TANIUM

Erfolgreich in der Cybersecurity

Ein strategischer Ansatz

Zac Warren

2023

Technologische Trends

Digitale Transformation

Die digitale Technologie, z.B. KI, verändert die Art und Weise, wie Unternehmen arbeiten und Werte liefern.

Hybride Arbeit

Arbeit ist kein Ort mehr und schafft einen sich ständig verändernden Umfang.

Cloud Migration

Infrastruktur, Anwendungen und Daten werden in die Multicloud verlagert

TANIUM

IT- und Sicherheitsprioritäten

Modernisieren und Updates

Legacy-Plattformen und Umgebungen

Compliance

Einhaltung von Compliance- und regulatorischen Anforderungen

Risiko

Verwalten Sie den wachsenden IT-Bestand und mindern Sie das Risiko

TANIUM

11 sec

Alle 11 Sekunden erfolgt ein Ransomware-Angriff

$180 B

Wird die Cybersicherheit immer schlechter?

94%

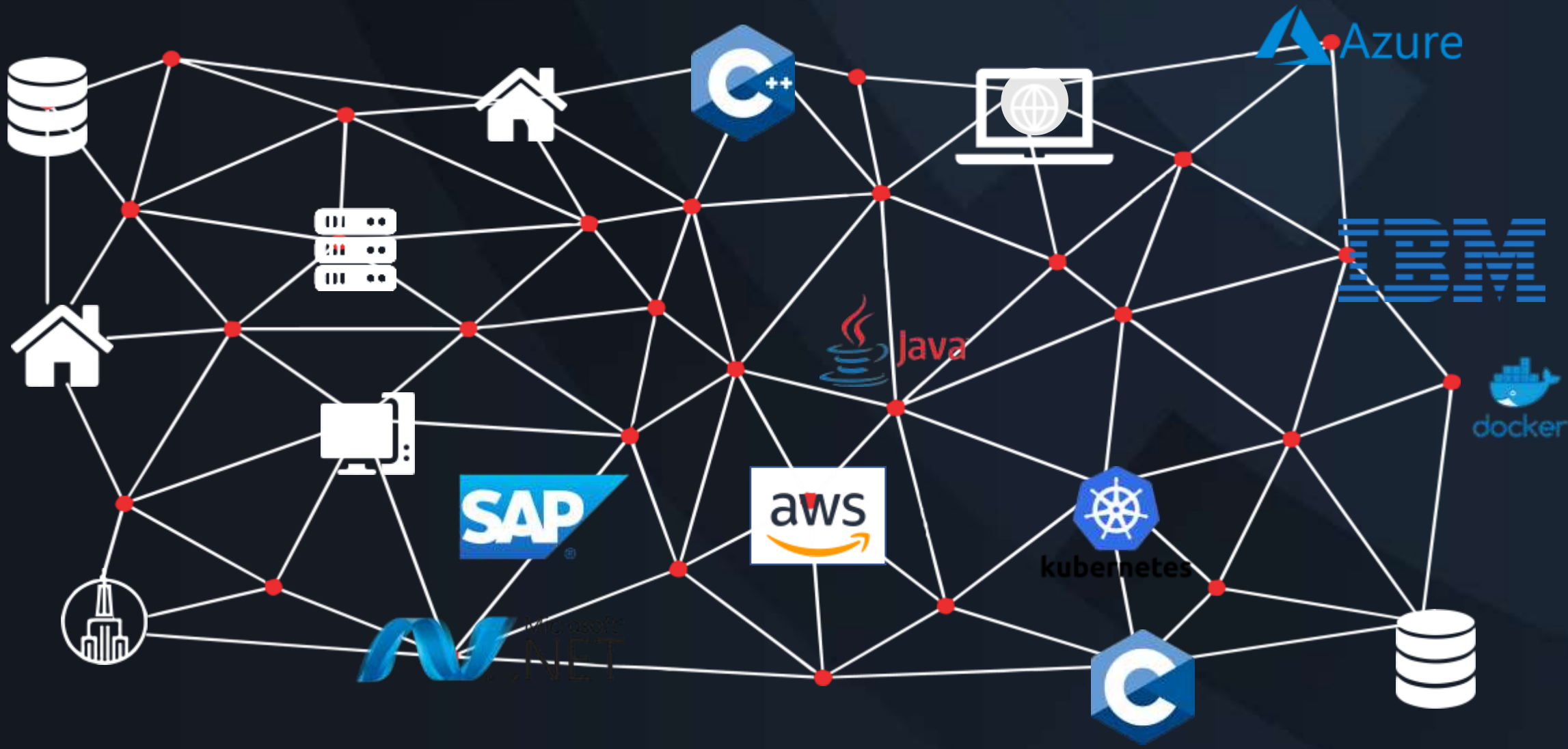
der Unternehmen fehlen bis zu 20 % der Endpunkte

Best-of-Breed-Punktlösungen

Sie können nicht schützen, was Sie nicht sehen können.

TANIUM

Fülle von Daten … Mangel an Transparenz



Den Angreifern ist es egal, wo oder wie diese eindringen

Vorbereitung und Gegenmaßnahmen

TANIUM

Sichtbarkeit & Kontrolle

Kontinuierliche Sicherung

Erkennung & Gegenmaßnahmen

TANIUM

Sichtbarkeit & Kontrolle

Kontinuierliche Sicherung

Erkennung & Gegenmaßnahmen

TANIUM

Sichtbarkeit & Kontrolle

Asset-Erkennung	Nur was man kennt, kann man schützen
Kontrolle	Sie benötigen Kontrolle, um Aktionen auszuführen
Identifizieren Sie ihre „Kronjuwelen“	Das Budget ist begrenzt, konzentrieren Sie sich auf wichtige Assets

TANIUM

Wo soll man anfangen?

Richten Sie umfassende Sichtbarkeitsprogramme ein

Asset-Lifecycle-Programme

- Genauigkeit und Verfügbarkeit
- CMDB verbessern

Authentifizierungs- und Autorisierungsprogramme

- Multi-Faktor-Authentifizierung

Schwachstellenanalyse und –management

- Vulnerability Scanner / Config Scanner
- Patching und Policies

Es gibt kein „Set and Forget“
um GESCHÜTZT zu BLEIBEN!

TANIUM

Wichtige Fragen, die jeder IT-Leiter stellen und beantworten muss!

Wie viele Assets haben wir und welchen Umfang? unser Netzwerk?

Was läuft auf allen Geräten in unserem Netzwerk?

Was geht in und aus unserem Netzwerk?

Wie sehen wir für einen Angreifer aus?

TANIUM

Sichtbarkeit & Kontrolle

Kontinuierliche Sicherung

Erkennung & Gegenmaßnahmen

TANIUM

Kontinuierliche Absicherung

Administratoren	Kennen und beschränken Sie Ihre leistungsstarken Benutzer
Patchen	Schließen Sie Sicherheitslücken
Schwachstelle & Compliance	Erhöhen Sie die Kosten und den Aufwand von Angreifern

TANIUM

Wo soll man anfangen?

Richten Sie umfassende kontinuierliche Sicherheitsprogramme ein

Grundlegende Programme

- Operations Prozesse: ITIL / ITSM
- Security Prozesse : Vuln/Config **Management**
- Aktive Jagd nach Bedrohungen

Automatisierungs- und Skalierbarkeitsprogramme

- Patch-Verwaltung

Es gibt kein „Set and Forget“
um GESCHÜTZT zu BLEIBEN!

TANIUM

Wichtige Fragen, die jeder IT-Leiter stellen und beantworten muss!

Sind unsere Sicherheitskontrollen vorhanden und wirksam?

Woher stammen unsere Daten und wo werden sie gespeichert?

Sind unsere Teams gut ausgebildet und sprechen sie eine gemeinsame Sprache?

Gibt es Möglichkeiten, Prozesse zu skalieren und zu automatisieren? …um es einfacher zu machen? …bereit zu bleiben?

TANIUM

Sichtbarkeit & Kontrolle

Kontinuierliche Sicherung

Erkennung & Gegenmaßnahmen

TANIUM

Erkennung & Gegenmaßnahmen

Erkennen

Identifizieren Sie kompromittierte Endpunkte und stoppen Sie verdächtiges Verhalten

Antworten

Ergreifen Sie eine Vielzahl von Abhilfemaßnahmen, z. B. das Auferlegen von Netzwerkquarantänen, das Bereitstellen von Patches oder das Ausführen benutzerdefinierter Skripts

TANIUM

Wo soll man anfangen?

Richten Sie umfassende Erkennungs- und Gegenmaßnahmenprogramme ein

Incident Response Plan

- Bereiten Sie sich darauf vor, schnell und effektiv auf eine Sicherheitsverletzung zu reagieren
- Skizzieren Sie Rollen, Verantwortlichkeiten und Verfahren für die Reaktion auf Sicherheitsvorfälle

Regelmäßige Penetrationstests

- Identifizieren und beheben Sie Sicherheitslücken, bevor sie ausgenutzt werden können

Es gibt kein „Set and Forget“
um GESCHÜTZT zu BLEIBEN!

TANIUM

Wichtige Fragen, die jeder IT-Leiter stellen und beantworten muss!

Welche Prozesse haben wir zur Überwachung und Erkennung potenzieller Sicherheitsvorfälle eingerichtet?

Wie reagieren wir auf eine Sicherheitsverletzung oder eine potenzielle Bedrohung?

Wie stellen wir sicher, dass unsere Systeme und Anwendungen mit den neuesten Sicherheitspatches und -funktionen aktualisiert werden?

Kann unser Team unseren Plan zur Reaktion auf Vorfälle ausführen?

TANIUM

Sichtbarkeit & Kontrolle

Kontinuierliche Sicherung

Erkennung & Gegenmaßnahmen

TANIUM

Was bedeutet es wirklich, diese Themen und Programme zu beherrschen?

Großes Risiko

Sicher

(kleines Risiko)

TANIUM

© 2023 Tanium. All rights reserved.

Vielen Dank.

TANIUM