Automatisierung, KI und Shared Ressource Konzepte im Security Operation Center

Ralf Kulke, Cyber Security Executive

09. Oktober 2019

verizon

Proprietary statement.

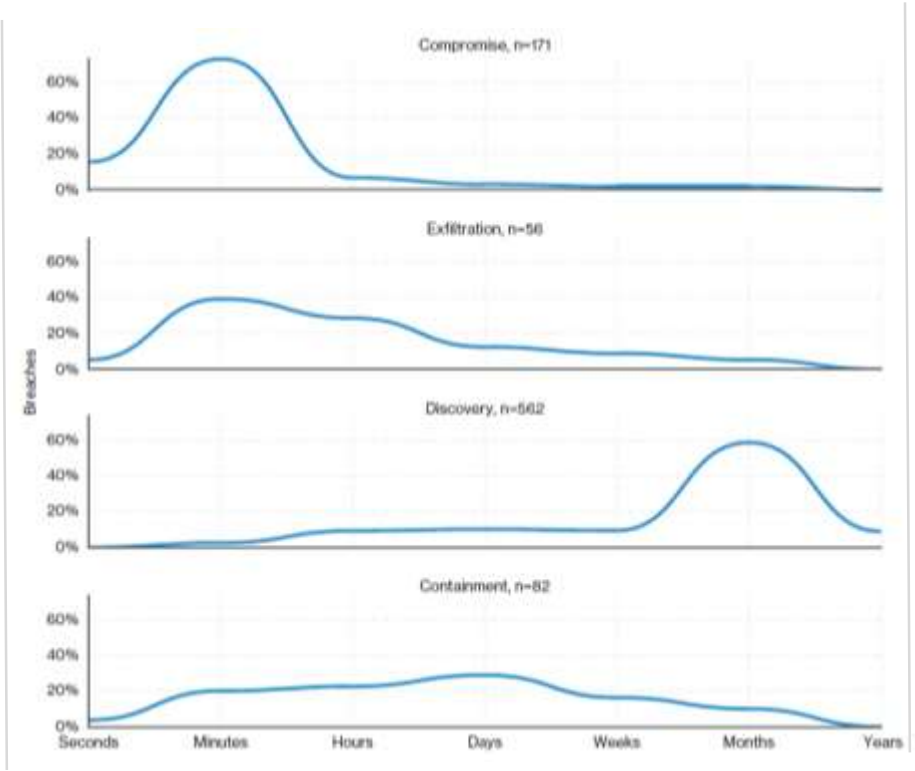
This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

Wachsende Kluft zwischen Angriff und Entdeckung.

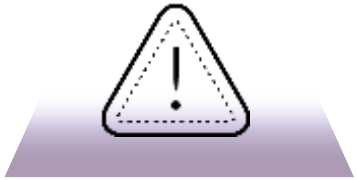
Der Zeitraum in der Ereigniskette vom initialen Breach bis zum Datenzugriff auf Daten wird in Sekunden und Minuten gemessen; der Zeitraum bis zur Entdeckung in Monaten.*

Folge: Unnötiges Risiko & Kosten



** 2019 Verizon Data Breach investigations Report (DBIR)*

Viele Ursachen*

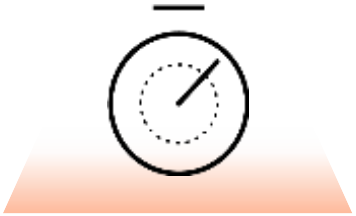


Gaps in Prevention

Bestandssysteme verursachen zu viele Meldungen

174k

Meldungen pro Woche



Zeitmangel

Manuelle Prozesse über gekapselte Systeme hinweg dauern zu lange

30+

Einzelprodukte

Limitierter Kontext

Gefahrenanalyse dauert Tage

4+ Tage

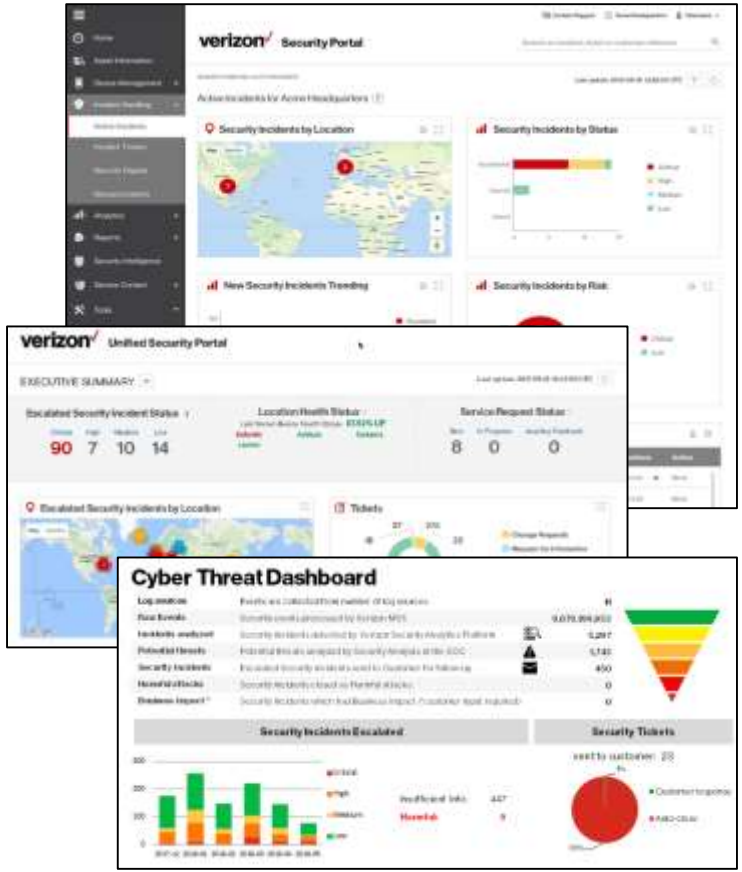
Um eine Ermittlung abzuschließen

** Quelle: 2019 Palo Alto*

verizon

Ziele für ein SOC.

- **Umfangreiche Datenverfügbarkeit** und Fokussierung
- **Effiziente Datenanalyse** hinsichtlich Zeit und Kosten
    - Schnelle Entdeckung und Neutralisierung von Bedrohungen – Zeit ist wesentlich
    - Effizienter Einsatz bestehender Systeme und Mitarbeiter / Kostenreduktion
- **Zeitnahe und Effektive Response**
- **Verfügbarkeit und Flexibilität von Ressourcen**



Beispiel Verizon - Organization, Automatisierung & Transparenz.

Umsetzung eines SOAR Ansatzes mit Hilfe einer Lösungssuite von Palo Alto (Demisto)®

- Orchestrierung der Prozesse: Gestaltung und sinnvoller Playbooks/Workflows und Systemübergreifende Implementierung
- Automatisierung und Umsetzung in der Systemlandschaft mittels Scripts, weiterführender Produktintegration und Umsetzung der Playbook-Tasks
    - Automatisierte Response Prozesse
    - Automatisierte Network Security Policy Changes
- Zusammenführen aller angriffsrelevanter Daten in einem Single Pane of Glass / Dash Board
    - Threat Intelligence, Case Management
    - Anayse & Reporting, Response, Zusammenarbeit

Banale, wiederkehrende und/oder „harmlose“ Bedrohungen müssen durchgehend automatisiert verarbeitet werden!

verizon

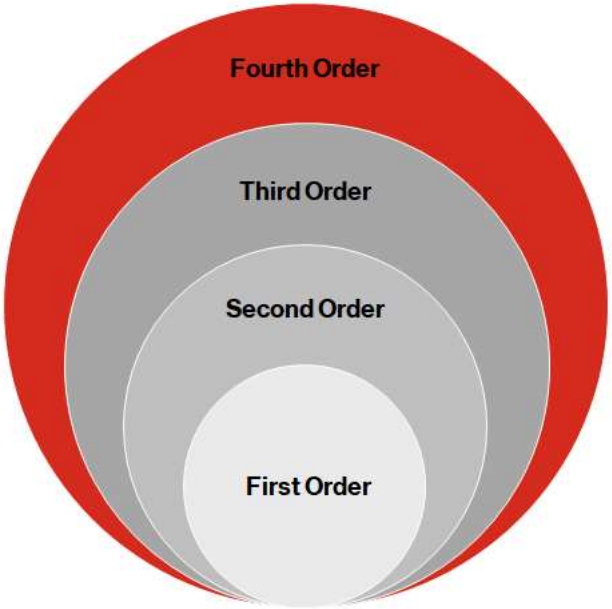
Beispiel Verizon - Künstliche Intelligenz / Analytics.

Verizon nutzt in seinem globalen IP-Backbone und Netzwerken schon lange KI-basierte Modelle zur Gefahrenabwehr.

Der Einsatz von KI-basierten Tools:

- Erkennung von Bedrohungen in großen Datenmengen
- Silo-übergreifende Zusammenhänge werden erkannt
- Zeitlich nicht in Zusammenhang stehende Muster werden erkannt
- Hohe Genauigkeit und Verlässlichkeit

Generelle Steigerung der Analysequalität bei „vernünftiger“ Anwendung.



The Threat Hunting Maturity Model

Shared-Ressource-Konzepte.

Sinnvoller Einsatz interner und externer Ressourcen: Make and Buy

Shared-Ressource-Konzept	
Verizon MSS-Analytics, Managed SIEM, Advanced SOC	
Global intelligence	Local intelligence
Standard best of breed	Tailored
Scalable, feasible pricing point	Dedicated
Knowledge and people sharing	Integrated

Ergbnisse.

Umsetzung der Aktivitäten resultiert in

- Schnellere Gefahrenerkennung
- Kostensenkung durch Effizienzsteigerung
    - Weniger Analyseaufwand durch Informationsintegration & Automatisierung
    - Ressourcenfreistellung für bessere und schnellere Analyse von schwerwiegenden Incidents
    - Verbesserte Kundenzufriedenheit (SLAs)
    - Senkung des Datendurchsatzes durch sinnvolles Filtern
- Höhere Mitarbeiterzufriedenheit dank Wegfall minderwertiger Tätigkeiten
- Besseres Reporting zur nachhaltigen Serviceoptimierung