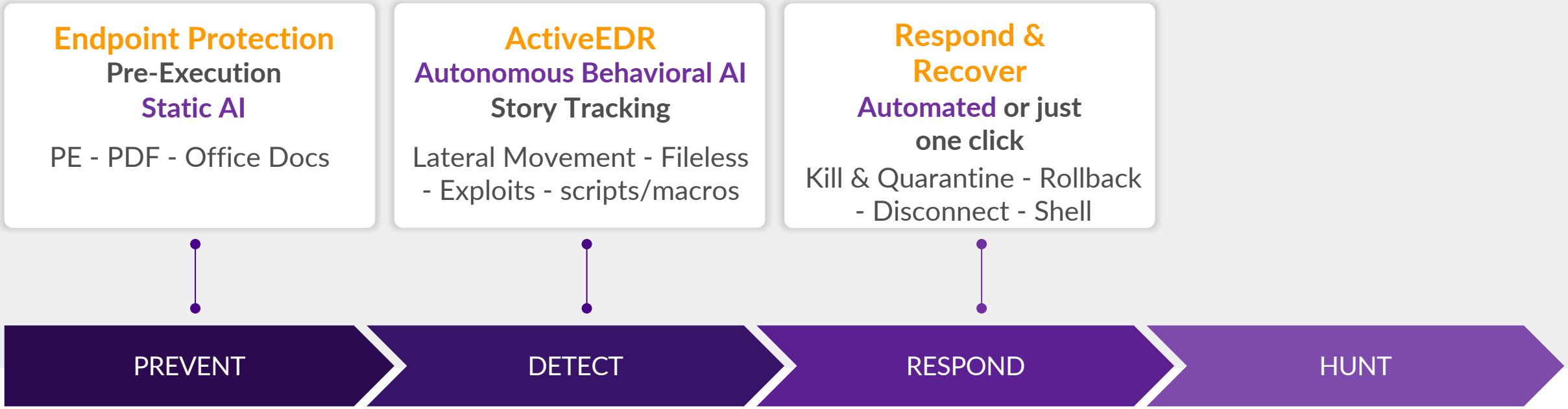
ENDPOINT NETWORK CONNECTION

ATTACK OVERVIEW

ATTACK STORY LINE

The Workflow

SentinelOne



The Workflow

Endpoint Protection
Pre-Execution
Static AI
PE - PDF - Office Docs

ActiveEDR
Autonomous Behavioral AI
Story Tracking
Lateral Movement - Fileless - Exploits - scripts/macros

Respond & Recover
Automated or just one click
Kill & Quarantine - Rollback - Disconnect - Shell

Timeframe = Seconds

One Agent | Automated | Not cloud reliant

The Workflow

SentinelOne

Endpoint Protection
Pre-Execution
Static AI
PE - PDF - Office Docs

ActiveEDR
Autonomous Behavioral AI
Story Tracking
Lateral Movement - Fileless - Exploits - scripts/macros

Respond & Recover
Automated or just one click
Kill & Quarantine - Rollback - Disconnect - Shell

ActiveEDR Advanced
Deep Visibility
Threat Hunting
Visibility - Ease Of Use - Living Off the Land Detection

PREVENT | DETECT | RESPOND | HUNT

Timeframe = Seconds
One Agent | Automated | Not cloud reliant

Timeframe = 90+ Days
Agent Maintains TrueContext

ONE AGENT | ONE PLATFORM

SentinelOne

Any OS

- Windows
- Linux
- macOS
- VDI

Any Deployment

- Cloud
- GovCloud
- On-prem
- Hybrid

Any Connection

- Online
- Offline

Any Integration

300+

APIs

Any Person

- Big team
- One person
- No team

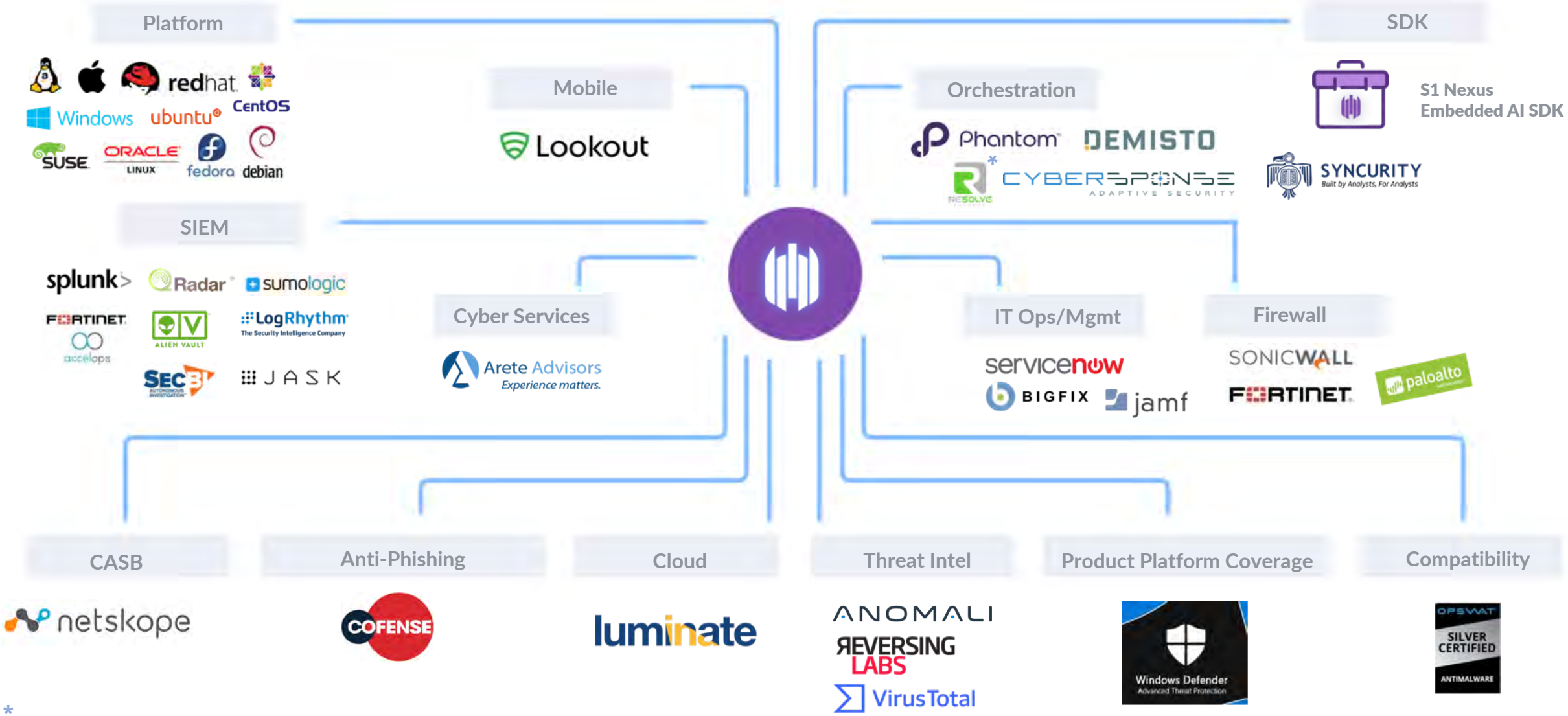
Any Response

- Automated
- Manual
- Vigilance MDR

Features

- USB Control
- Bluetooth Control
- Firewall Control
- Threat Hunting
- Full Remote Shell
- Vulnerability Reporting
- Advanced Remediation

S1 Nexus Integration Ecosystem
An API-First Approach



*

Vigilance

SentinelOne's MDR Offering

Monitor

Empower and accelerate your security team with expert advice

Benefit from actionable recommendations, and security event prioritization.

Coverage 365 days, 24/7
First response SLA Standard

Respond

Ensure business continuity and network hygiene in near real-time

Utilize SentinelOne experts to act upon your security events

Coverage 365 days, 24/7
First response SLA Premium

Deploy

Just looking for a quick start?

Ensure successful onboarding with Vigilance Deploy with 90 days of tuning of policies, threat handling, exclusions, and deployment best practices.

Alle 20 Minuten verliebt sich ein Kunde.

SentinelOne™