# Cybersecurity

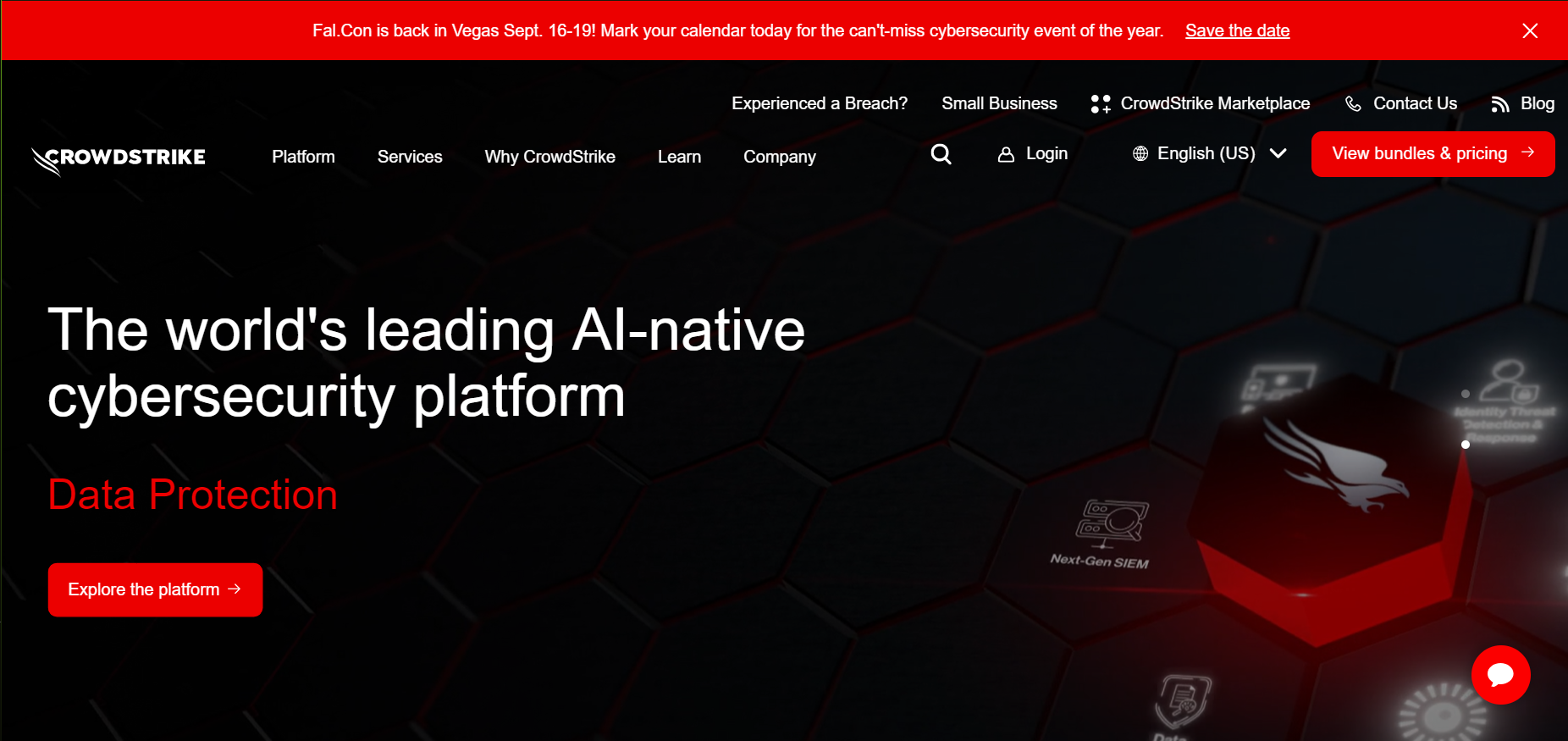
**Thema:**

In het kader van mijn studie, waarbij de focus ligt op cybersecurity, heb ik besloten om een website te bouwen die informatief en educatief is op het gebied van cyberbeveiliging. Deze website zal dienen als een bron van kennis en middelen voor zowel beginners als gevorderden die geïnteresseerd zijn in het beschermen van hun digitale wereld tegen cyberdreigingen.

## Opdracht inspiratie

1. Website CrowdStrike:

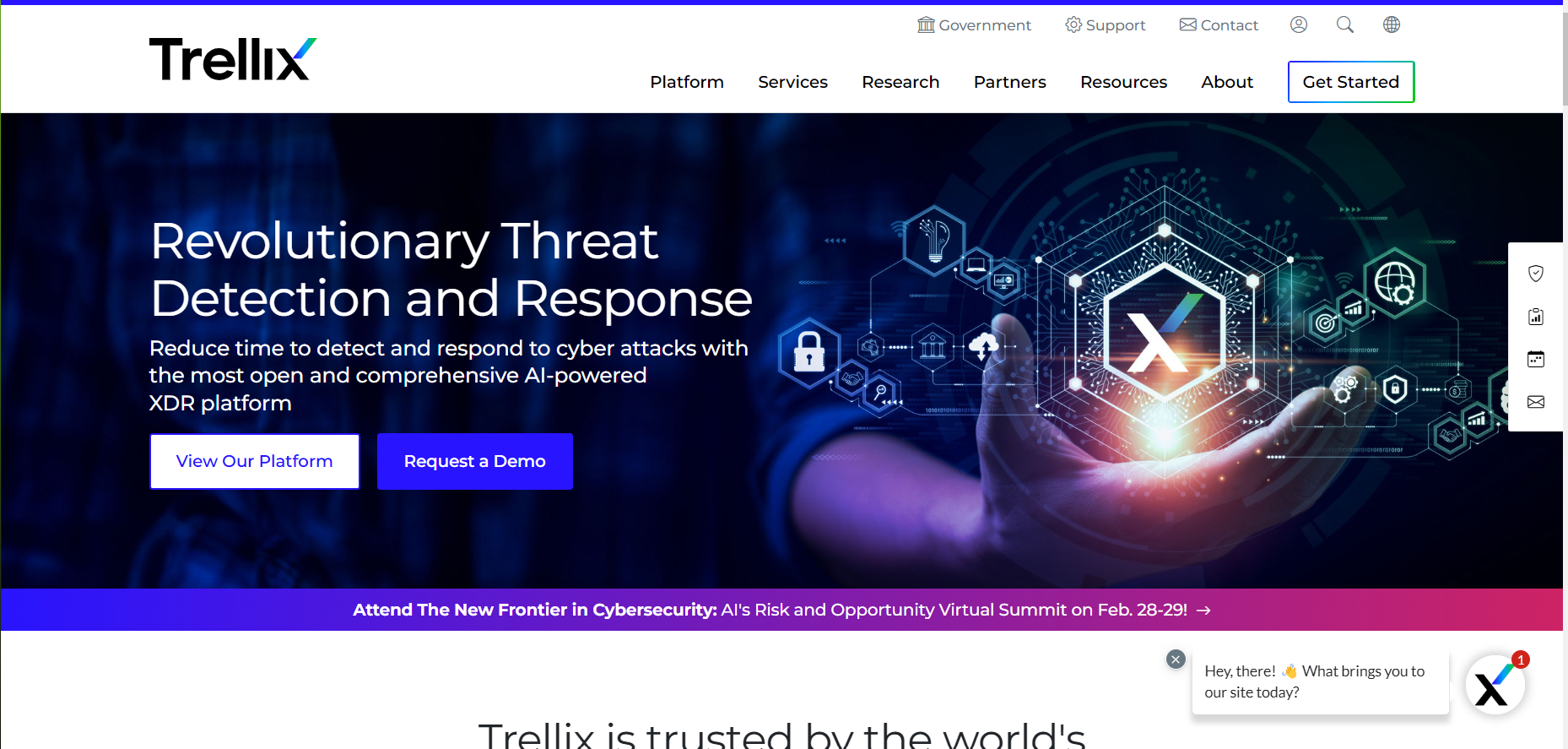
<https://www.crowdstrike.com/en-us/>



Ik vind deze site aantrekkelijk omdat het qua kleuren best wel goed in elkaar zit. Ook het feit dat ze werken met AI om hun diensten aan te bieden, wat het nog interessanter maakt volgens mijn perspectief.

1. Website Trellix:

<https://www.trellix.com>



De foto’s spreken me aan, en ook de manier hoe ze hun diensten over brengen.

1. Website Sogeti:

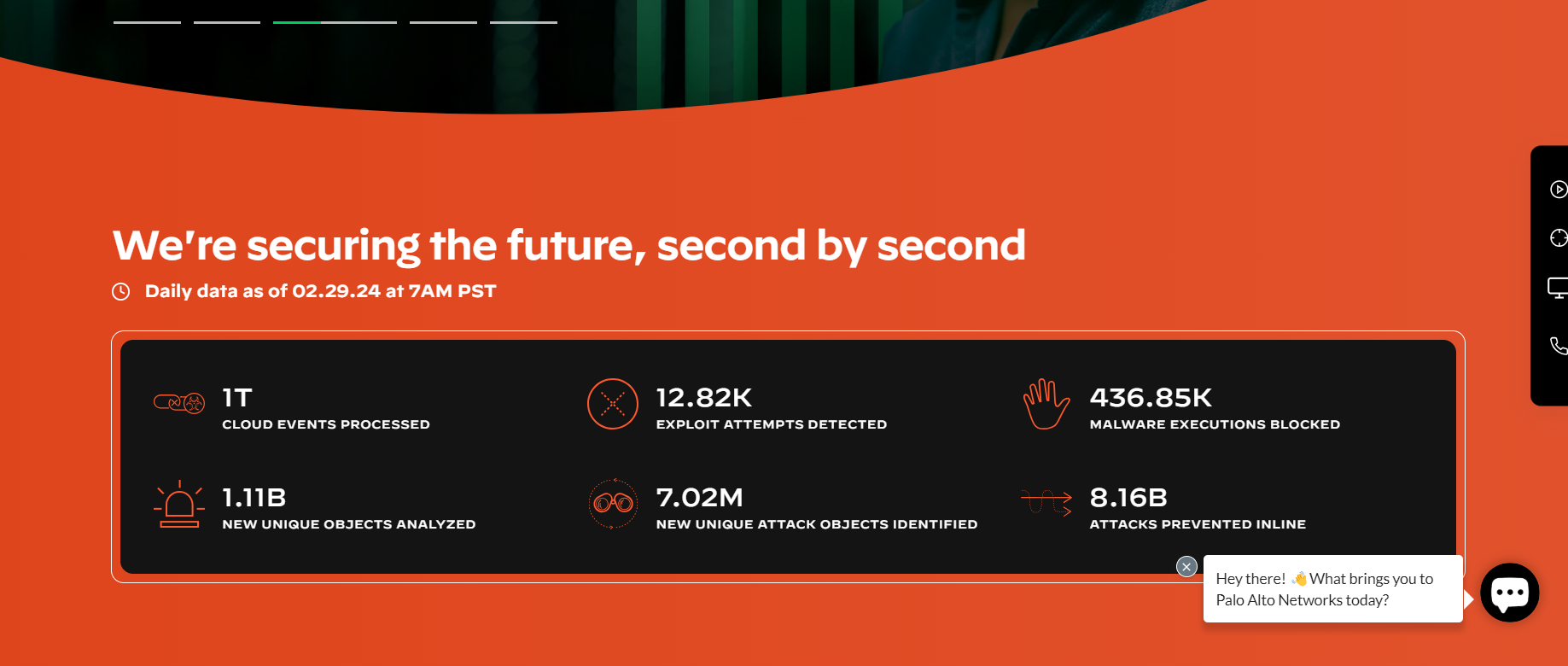
<https://www.sogeti.nl/services/cyber-security>



Eens een Nederlandse cybersecurity bedrijf zien kan ook geen kwaad, ik vind het vooral aantrekkelijk omdat het handiger is om mee te communiceren.

1. Website PaloAltoNetworks:

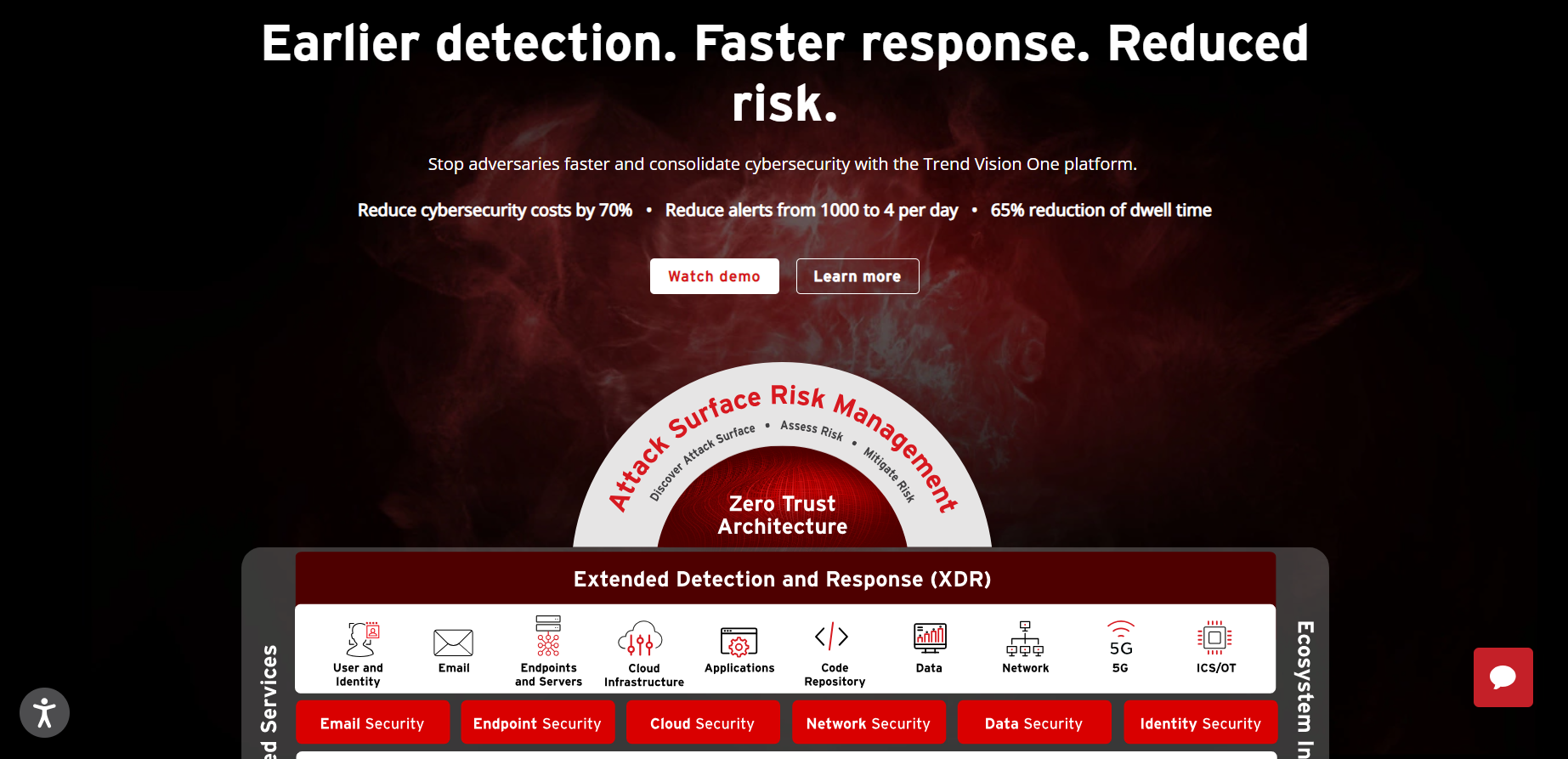
<https://www.paloaltonetworks.com>



Het is vooral aantrekkelijk door de kleuren en hun prestaties, ze hebben heel wat professionele mensen in dienst wat zeker belangrijk is.

1. Website Trendmicro:

<https://www.trendmicro.com/en_be/business.html>



Hun slogan, kleuren wat het mysterieus maakt, en hun diensten opgesomd is erg aantrekkelijk.

## Kleurenpalet

Donkerblauw (Logo): #001f3f

Zilvergrijs (Titels): #bdc3c7

Rood (Accenten): #e74c3c

Afbeelding met schermopname, tekst, Kleurrijkheid, ontwerp

Automatisch gegenereerde beschrijvingDit kleurenpalet combineert donkere en krachtige tinten die vaak worden geassocieerd met beveiliging en cybersecurity.

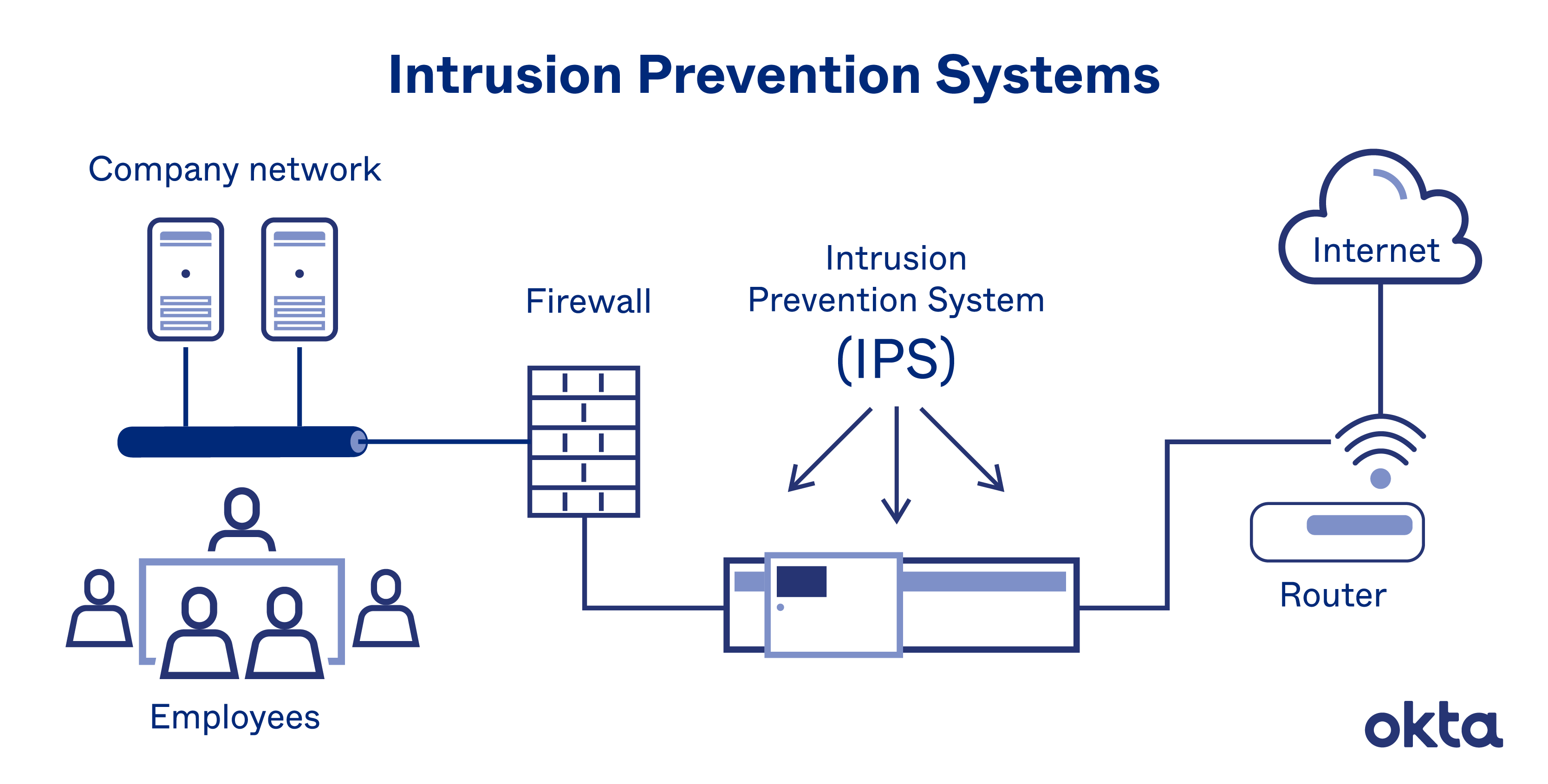
## Beeldmateriaal:

**Vulnerability Assessment en Penetratietesten:**

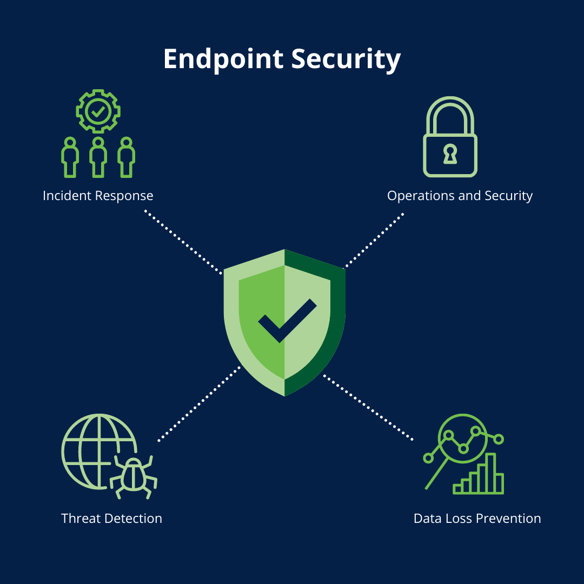


Identificeren van zwakke plekken en kwetsbaarheden in systemen, netwerken of applicaties. Penetratietesten gaan een stap verder door daadwerkelijk aanvallen te simuleren om de reactie van het systeem te evalueren.

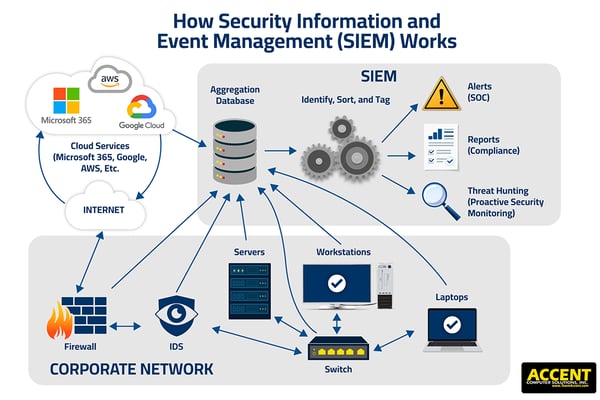
**Firewall- en Intrusion Prevention Services:**



Implementeren en onderhouden van firewalls om ongeautoriseerde toegang tot netwerken te voorkomen. Intrusion Prevention Systems (IPS) detecteren en blokkeren kwaadwillige activiteiten.

**Endpoint Security:**

Beschermen van individuele apparaten zoals computers, laptops en mobiele apparaten tegen malware, ransomware en andere bedreigingen. Dit omvat antivirussoftware, geavanceerde bedreigingsbescherming en device management.

**Security Information and Event Management (SIEM):**

Monitoren, analyseren en reageren op beveiligingsgebeurtenissen in real-time. SIEM-systemen verzamelen en correlateren loggegevens van verschillende bronnen om potentiële beveiligingsincidenten te identificeren.

**Identity and Access Management (IAM):**

Beheren en beveiligen van digitale identiteiten en toegangsrechten binnen een organisatie. IAM-systemen zorgen ervoor dat alleen geautoriseerde gebruikers toegang hebben tot specifieke middelen.

**Encryptie en Data Protection Services:**



Beschermen van gevoelige gegevens door middel van versleuteling, zowel tijdens de overdracht als opgeslagen op systemen. Dit voorkomt ongeautoriseerde toegang tot vertrouwelijke informatie.