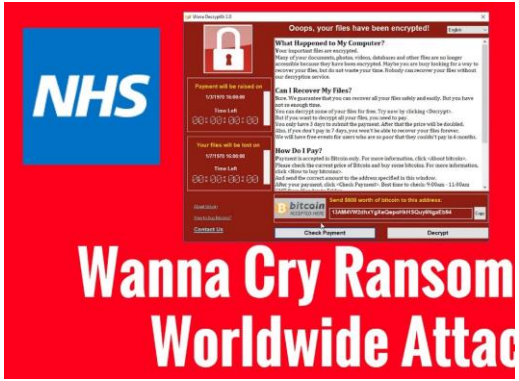
Kako zaznati napade, ki jih nihče ne zazna?

4. april, 2019. Vladimir Ban, Vodilni expert za implementacijo varnostnih rešitev

Varnostni krog



Below is a summary of incidents from 2018 and 2019. For the full list, click the download link above.

February 2019. State-sponsored hackers were caught in the early stages of gaining access to computer systems at the Australian Federal Parliament

February 2019. European aerospace company Airbus reveals it was targeted by Chinese hackers who stole the personal and IT identification information of some of its European employees

February 2019. Norwegian software firm Visma revealed that it had been targeted by hackers from the Chinese Ministry of State Security who were attempting to steal trade secrets from the firm's clients

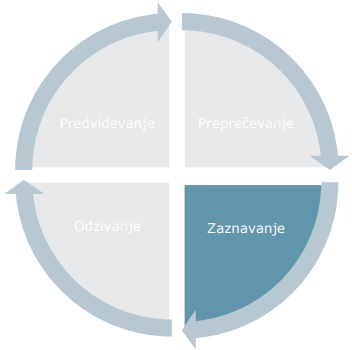
January 2019. Hackers associated with the Russian intelligence services were found to have targeted the Center for Strategic and International Studies

January 2019. The U.S. Department of Justice announced an operation to disrupt a North Korean botnet that had been used to target companies in the media, aerospace, financial, and critical infrastructure sectors

Skrbniki, lastniki

Napadalci

Dovolj je ena napaka….

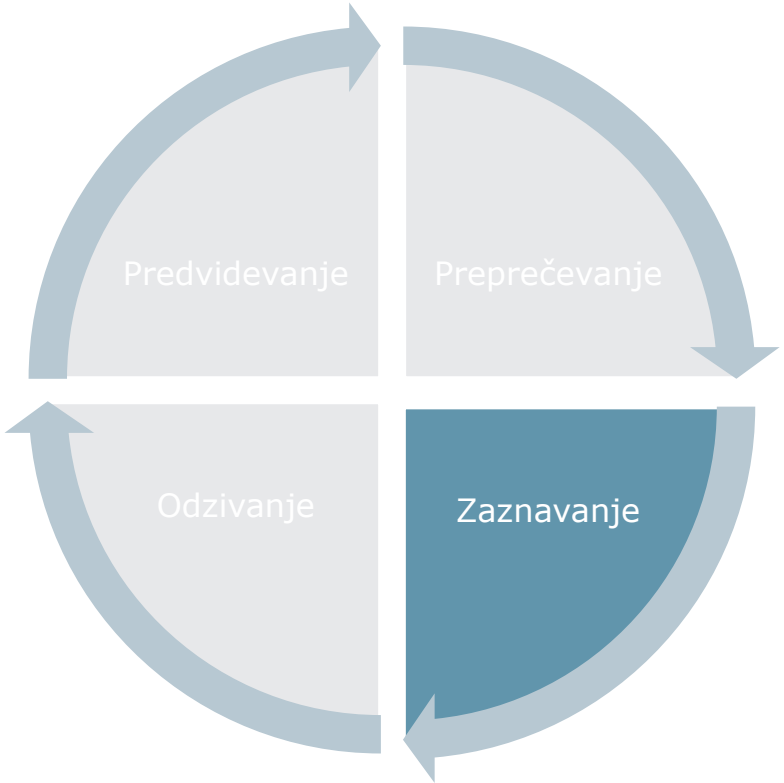


Napadalci

Dovolj je ena napaka….

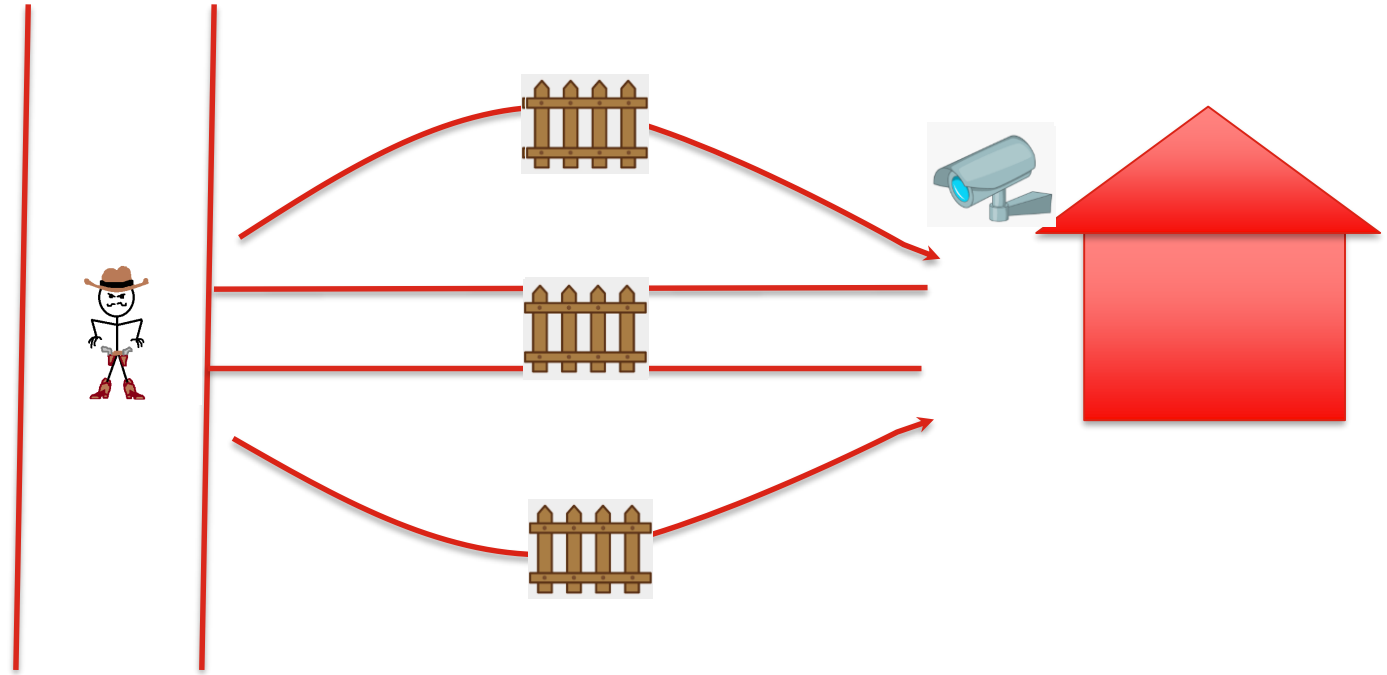
Skrbniki, lastniki

Varnostni krog




WHERE
IS THE CATCH...
memegenerator.net

Kaj je sploh razlika med preprečevanjem in zaznavanjem?



Kaj je sploh razlika med preprečevanjem in zaznavanjem?

Če obe metodi temeljita na enostavnem predvidevanju, razlike niti ni…

Če zaznavanju dodamo „inteligenco“, je razlika lahko očitna…

AI Security system

Procesu zaznavanja anomalij dodamo umetno inteligenco

Trije različni zorni koti razumevanja AI varnostnih sistemov

- Pogled napadalca: Kaj je sedaj drugače?
- Pogled skrbnika: Kaj so možne napake pri implementaciji sistema?
- Pogled matematika: Kako AI inteligenca sploh deluje?

Pogled matematika – osnovni pristop

Zajem prometa/podatkov → Identifikacija struktur v podatkih → Zajem prometa/podatkov → Iskanje razlik/anomalij v strukturi

Standard algorithm [edit]

The most common algorithm uses an iterative refinement technique. Due to its ubiquity it is often called the *k*-means algorithm; it is also referred to as Lloyd's algorithm, particularly in the computer science community.

Given an initial set of *k* means $m_1^{(1)},\ldots,m_k^{(1)}$ (see below), the algorithm proceeds by alternating between two steps:[6]

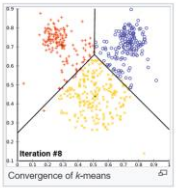
Assignment step: Assign each observation to the cluster whose mean has the least squared Euclidean distance, this is intuitively the "nearest" mean.[7] (Mathematically, this means partitioning the observations according to the Voronoi diagram generated by the means).

$$S_i^{(t)} = \left\{ x_p : \left\| x_p - m_i^{(t)} \right\|^2 \le \left\| x_p - m_j^{(t)} \right\|^2 \forall j, 1 \le j \le k \right\},$$

where each x_p is assigned to exactly one $S^{(t)}$, even if it could be assigned to two or more of them.

Update step: Calculate the new means to be the centroids of the observations in the new clusters.

$$m_i^{(t+1)} = \frac{1}{|S_i^{(t)}|} \sum_{x_j \in S_i^{(t)}} x_j$$



Convergence of *k*-means

The algorithm has converged when the assignments no longer change. The algorithm does not guarantee to find the optimum.[8]

The algorithm is often presented as assigning objects to the nearest cluster by distance. Using a different distance function other than (squared) Euclidean distance may stop the algorithm from converging. Various modifications of *k*-means such as spherical *k*-means and *k*-medoids have been proposed to allow using other distance measures.

Initialization methods [edit]

Pogled matematika – osnovni pristop

Unsupervized machine learning

\+

- Anomalije se zelo efektivno odkrijejo

–

- Vsaka anomalija še ni varnostni dogodek, zaradi česar imamo v tej fazi veliko število „lažnih“ alarmov

Pogled matematika – dodatni pristop

Upoštevanja znanih metod poteka napada

Vzpostavitev vhodnih podatkov za AI algoritme

Pregled zajetega prometa s temi algoritmi

Iskanje kandidatov za varnostne incidente

Decision tree learning is a method commonly used in data mining.[1] The goal is to create a model that predicts the value of a target variable based on several input variables. An example is shown in the diagram at right. Each interior node corresponds to one of the input variables; there are edges to children for each of the possible values of that input variable. Each leaf represents a value of the target variable given the values of the input variables represented by the path from the root to the leaf.

A decision tree is a simple representation for classifying examples. For this section, assume that all of the input features have finite discrete domains, and there is a single target feature called the "classification". Each element of the domain of the classification is called a *class*. A decision tree or a classification tree is a tree in which each internal (non-leaf) node is labeled with an input feature. The arcs coming from a node labeled with an input feature are labeled with each of the possible values of the target or output feature or the arc leads to a subordinate decision node on a different input feature. Each leaf of the tree is labeled with a class or a probability distribution over the classes, signifying that the data set has been classified by the tree into either a specific class, or into a particular probability distribution (which, if the decision tree is well-constructed, is skewed towards certain subsets of classes).

A tree can be "learned"[clarification needed] by splitting the source set[clarification needed] into subsets based on an attribute value test[clarification needed][citation needed]. This process is repeated on each derived subset in a recursive manner called recursive partitioning. The recursion is completed when the subset at a node has all the same value of the target variable, or when splitting no longer adds value to the predictions. This process of *top-down induction of decision trees* (TDIDT)[2] is an example of a greedy algorithm, and it is by far the most common strategy for learning decision trees from data[citation needed].

In data mining, decision trees can be described also as the combination of mathematical and computational techniques to aid the description, categorization and generalization of a given set of data.

Data comes in records of the form:

$$(\mathbf{x}, Y) = (x_1, x_2, x_3, \ldots, x_k, Y)$$

The dependent variable, Y, is the target variable that we are trying to understand, classify or generalize. The vector **x** is composed of the features, x_1, x_2, x_3 etc., that are used for that task.

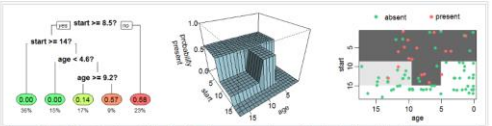
A tree showing survival of passengers on the Titanic ("sibsp" is the number of spouses or siblings aboard). The figures under the leaves show the probability of survival and the percentage of observations in the leaf. Summarizing: Your chances of survival were good if you were (i) a female or (ii) a male younger than 9.5 years with less than 2.5 siblings.

Decision tree types [edit]

Decision trees used in data mining are of two main types:

- **Classification tree** analysis is when the predicted outcome is the class (discrete) to which the data belongs.
- **Regression tree** analysis is when the predicted outcome can be considered a real number (e.g. the price of a house, or a patient's length of stay in a hospital).

The term **Classification And Regression Tree (CART)** analysis is an umbrella term used to refer to both of the above procedures, first introduced by Breiman et al. in 1984.[3] Trees used for regression and trees used for classification have some similarities - but also some differences, such as the procedure used to determine where to split.[3]



An example tree which estimates the probability of kyphosis after surgery, given the age of the patient and the vertebra at which surgery was started. The same tree is shown in three different ways. **Left** The colored leaves show the probability of kyphosis after surgery, and percentage of patients in the leaf. **Middle** The tree as a perspective plot. **Right** Aerial view of the middle plot. The probability of kyphosis after surgery is higher

Pogled matematika – dodatni pristop

Supervized machine learning

\+

- Zaznane anomalije lahko opredelimo glede varnosti

–

- Smo se vrnili na „predvidevanja“?

Pogled matematika

Supervized machine learning

+

Unsupervized machine learning

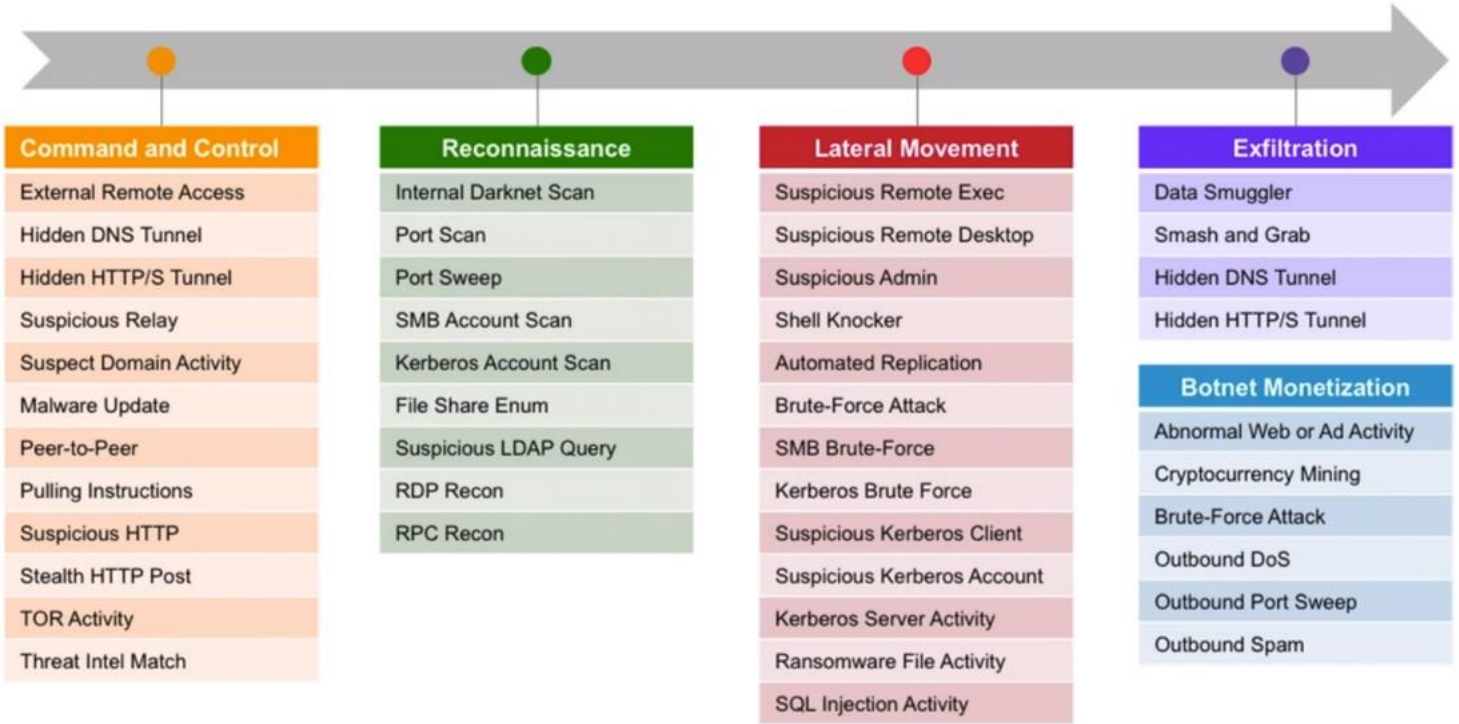
Pogled napadalca

Izogniti se unsupervized metodi zaznavanja

Upati, da je sistem nepopolno postavljen

Upadi, da skrbniki ne bodo reagirali na alarme

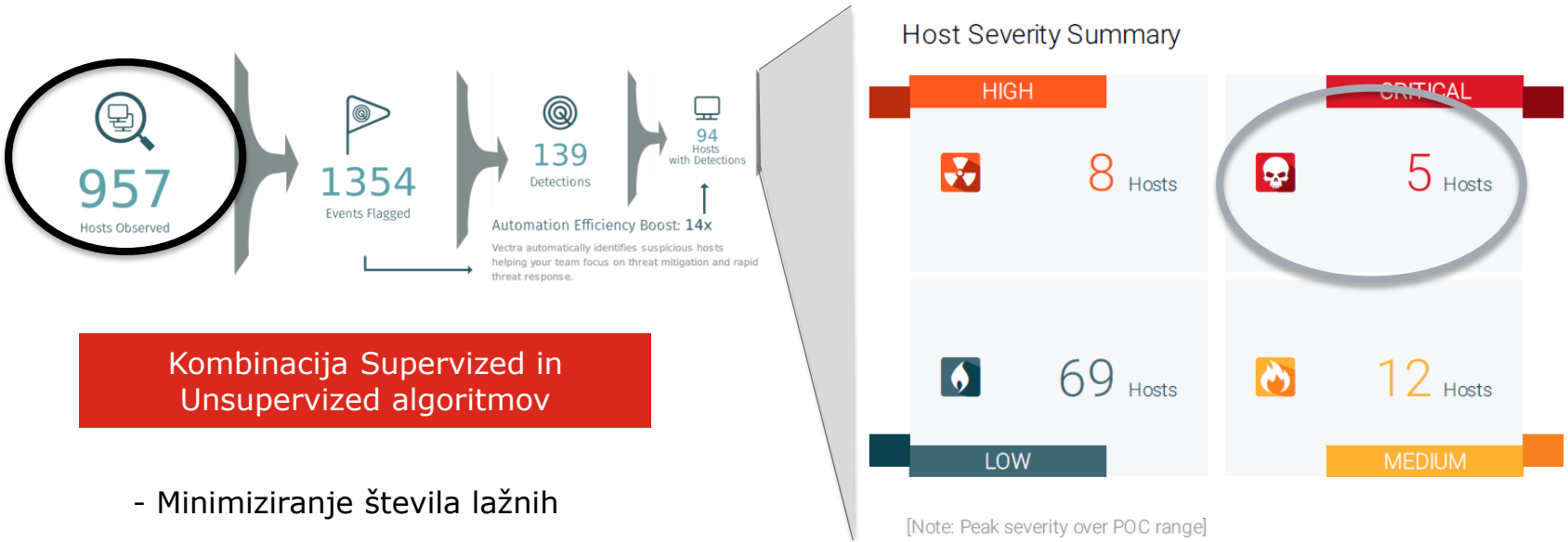
Pogled napadalca – supervized metologija



Pogled skrbnika

- Je alarmov preveč?
- Kako iz alarma dobiti širšo sliko?
- Kako zajeti celotno okolje?
- Kako izkoristiti obstoječe varnostne sisteme?

Pogled skrbnika – je alarmov preveč?



Kombinacija Supervized in Unsupervized algoritmov

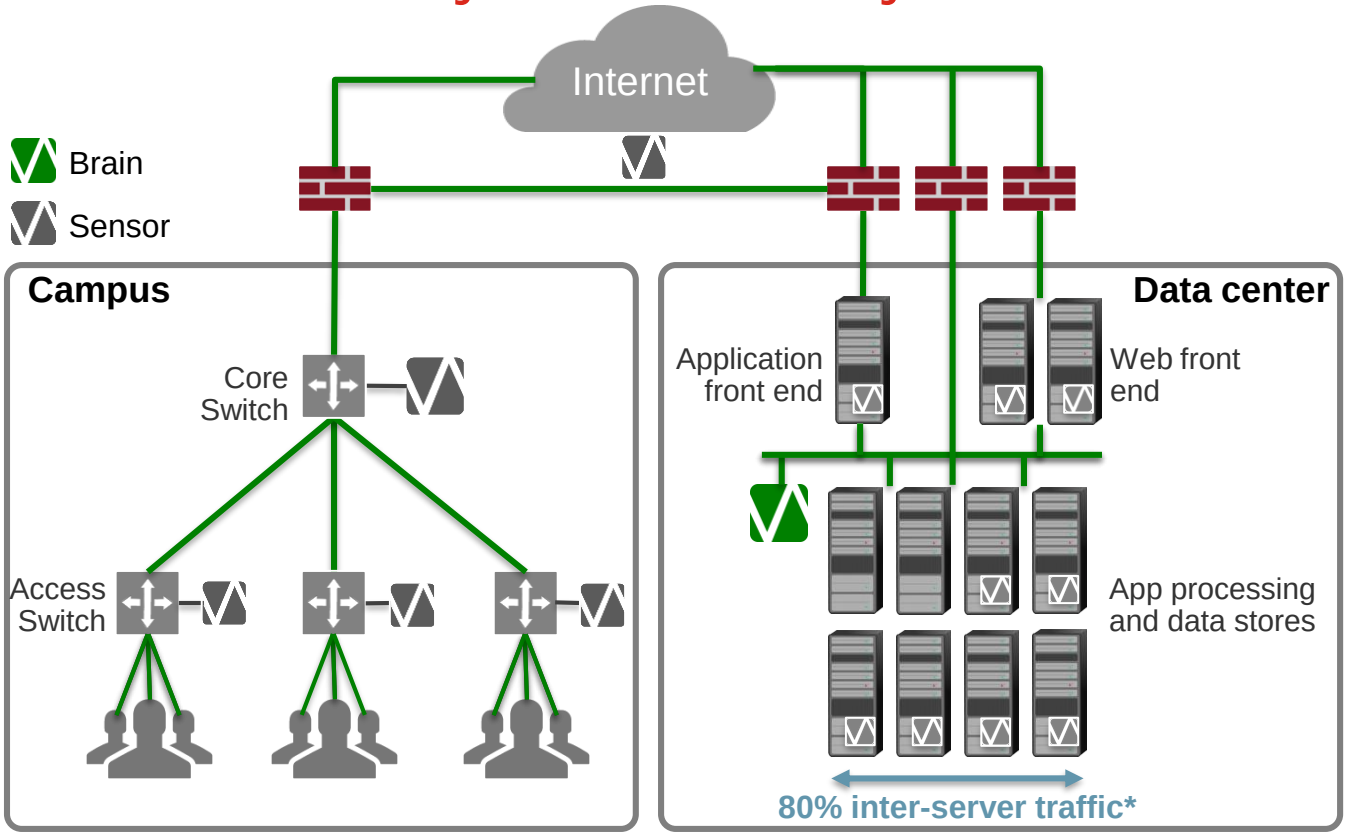
- Minimiziranje števila lažnih alarmov

Pogled skrbnika – kako iz alarma dobiti širšo sliko?

Vectra Cognito Recall

- Vpogled v zgodovino podatkov in dogodkov
- Rekonstruiranje dogodkov „za nazaj“

Pogled skrbnika – kako zajeti celotno okolje



Pogled skrbnika – kako izkoristiti obstoječe varnostne sisteme?

Endpoint/vCenter context

CARBON BLACK ARM YOUR ENDPOINTS

vmware

Ticketing / IR

JIRA

servicenow

SIEM

splunk>

ArcSight An HP Company

Radar

VECTRA

Visibility

Gigamon

ixia

Security Orchestration

Endpoint

CARBON BLACK ARM YOUR ENDPOINTS

CROWDSTRIKE

McAfee

Symantec.

TANIUM

NAC

CISCO ISE

ForeScout

Firewall

paloalto NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD.

JUNIPER NETWORKS

CISCO

Pogled skrbnika – kako izkoristiti obstoječe varnosne sisteme?

- Samodejno odzivanje in preprečevanje napadov
- Hitrejša analiza grožnje
- Integracija z obstoječimi procesi
- …..

Povzetek

- **PREVENCIJA** (na žalost) ni dovolj
- AI je pomemben za **DETEKCIJO**
- Izziv ni zaznati anomalijo, ampak **UGOTOVITI KATERA ANOMALIJA PREDSTAVLJA VARNOSTNO GROŽNJO**
- V detekcijo je potrebno zajeti **CELOTEN** promet
- Potrebno je videti **GOZD** in ne samo dreves
- AI **NI NADOMESTEK** za varnostne sisteme, ampak je dodatek varnostnim sistemom (ter procesom!)

Thank you

Vladimir.ban@a1.si