paloalto NETWORKS | Cybersecurity Partner of Choice

CYBERSECURITY OPERATIONS

Didzis Ozoliņš
Systems engineer

Setting up the stage, a simplified enterprise

Responsible for Endpoints. Care about other things.	Responsible for Firewalls. Care about global reachability.	Responsible for Security. Care about security, not about operations.	Common enemy
Sick of being exposed. Want to be left alone.	Always blamed first. Want to be left alone.	Make other people lifes harder. Want to be involved.	
Ease of deployment. No false positives.	Throughput, port density. Ease of software upgrades. Network protocol support.	Products which can be maintained without involving anybody else (SIEM, i.e.)	

Fix security team needs and it will automagically fix a lot of other stuff as well.

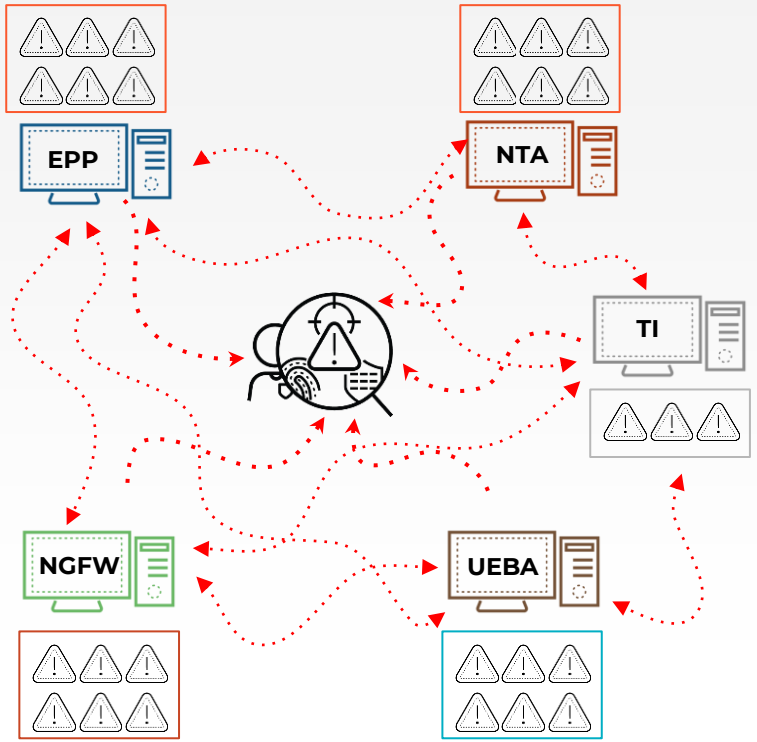
- Selecting the right tools
- Security rules → SecOps
- Security logs → SecOps
- Single source of truth
- …

- Independent analysis
- Root cause identification
- Single source of truth
- …

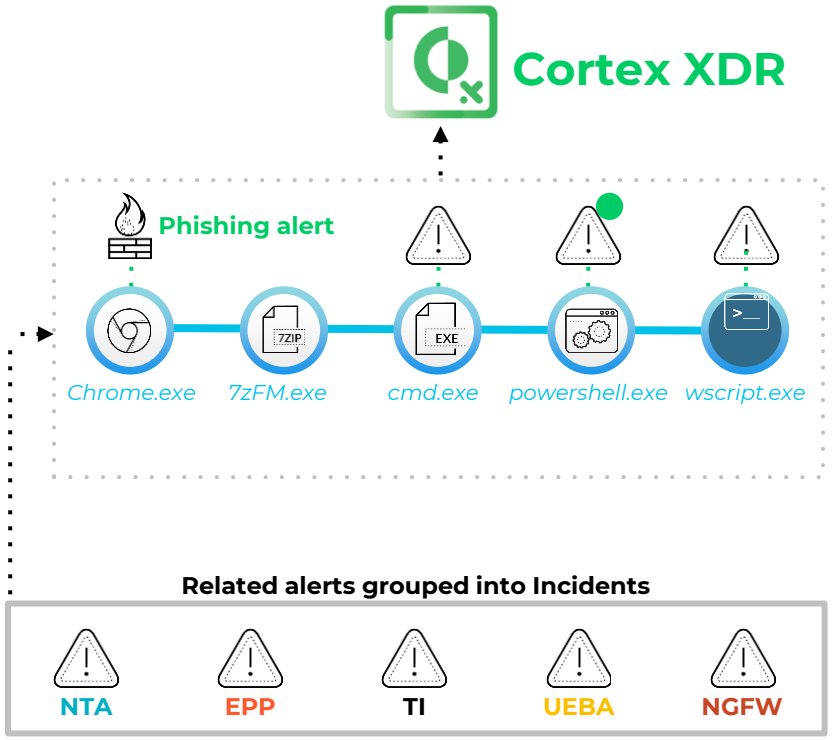
- Single source of truth
- …

Everybody's dream - independent investigation by security analyst

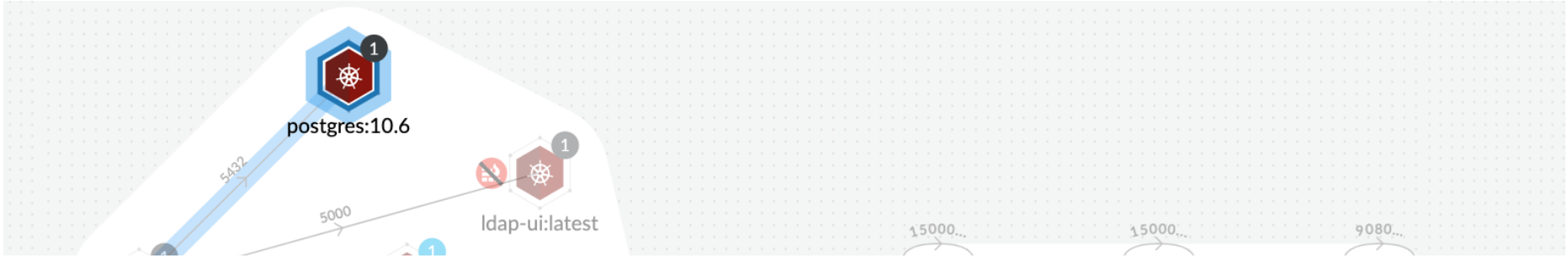
Before



After



Single source of truth



Type	Highest severity	Description
Application	high	postgres version 10.6 has 2 vulnerabilities

Severity	Package	CVE	Fix Status	Grace period	Risk factors	Description	Tags
high	postgres	CVE-2021-43766	Fixed in: 13.5, 12.9, 11.14,... 40 days ago		4	Impacted versions: <10.19,10 and >=10.0,10 Discovered: 40 days ago Published: 40 days ago Odyssey passes to server unencrypted bytes from man-in-the-middle When Odyssey is configured to use certificate Common Name for client authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first	

Single source of truth

Vulnerabilities | **Compliance** | Runtime | Layers | Process info | Package info | Environment | Trust groups | Labels

Filter compliance by keywords and attributes

4 total entries

ID	Category	Severity	Result	Description
425	twistlock	high	Fail	Private keys stored in image
406	CIS	medium	Fail	(CIS_Docker_v1.3.1 - 4.6) Add HEALTHCHECK instruction to the container image
422	twistlock	critical	Pass	Image contains malware
424	twistlock	high	Pass	Sensitive information provided in environment variables

Decisions based on actual state of your system.

Summary, the outcome

1. Take away functions from your employees **they do not do anyway;**
2. Serve information for security team **on a plate;**
3. **Single source of truth** for asset inventory, vulnerability and compliance management;
4. **..**

Security is now a board-level issue.

Palo Alto Networks

We provide next-gen cybersecurity to enable cyber transformation

Security Operations

- **Network Security**
- **Cloud Security**
- **Endpoint Security**

Threat Intelligence and Incident Response

85k+ customers

 |

8

paloalto NETWORKS | Cybersecurity Partner of Choice

THANK YOU

Didzis Ozoliņš
dozolins@paloaltonetworks.com