Corfu

Ψηφιακή Εγκληματολογία και Αναγνώριση Απειλών: Διαχείριση Κυβερνοεπιθέσεων

Dr. Stylianos Karagiannis (PhD)
Ionian University, Corfu, Greece

</> Stylianos Karagiannis

Corfu, Kozani, Greece Lisbon, Portugal

PhD in Cybersecurity - Post Doc @ Ionian University Department of Informatics, Corfu, Greece
Senior Researcher @ PDMFC, Lisbon, Portugal

Research Interests: Cybersecurity, Privacy, Capture The Flag (CTF) Challenges, Cyber Ranges
Gamification, Incident Handling, Virtual Labs, Game-Based Learning
Social Constructivism, Learning Theories

Email: skaragiannis@ionio.gr, LinkedIn, NMSLab

Διαχείριση Κυβερνοεπιθέσεων

- Το προηγούμενο μάθημα παρουσίασε το πλαίσιο αντιμετώπισης περιστατικών, περιγράφοντας τη **δομή και τη λειτουργία της CSIRT**, καθώς και τη συνεργασία της με άλλες επιχειρησιακές μονάδες. Επίσης, αναλύθηκε ο σχεδιασμός και η προετοιμασία που απαιτείται για την αντιμετώπιση κυβερνοεπιθέσεων.
- Ωστόσο, ακόμη και η καλύτερη προετοιμασία δεν μπορεί να καλύψει όλες τις μεταβλητές και αβεβαιότητες που εμφανίζονται σε πραγματικά περιστατικά. Όπως είπε ο πυγμάχος Mike Tyson: ***«Όλοι έχουν ένα σχέδιο μέχρι να φάνε ένα χαστούκι στο πρόσωπο».***
- Η ύπαρξη σταθερής βάσης και σαφούς κατανόησης της διαχείρισης κυβερνοεπιθέσεων επιτρέπει στους οργανισμούς:
  - να εφαρμόζουν τα σχέδιά τους αποτελεσματικά,
  - να επικοινωνούν έγκαιρα με βασικούς ενδιαφερόμενους, και
  - να μειώνουν τις πιθανές ζημιές ή τη διακοπή λειτουργίας λόγω ενός περιστατικού κυβερνοασφάλειας.

Συνεργασία με την ομάδα αντιμετώπισης περιστατικών

Σύγκριση με πυροσβεστική: Η CSIRT λειτουργεί όπως μια πυροσβεστική υπηρεσία. Η πυροσβεστική διαθέτει εξειδικευμένο προσωπικό και εξοπλισμό για τον περιορισμό και την εξάλειψη πυρκαγιών. Οι πολίτες παρέχουν βασικές πληροφορίες για το περιστατικό, όπως τοποθεσία και κίνδυνο για ανθρώπους.

Ενεργοποίηση της CSIRT: Η ενεργοποίηση μιας CSIRT είναι παρόμοια με αυτή της πυροσβεστικής. Το προσωπικό κλιμακώνει ενδείξεις περιστατικού στο κατάλληλο μέλος της ομάδας. Στη συνέχεια, οι πόροι στέλνονται στην κατάλληλη τοποθεσία για τον περιορισμό και την αντιμετώπιση του περιστατικού.

Κρίσιμα στοιχεία ενεργοποίησης

- **Μοντέλα CSIRT:** Παρέχουν πλαίσιο ενσωμάτωσης της CSIRT και των διαδικασιών κλιμάκωσης στη δομή του οργανισμού.
- **War Room:** Καθορίζει την τοποθεσία από την οποία η CSIRT διαχειρίζεται το περιστατικό.
- **Επικοινωνίες:** Διασφαλίζουν ότι η CSIRT μπορεί να επικοινωνεί αποτελεσματικά, εσωτερικά και εξωτερικά.
- **Περιστροφή προσωπικού:** Εξασφαλίζει ανάπαυση και ετοιμότητα κατά τη διάρκεια παρατεταμένων περιστατικών.

Καθορισμένη πορεία κλιμάκωσης: Όπως και στη λειτουργία της πυροσβεστικής, η ενεργοποίηση της CSIRT απαιτεί σαφή και προκαθορισμένη διαδικασία κλιμάκωσης. Στις επόμενες ενότητες παρουσιάζονται τρία μοντέλα CSIRT που περιγράφουν διαφορετικές επιλογές ορθής κλιμάκωσης.

Συνεργασία SOC-CSIRT

Η εμπλοκή πολλών ατόμων πριν την ανάληψη από την CSIRT μπορεί να δημιουργήσει καθυστερήσεις. Η σωστή τεκμηρίωση και η εκπαίδευση του προσωπικού SOC είναι κρίσιμες για τον εντοπισμό πραγματικών περιστατικών και τον περιορισμό ψευδών θετικών.

Εκπαίδευση και επικοινωνία: Το SOC χρειάζεται εκπαίδευση για την αναγνώριση περιστατικών και το CSIRT πρέπει να διαχειρίζεται πληροφορίες με σαφήνεια. Η επικοινωνία πρέπει να είναι πλήρης και σε πραγματικό χρόνο για την αποτελεσματική αντίδραση.

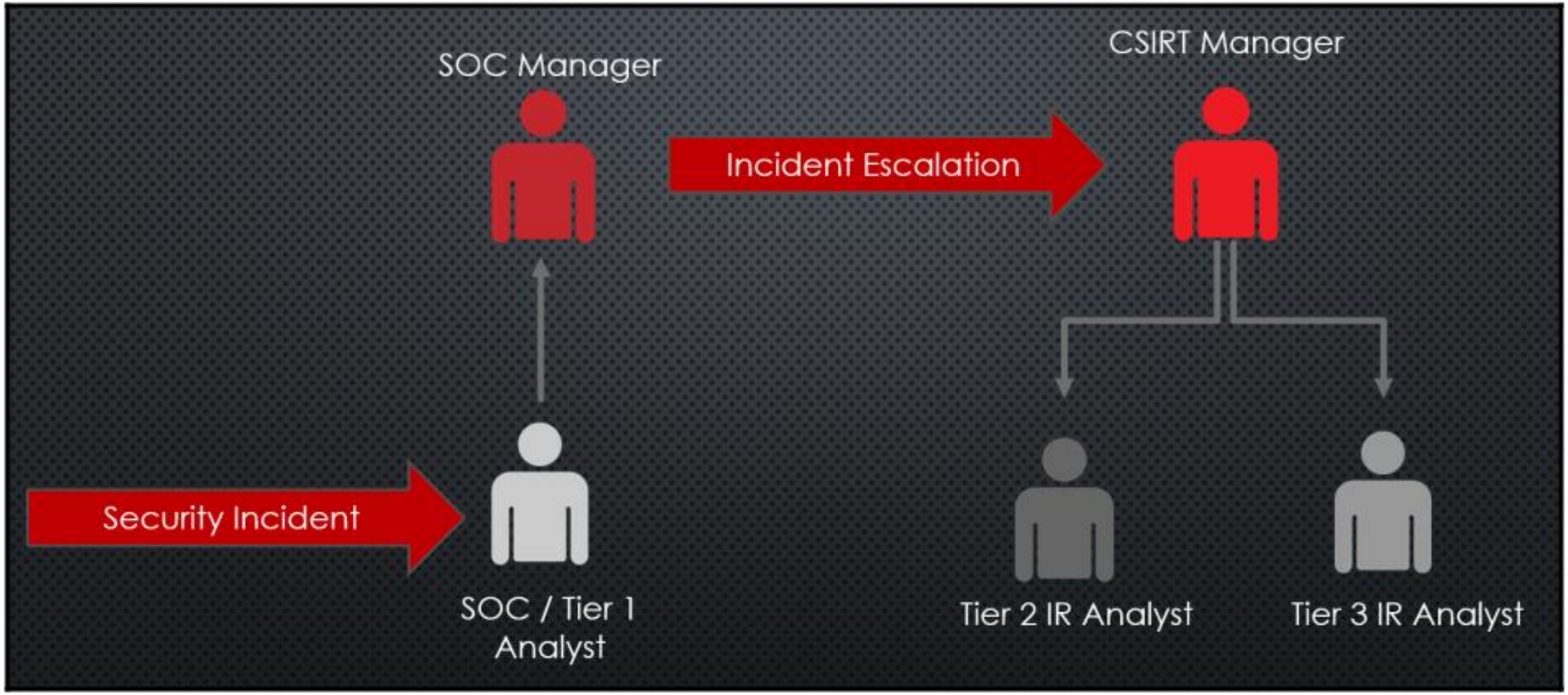
Παραλλαγές για οργανισμούς χωρίς SOC - Άμεση λήψη ειδοποιήσεων: Το αρχικό περιστατικό μπορεί να αναφερθεί από helpdesk ή NOC. Αυτό προσθέτει πολυπλοκότητα στην κλιμάκωση και απαιτεί εκπαίδευση για βασικό έλεγχο (triage) και σωστή προώθηση στο CSIRT.

Ρόλος του SOC: Το Κέντρο Λειτουργιών Ασφάλειας (SOC) είναι υπεύθυνο για την αρχική ανίχνευση και διερεύνηση περιστατικών. Παρακολουθεί την υποδομή, διαχειρίζεται εργαλεία ανίχνευσης εισβολών και antivirus και αξιολογεί ειδοποιήσεις για πιθανές απειλές.

Ροή κλιμάκωσης

- Λήψη ειδοποίησης από αναλυτή SOC ή Tier 1.
- Αξιολόγηση εάν η ειδοποίηση πληροί τα κριτήρια περιστατικού.
- Αρχική διερεύνηση από αναλυτή.
- Προώθηση στον υπεύθυνο SOC εάν απαιτείται.
- Κλιμάκωση στον υπεύθυνο CSIRT για πλήρη αντιμετώπιση.

Συνεργασία SOC-CSIRT



Συνεργασία SOC-CSIRT

Η εμπλοκή πολλών ατόμων πριν την ανάληψη από την CSIRT μπορεί να δημιουργήσει καθυστερήσεις. Η σωστή τεκμηρίωση και η εκπαίδευση του προσωπικού SOC είναι κρίσιμες για τον εντοπισμό πραγματικών περιστατικών και τον περιορισμό ψευδών θετικών.

Εκπαίδευση και επικοινωνία: Το SOC χρειάζεται εκπαίδευση για την αναγνώριση περιστατικών και το CSIRT πρέπει να διαχειρίζεται πληροφορίες με σαφήνεια. Η επικοινωνία πρέπει να είναι πλήρης και σε πραγματικό χρόνο για την αποτελεσματική αντίδραση.

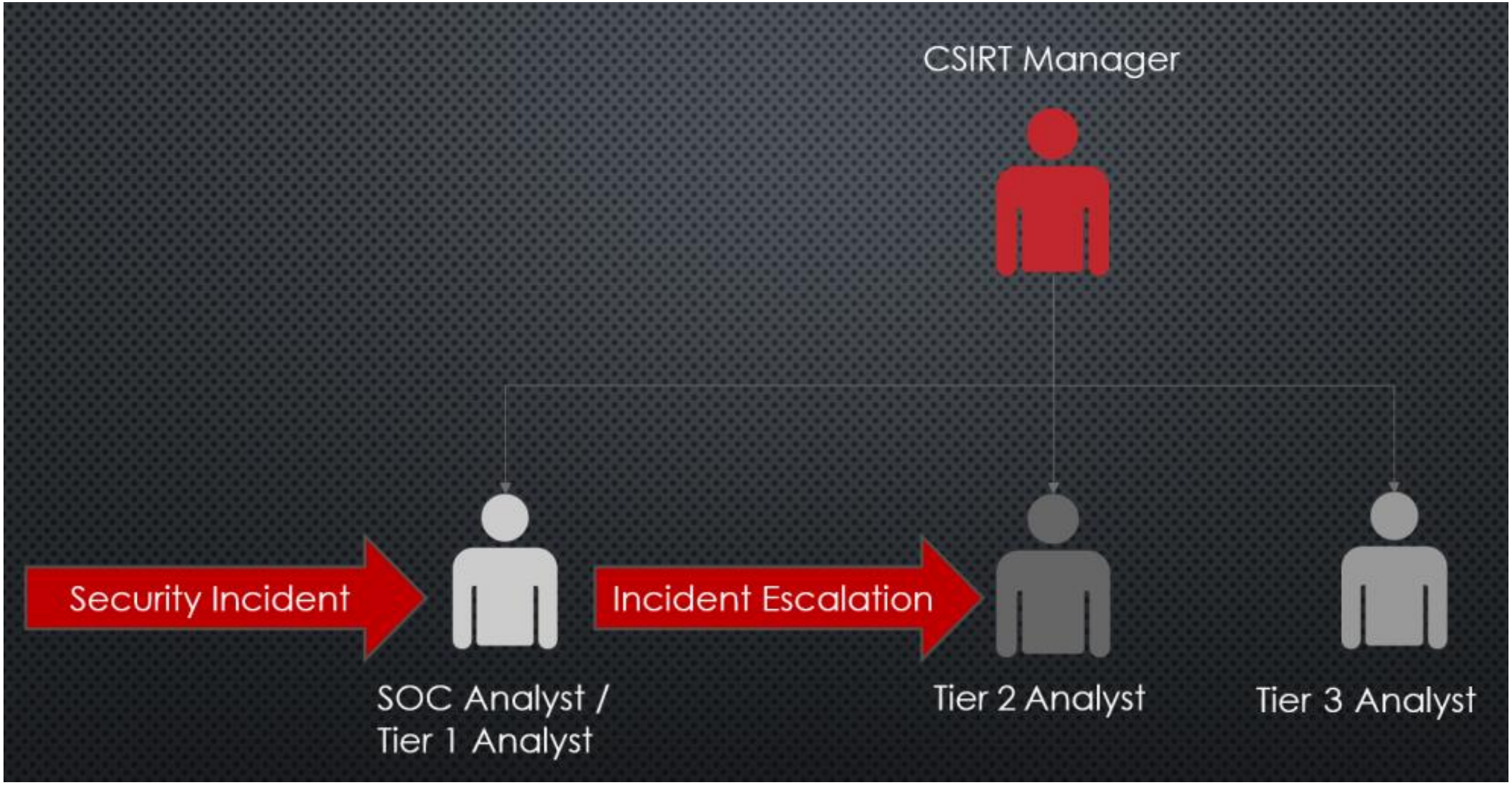
Παραλλαγές για οργανισμούς χωρίς SOC - Άμεση λήψη ειδοποιήσεων: Το αρχικό περιστατικό μπορεί να αναφερθεί από helpdesk ή NOC. Αυτό προσθέτει πολυπλοκότητα στην κλιμάκωση και απαιτεί εκπαίδευση για βασικό έλεγχο (triage) και σωστή προώθηση στο CSIRT.

Ρόλος του SOC: Το Κέντρο Λειτουργιών Ασφάλειας (SOC) είναι υπεύθυνο για την αρχική ανίχνευση και διερεύνηση περιστατικών. Παρακολουθεί την υποδομή, διαχειρίζεται εργαλεία ανίχνευσης εισβολών και antivirus και αξιολογεί ειδοποιήσεις για πιθανές απειλές.

Ροή κλιμάκωσης

- Λήψη ειδοποίησης από αναλυτή SOC ή Tier 1.
- Αξιολόγηση εάν η ειδοποίηση πληροί τα κριτήρια περιστατικού.
- Αρχική διερεύνηση από αναλυτή.
- Προώθηση στον υπεύθυνο SOC εάν απαιτείται.
- Κλιμάκωση στον υπεύθυνο CSIRT για πλήρη αντιμετώπιση.

Συνεργασία SOC-CSIRT



CSIRT Fusion Center

Συνδυασμός Αναλυτών: Οι αναλυτές CSIRT, SOC και threat intelligence συνεργάζονται σε μία ενιαία ομάδα. Η δομή αυτή ενσωματώνει τα πλεονεκτήματα του SOC-CSIRT μοντέλου και προσθέτει εξειδικευμένη γνώση threat intelligence. **Ρόλοι Αναλυτών Threat Intelligence:** Υποστηρίζουν τις διερευνήσεις περιστατικών χρησιμοποιώντας εσωτερικούς και εξωτερικούς πόρους. Εκτελούν λεπτομερή ανάλυση για άλλες περιοχές που σχετίζονται με το περιστατικό, ενισχύοντας την απόδοση της CSIRT. **Προκλήσεις και Περιορισμοί:** Η δομή δεν είναι ευρέως διαδεδομένη λόγω υψηλού κόστους και απαιτήσεων σε πόρους.Λίγοι οργανισμοί διαθέτουν επαρκές τεχνολογικό και ανθρώπινο δυναμικό για να υποστηρίξουν πλήρως ένα CSIRT Fusion Center.

Ορισμός War Room: Ένας ενιαίος χώρος λειτουργίας της CSIRT, γνωστός ως war room, επιτρέπει στην ομάδα να διαχειρίζεται τα περιστατικά με οργανωμένο τρόπο. Μπορεί να είναι προσωρινός ή μόνιμος, ανάλογα με τις ανάγκες του οργανισμού.

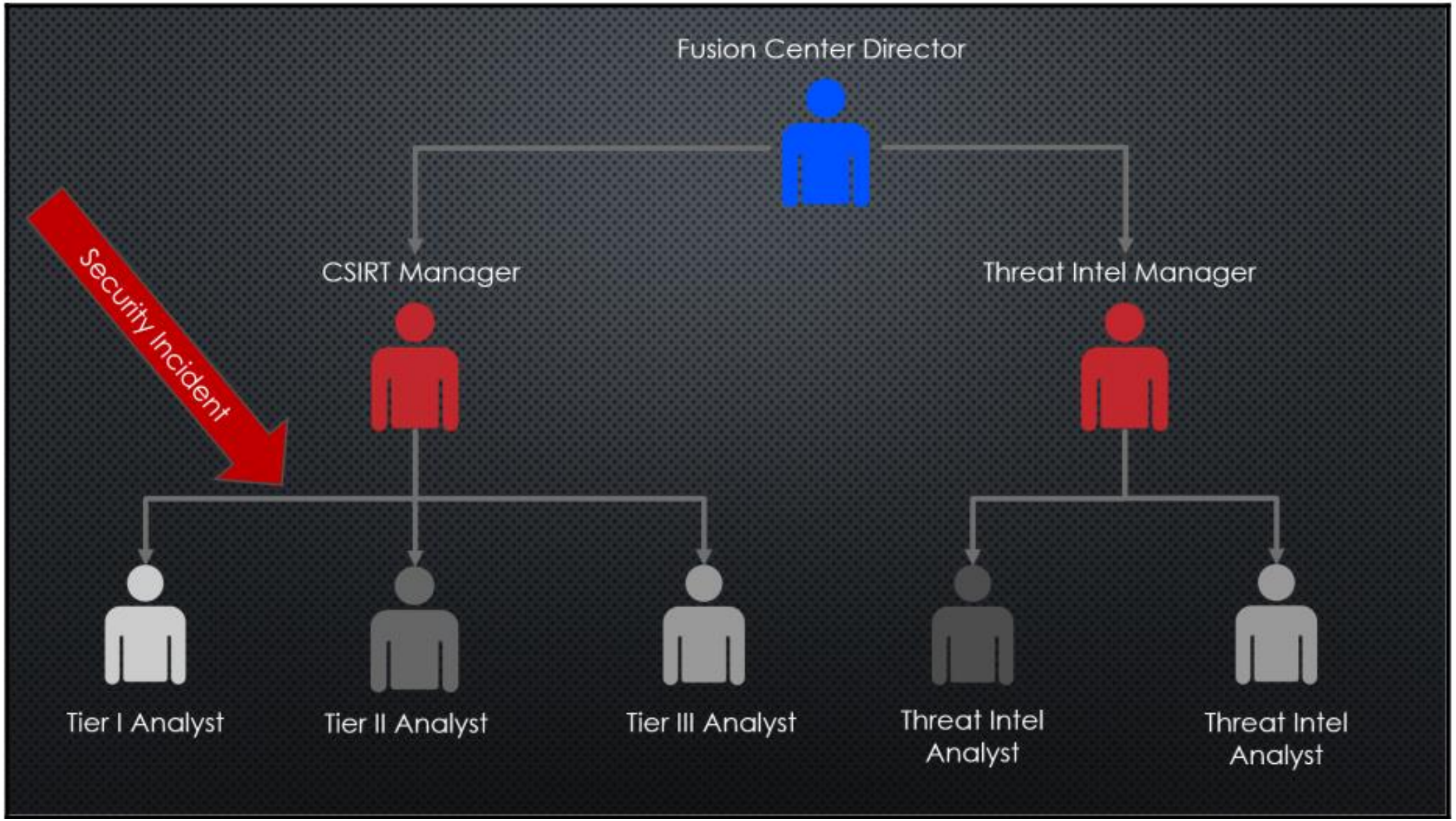
Προσωρινό: Χρήση υπάρχουσας αίθουσας συνεδριάσεων κατά τη διάρκεια περιστατικών.

Μόνιμο: Για οργανισμούς με μεγάλο αριθμό ή σύνθετα περιστατικά, παρέχει πλήρη εξοπλισμό και υποδομές για συνεχή χρήση.

Κύριες Δυνατότητες War Room

- Χώροι εργασίας: Προσωπικός χώρος για κάθε μέλος, με σύνδεση δικτύου, ρεύμα και οθόνες.
- Οθόνες ομάδας: Διευκολύνουν την ανταλλαγή δεδομένων και την οπτικοποίηση πληροφοριών.
- Κοινοποίηση σημειώσεων: Χρήση εργαλείων συνεργασίας για ομάδες σε διαφορετικές τοποθεσίες.
- Whiteboards: Ορατή παρουσίαση αναθέσεων εργασιών και λιστών παραβιασμένων συστημάτων.
- Περιορισμένη πρόσβαση: Εξασφαλίζει ότι μόνο εξουσιοδοτημένο προσωπικό εισέρχεται στη war room.

CSIRT Fusion Center



Επικοινωνία

Σημασία επικοινωνιών: Η σωστή εσωτερική επικοινωνία κατά τη διάρκεια ενός περιστατικού είναι κρίσιμη. Απλές πλατφόρμες όπως email ή άμεσα μηνύματα μπορεί να μην είναι ασφαλείς σε επιθέσεις που επηρεάζουν αυτά τα συστήματα.

Εναλλακτικά κανάλια: Εάν υπάρξει υποψία παραβίασης, πρέπει να υπάρχουν δευτερεύουσες ή τριτογενείς επιλογές επικοινωνίας. Τα ασφαλή κινητά ή προσωρινά εργαλεία συνεργασίας μπορούν να χρησιμοποιηθούν μέχρι να αποκατασταθεί η ασφάλεια των κύριων συστημάτων. **Παράδειγμα:** α) Σε παραβίαση cloud-based email (π.χ., Office 365), οι επιτιθέμενοι μπορεί να έχουν πρόσβαση και σε εφαρμογές άμεσων μηνυμάτων όπως το Skype. Η εξάρτηση από αυτά κατά τη διάρκεια του περιστατικού μπορεί να διαρρεύσει πληροφορίες CSIRT.

Εναλλαγή προσωπικού: Η παρατεταμένη εργασία επηρεάζει σωματικά και ψυχικά το προσωπικό. Ο Incident Commander (IC) πρέπει να θέτει σε βάρδιες τους απαντητές μετά από καθορισμένο χρόνο, ώστε να διατηρείται η λειτουργικότητα της ομάδας. **Παράδειγμα βαρδιών:** Περίπου 24 ώρες μετά την έναρξη μιας έρευνας, η ομάδα πρέπει να εναλλάσσεται, με 8 ώρες ανάπαυσης για κάθε μέλος, συμπεριλαμβανομένου του IC. Κατά τη διάρκεια παρατεταμένων περιστατικών, ορίζεται εναλλακτικός IC για διατήρηση της συνέχειας.

Υποστηρικτικό προσωπικό: Κατά τις περιόδους αδράνειας ενός περιστατικού, όταν η πιθανή κίνηση εντολών και ελέγχου (C2) έχει περιοριστεί, υποστηρικτικό προσωπικό μπορεί να παρακολουθεί το δίκτυο, επιτρέποντας στο βασικό CSIRT να αναπαυθεί.

Διερεύνηση Περιστατικών

Στόχος CSIRT: Η CSIRT αξιοποιεί συστημική ανάλυση για την αντιμετώπιση βασικών στοιχείων ενός περιστατικού, εξασφαλίζοντας ότι η αντίδραση είναι πλήρης και στοχευμένη.

- **Εύρος περιστατικού:** Το αρχικό εύρος μπορεί να μην είναι σαφές. Για παράδειγμα, η ανίχνευση ενός διακομιστή C2 οδηγεί σε αρχικό καθορισμό του ολόκληρου δικτύου, το οποίο στη συνέχεια περιορίζεται με ανάλυση firewall και web proxy. **Patient Zero:** Η αναγνώριση του πρώτου παραβιασμένου συστήματος (patient zero) παρέχει πολύτιμα δεδομένα, αλλά προτεραιότητα έχει ο προσδιορισμός του συνολικού εύρους των επηρεαζόμενων συστημάτων.
- **Καθορισμός του Αντίκτυπου:** Τριάδα CIA. Η εκτίμηση του αντίκτυπου βασίζεται στην Ακεραιότητα, Διαθεσιμότητα και Εμπιστευτικότητα. **Παραδείγματα:** ransomware επηρεάζει τη διαθεσιμότητα, κλοπή πνευματικής ιδιοκτησίας επηρεάζει την εμπιστευτικότητα, μη εξουσιοδοτημένη τροποποίηση δεδομένων επηρεάζει την ακεραιότητα. **Σημασία αντίκτυπου:** Ο προσδιορισμός του αντίκτυπου καθοδηγεί την κατανομή πόρων, επηρεάζει τη συμμόρφωση με κανονισμούς και καθορίζει τον τύπο απόκρισης που απαιτείται.
- **Καθορισμός της Ρίζας του Προβλήματος:** Η βασική ερώτηση: «Πώς συνέβη αυτό;». Στόχος είναι η αλληλουχία γεγονότων, ευπαθειών και συνθηκών που επέτρεψαν την παραβίαση να αναγνωριστεί και να διορθωθεί. **Σύνθετη αιτία:** Συχνά η ρίζα δεν είναι μία απλή ευπάθεια, αλλά συνδυασμός παραγόντων που πρέπει να εντοπιστούν για μελλοντική πρόληψη.
- **Ανάθεση Ευθυνών (Attribution):** Η ομάδα CSIRT μπορεί να προσπαθήσει να προσδιορίσει ποιος βρίσκεται πίσω από την επίθεση: κρατικός φορέας, εγκληματική ομάδα ή άλλος αντιπαλός. **Πρακτική σημασία:** Η ανάθεση είναι δευτερεύουσα σε σχέση με την έρευνα και την περιχαράκωση του περιστατικού. Αν απαιτείται, η τεκμηρίωση παραδίδεται σε ειδικούς οργανισμούς για επεξεργασία.

Ενσωμάτωση Στρατηγικών Περιορισμού

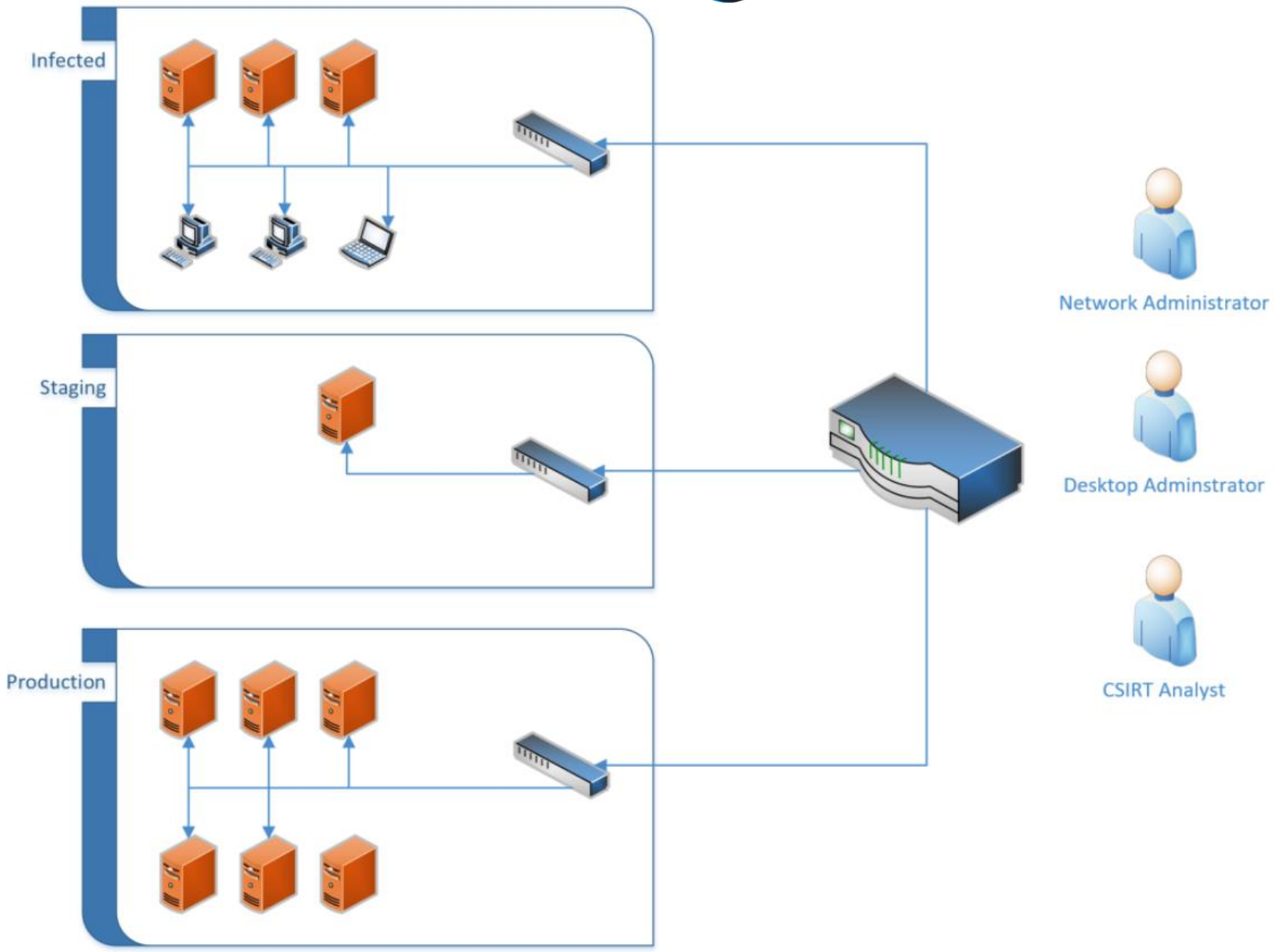
- **Σκοπός περιορισμού:** Οι στρατηγικές περιορισμού στοχεύουν στον περιορισμό της ζημιάς σε συγκεκριμένα συστήματα ή περιοχές δικτύου. Είναι κρίσιμες για την ταχεία αντιμετώπιση περιστατικών, όπως επιθέσεων ransomware που εξαπλώνονται γρήγορα.
- **Προκλήσεις περιορισμού. α) Flat τοπολογία δικτύου:** Πολλά επιχειρησιακά δίκτυα επιτρέπουν στα συστήματα να επικοινωνούν ελεύθερα μεταξύ τους. Αυτό διευκολύνει τη γρήγορη διάδοση malware μέσω πρωτοκόλλων όπως RDS ή SMB, όπως στην περίπτωση του WannaCry (CVE-2017-0144). **β) Επίγνωση τοπολογίας:** Η αποτελεσματική στρατηγική περιορισμού απαιτεί σαφή εικόνα του δικτύου μέσω διαγραμμάτων, εργαλείων ανακάλυψης και σαρώσεων ευπαθειών, ώστε η CSIRT να συντονίζει τα σχέδια με το προσωπικό IT.
- Διαχείριση αλλαγών κατά τον περιορισμό. **Εξουσιοδότηση αλλαγών:** Κατά τη διάρκεια περιστατικών, οι αλλαγές εφαρμόζονται άμεσα χωρίς να περιμένουν την τυπική έγκριση, με πλήρη τεκμηρίωση από CSIRT και προσωπικό IT για μελλοντική επανόρθωση.
- **Στρατηγικές περιορισμού: α) Φυσικός περιορισμός (Physical containment):** Αποσύνδεση συστήματος από το δίκτυο, όπως καλώδιο, ασύρματη πρόσβαση ή μέσω OS. Ιδανικός για μικρό αριθμό συστημάτων, αλλά δύσκολος σε μεγάλα ή γεωγραφικά διασκορπισμένα περιβάλλοντα. **β) Περιορισμός δικτύου (Network containment):** Αλλαγές σε switches ή κονσόλες διαχείρισης για απομόνωση μολυσμένων συστημάτων. Απαιτεί εμπειρογνωμοσύνη δικτύου και τεκμηρίωση αλλαγών για πιθανή αναστροφή. **γ) Περιορισμός περιμέτρου (Perimeter containment):** Χρήση firewall περιμέτρου για περιορισμό κυκλοφορίας. Μπορεί να συνδυαστεί με network containment, εφαρμόζοντας προσέγγιση «ρώσικης κούκλας» για σταδιακό περιορισμό. **δ) Εικονικός περιορισμός (Virtual containment):** Χρήση hypervisor ή virtual switch για αποσύνδεση εικονικών συστημάτων. Επιτρέπει ταυτόχρονο περιορισμό πολλαπλών servers και διατήρηση δεδομένων για μετέπειτα ανάλυση.

Στρατηγικές Εκρίζωσης

- **Προβλήματα με τον σύγχρονο κακόβουλο κώδικα:** Οι τεχνικές όπως η έγχυση διεργασιών (process injection) και η κατάληψη DLL (DLL hijacking) καθιστούν δύσκολη την πλήρη εκρίζωση malware. Ακόμη και αν αφαιρεθεί ο αρχικός κώδικας, τα συστήματα μπορεί να παραμένουν μολυσμένα.
- **Επαναφορά με γνωστή καλή εικόνα:** Οι περισσότερες στρατηγικές βασίζονται στη λήψη των μολυσμένων μηχανών και την επανεγκατάστασή τους με μια known good image ή την επαναφορά από γνωστό καλό backup.
- **Στρατηγική τριών VLAN για εκρίζωση**
  - Μολυσμένο VLAN: Όλες οι μολυσμένες μηχανές τοποθετούνται σε ένα ξεχωριστό VLAN για απομόνωση.
  - Staging VLAN: Μια μολυσμένη συσκευή μεταφέρεται σε δευτερεύον VLAN σταδίου. Το σύστημα επανεγκαθίσταται ή αποκαθίσταται από backup.
  - Production VLAN: Μετά την επανεγκατάσταση, το σύστημα μεταφέρεται στο παραγωγικό VLAN με επιπλέον παρακολούθηση για τυχόν υπολειπόμενη μόλυνση.

Εικονικά συστήματα: Χρήση στιγμιότυπων (snapshots). Αν τα μολυσμένα συστήματα είναι εικονικά και έχουν απομονωθεί, η επαναφορά στην τελευταία γνωστή καλή κατάσταση (last-known good snapshot) είναι η απλούστερη στρατηγική. **Προσοχή στη χρονική ακολουθία:** Το CSIRT πρέπει να έχει εμπιστοσύνη στη σειρά των γεγονότων. Ένα στιγμιότυπο που τραβήχτηκε μετά την παραβίαση μπορεί να περιέχει ακόμα malware.ΣχόλιοΠαρά τη χρονοβόρα φύση της στρατηγικής με VLAN ή snapshots, αποτελεί ασφαλή τρόπο να διασφαλιστεί ότι όλα τα επηρεασμένα συστήματα εκκαθαρίζονται πλήρως.

Στρατηγικές Εκρίζωσης



Στρατηγικές Ανάκαμψης

1. **Ενημερώσεις ασφαλείας (Patching):** Όλα τα συστήματα πρέπει να έχουν εγκαταστήσει τις πιο πρόσφατες ενημερώσεις ασφαλείας. Σε περιπτώσεις ευπάθειας zero-day ή νέας ευπάθειας χωρίς διαθέσιμο patch, το CSIRT προτείνει επιπλέον μέτρα ασφαλείας για περιορισμό υπολειπόμενου κινδύνου.
2. **Ενίσχυση ελέγχων ανίχνευσης και πρόληψης:** Το CSIRT συνεργάζεται με το προσωπικό IT και ασφάλειας για τη δημιουργία ή τροποποίηση κανόνων ανίχνευσης και πρόληψης. Οι κανόνες αυτοί βασίζονται στα στοιχεία του περιστατικού και στις εντοπισμένες ευπάθειες.
3. **Ανασκόπηση αλλαγών υποδομής:** Οι αλλαγές που έγιναν κατά τη διάρκεια του περιστατικού εξετάζονται για να διαπιστωθεί αν παραμένουν απαραίτητες. Οι μακροπρόθεσμες αλλαγές αξιολογούνται από τη διαδικασία ελέγχου αλλαγών και εγκρίνονται σύμφωνα με αυτήν.
4. **Σάρωση ευπαθειών:** Πριν το κλείσιμο του περιστατικού, διεξάγεται πλήρης σάρωση ευπαθειών σε όλα τα συστήματα. Αυτό διασφαλίζει ότι όλα τα επηρεασμένα συστήματα αντιμετωπίστηκαν και ότι άλλα συστήματα έχουν εγκαταστήσει τα απαραίτητα patches.
5. **Ανασκόπηση μετά την ενέργεια (After-Action Review):** Μετά την ολοκλήρωση, το CSIRT πραγματοποιεί ανασκόπηση όλου του περιστατικού. Εξετάζονται οι ενέργειες, τα playbooks, τα εργαλεία και οι διαδικασίες. Οι ελλείψεις εντοπίζονται και διορθώνονται, ενώ τα αποτελέσματα τεκμηριώνονται στο φάκελο του περιστατικού.

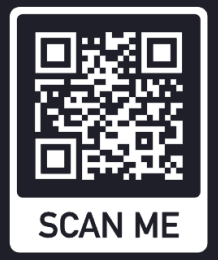
Στρατηγικές Ανάκαμψης

1. **Ενημερώσεις ασφαλείας (Patching):** Όλα τα συστήματα πρέπει να έχουν εγκαταστήσει τις πιο πρόσφατες ενημερώσεις ασφαλείας. Σε περιπτώσεις ευπάθειας zero-day ή νέας ευπάθειας χωρίς διαθέσιμο patch, το CSIRT προτείνει επιπλέον μέτρα ασφαλείας για περιορισμό υπολειπόμενου κινδύνου.
2. **Ενίσχυση ελέγχων ανίχνευσης και πρόληψης:** Το CSIRT συνεργάζεται με το προσωπικό IT και ασφάλειας για τη δημιουργία ή τροποποίηση κανόνων ανίχνευσης και πρόληψης. Οι κανόνες αυτοί βασίζονται στα στοιχεία του περιστατικού και στις εντοπισμένες ευπάθειες.
3. **Ανασκόπηση αλλαγών υποδομής:** Οι αλλαγές που έγιναν κατά τη διάρκεια του περιστατικού εξετάζονται για να διαπιστωθεί αν παραμένουν απαραίτητες. Οι μακροπρόθεσμες αλλαγές αξιολογούνται από τη διαδικασία ελέγχου αλλαγών και εγκρίνονται σύμφωνα με αυτήν.
4. **Σάρωση ευπαθειών:** Πριν το κλείσιμο του περιστατικού, διεξάγεται πλήρης σάρωση ευπαθειών σε όλα τα συστήματα. Αυτό διασφαλίζει ότι όλα τα επηρεασμένα συστήματα αντιμετωπίστηκαν και ότι άλλα συστήματα έχουν εγκαταστήσει τα απαραίτητα patches.
5. **Ανασκόπηση μετά την ενέργεια (After-Action Review):** Μετά την ολοκλήρωση, το CSIRT πραγματοποιεί ανασκόπηση όλου του περιστατικού. Εξετάζονται οι ενέργειες, τα playbooks, τα εργαλεία και οι διαδικασίες. Οι ελλείψεις εντοπίζονται και διορθώνονται, ενώ τα αποτελέσματα τεκμηριώνονται στο φάκελο του περιστατικού.

NMSLab

Ευχαριστώ για την Προσοχή σας!

Dr. Stylianos Karagiannis, PhD



https://nmslab.di.ionio.gr