Microsoft

IOC για τις ταυτότητες του Azure Active Directory

Daniel Wood

Διαχειριστής προγράμματος

Ασφάλεια ταυτότητας Azure Active Directory

18 Φεβρουαρίου 2021

Σειρά βίντεο Solorigate

4 μοτίβα επιθέσεων στο Azure Active Directory

01 Μοτίβο 1: Πλαστά διακριτικά SAML με χρήση του υλικού υπογραφής διακριτικών SAML που έχει κλαπεί

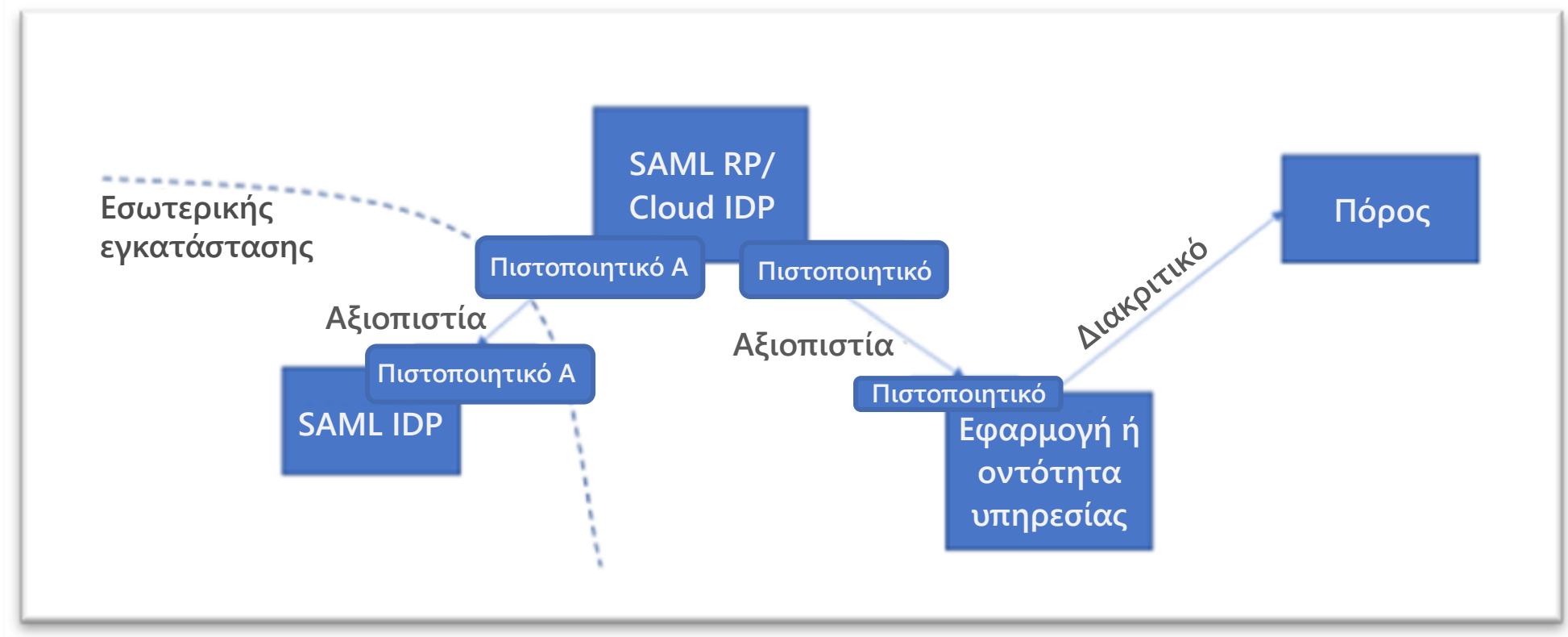
02 Μοτίβο 2: Παράνομες εγγραφές για τις σχέσεις αξιοπιστίας SAML.

03 Μοτίβο 3: Προσθήκη διαπιστευτηρίων σε υπάρχουσες εφαρμογές

04 Μοτίβο 4: Ερωτήματα που μιμούνται υπάρχουσες εφαρμογές

Microsoft Security

Σειρά βίντεο Solorigate



01. Μοτίβο

Πλαστά διακριτικά SAML με χρήση του υλικού υπογραφής διακριτικών SAML που έχει κλαπεί

Τι πρέπει να αναζητήσετε:

- Διακριτικά SAML που λαμβάνονται από το SP με ρυθμίσεις παραμέτρων που αποκλίνουν από τη διαμορφωμένη συμπεριφορά της υπηρεσίας παροχής ταυτότητας (IDP).
- Διακριτικά SAML που λαμβάνονται από το SP χωρίς αντίστοιχα αρχεία καταγραφής στην υπηρεσία παροχής ταυτότητας (IDP).
- Διακριτικά SAML που λαμβάνονται από το SP με αξιώσεις MFA αλλά χωρίς αντίστοιχα αρχεία καταγραφής δραστηριότητας MFA στην υπηρεσία παροχής ταυτότητας (IDP).
- Διακριτικά SAML που λαμβάνονται από διευθύνσεις IP, παράγοντες, χρόνους ή για υπηρεσίες που είναι μη κανονικές για τη σχετική ταυτότητα που αντιπροσωπεύεται στο διακριτικό.
- Αποδεικτικά στοιχεία μη εξουσιοδοτημένης δραστηριότητας διαχείρισης.

Τι πρέπει να κάνετε:

1	Προσδιορίστε τον μηχανισμό κρυφής εξαγωγής και αποκατάστασης πιστοποιητικών.
2	Διανέμετε όλα τα πιστοποιητικά υπογραφής διακριτικών SAML.
3	Εξετάστε το ενδεχόμενο να μειώσετε την εξάρτησή σας από την αξιοπιστία SAML εσωτερικής εγκατάστασης όπου αυτό είναι εφικτό.
4	Εξετάστε το ενδεχόμενο να χρησιμοποιήσετε ένα HSM για να διαχειριστείτε τα πιστοποιητικά υπογραφής διακριτικών SAML (TSC).

02. Μοτίβο

Παράνομες εγγραφές για τις σχέσεις αξιοπιστίας SAML

Τι πρέπει να αναζητήσετε:

Μη κανονική διαχειριστική περίοδος λειτουργίας που σχετίζεται με την τροποποίηση σχέσεων αξιοπιστίας ομοσπονδίας.

Τι πρέπει να κάνετε:

1	Εξετάστε όλες τις σχέσεις αξιοπιστίας ομοσπονδίας και βεβαιωθείτε ότι είναι έγκυρες.
2	Προσδιορίστε τον μηχανισμό απομίμησης λογαριασμού διαχείρισης.
3	Διανομή διαπιστευτηρίων λογαριασμού διαχείρισης.

03. Μοτίβο

Προσθήκη διαπιστευτηρίων σε υπάρχουσα εφαρμογή

Τι πρέπει να αναζητήσετε:

- Μη κανονική διαχειριστική περίοδος λειτουργίας που σχετίζεται με την τροποποίηση σχέσεων αξιοπιστίας ομοσπονδίας.
- Μη αναμενόμενες οντότητες υπηρεσίας που έχουν προστεθεί σε προνομιακούς ρόλους σε περιβάλλοντα cloud.

Τι πρέπει να κάνετε

1	Εξετάστε όλες τις εφαρμογές και τις οντότητες υπηρεσίας για τη δραστηριότητα τροποποίησης διαπιστευτηρίων.
2	Εξετάστε όλες τις εφαρμογές και τις οντότητες υπηρεσίας για πλεονάζοντα δικαιώματα.
3	Καταργήστε όλες τις ανενεργές οντότητες υπηρεσίας από το περιβάλλον σας.
4	Διανέμετε τακτικά διαπιστευτήρια για όλες τις εφαρμογές και τις οντότητες υπηρεσίας.

04. Μοτίβο

Ερωτήματα που μιμούνται υπάρχουσες εφαρμογές

Τι πρέπει να αναζητήσετε:

- Μη κανονικά αιτήματα προς τους πόρους σας από αξιόπιστες εφαρμογές ή οντότητες υπηρεσίας.
- Αιτήσεις από οντότητες υπηρεσίας που έχουν προσθέσει ή τροποποιήσει ομάδες, χρήστες, εφαρμογές, οντότητες υπηρεσίας ή σχέσεις αξιοπιστίας

Τι πρέπει να κάνετε:

1	Εξετάστε όλες τις σχέσεις αξιοπιστίας ομοσπονδίας και βεβαιωθείτε ότι είναι έγκυρες.
2	Προσδιορίστε τον μηχανισμό απομίμησης λογαριασμού διαχείρισης.
3	Διανομή διαπιστευτηρίων λογαριασμού διαχείρισης.

Σειρά βίντεο Solorigate

Επόμενα βήματα

01 Παρακολουθήστε τη σειρά βίντεο Solorigate σε αυτήν την τοποθεσία

02 Επισκεφθείτε την Ασφάλεια της Microsoft για περισσότερες ενημερώσεις: www.microsoft.com/en-us/security/business

03 Διαβάστε τις δημοσιεύσεις ιστολογίου στη διεύθυνση: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft