VEROSINT

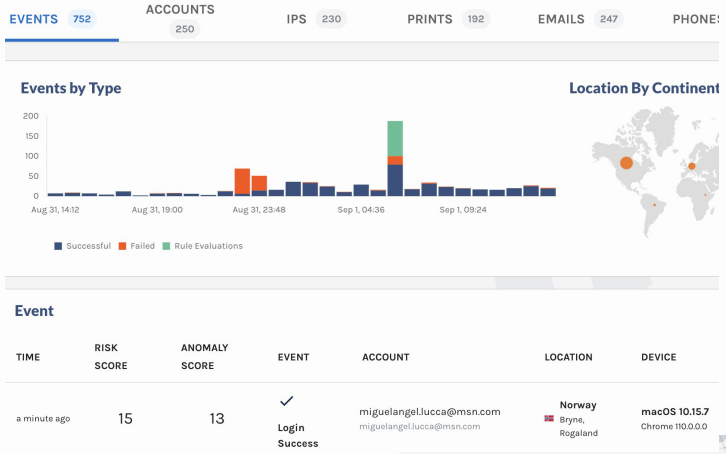
Improving Account Security with ITDR

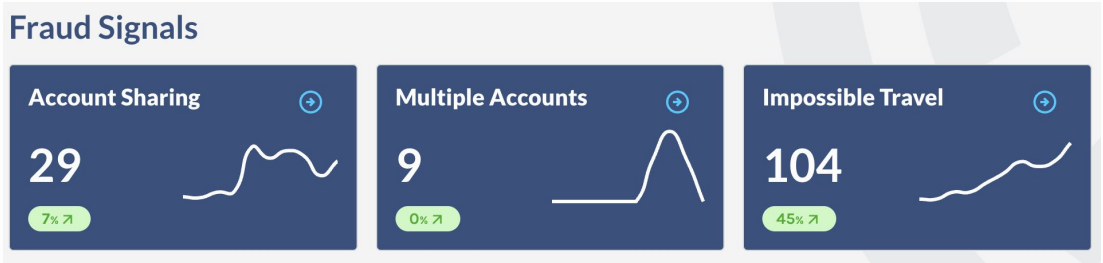
Bertold Kolics

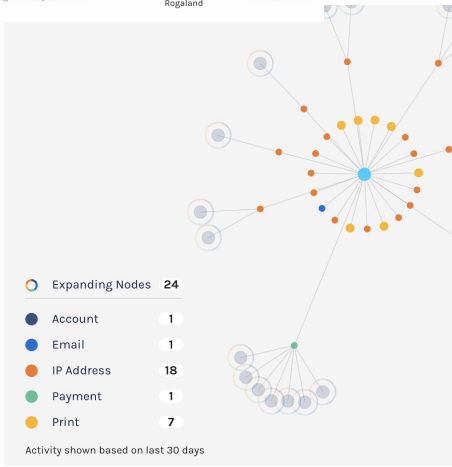
LASCON, Austin, TX
October 23, 2025

About Me

- Testing specialist
  - LDAP, SCIM, Identity Provisioning in past
- Advocate for Modern Testing Principles
- *News flash - October 14, 2025*
  - Imprivata acquires Verosint
- Verosint - software vendor
  - Detect & prevent online account fraud
- Slides: https://bertold.kolics.net/pages/







Why do we care?

- Detecting and preventing account fraud is **hard** with generic solutions
  - ITDR solutions are **account centric**
  - Some threats & attacks are hard to detect without this focus
  - Detection **speed** is key to reduce business impact
- Loss of … fill it in
  - **revenue** (e.g. promotion abuse, sharing services)
  - **customer satisfaction** (e.g. account takeover, noisy neighbor)
  - **brand reputation** (e.g. leaked PII)
- **Identity is the new perimeter**
  - cloud computing - explosion of hosted services
  - work from home - another threat vector
  - BYOD

VEROSINT

User Account Security is *broken* and *unsustainable*

61%

of all breaches exploit user accounts

User Accounts are Fastest Growing Attack Vector

3.3x

attack frequency increasing annually

$4.8M

average cost of a successful attack in 2024

292 days

average time from detection to remediation

VEROSINT

What is an identity?

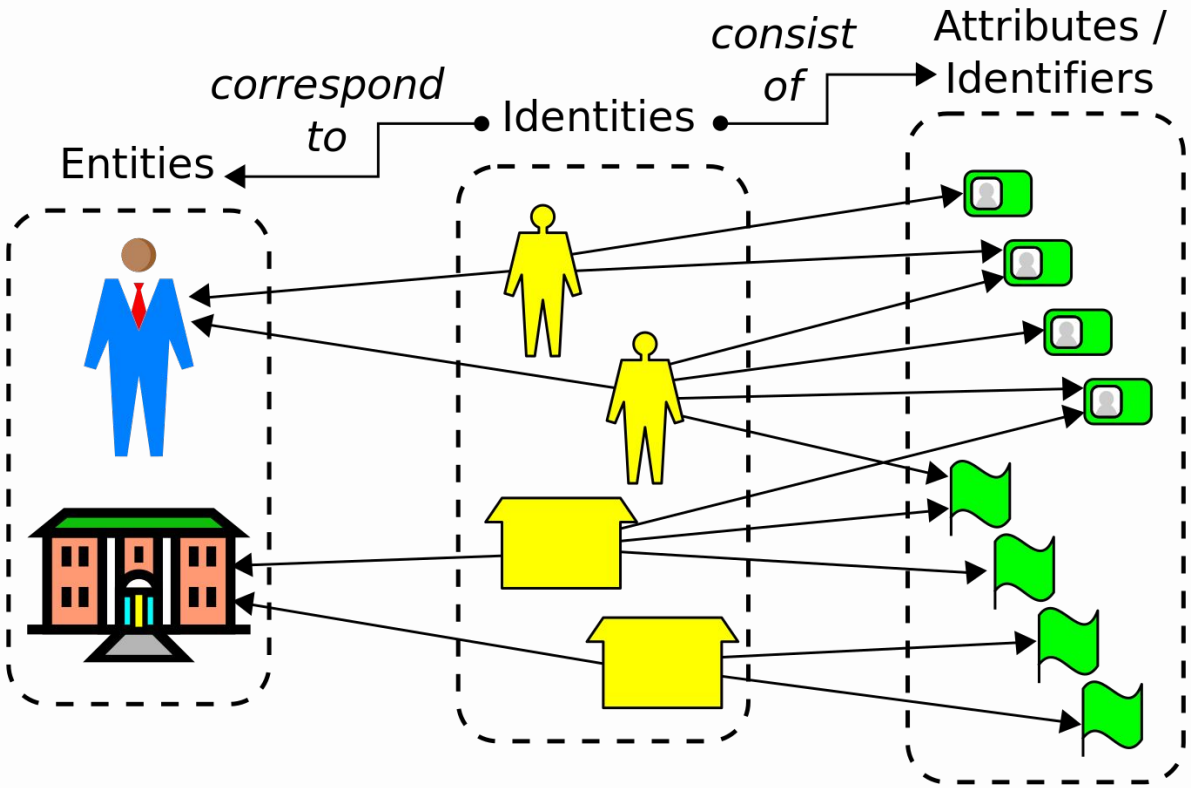


Image credit: Audun Jøsang / Wikipedia

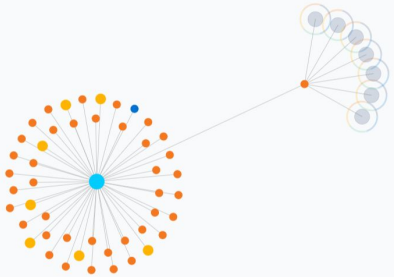
VEROSINT

User types

- Detection and prevention configuration may also depend on the **user type**
- Examples:
  - students, parents, staff at a school district
  - buyers, sellers, operators at a marketplace vendor
  - employees, contractors, and maybe executives at a traditional enterprise
- Different types
  - different behaviors
  - access patterns including location, time of day, time of week, frequency
  - devices, device types may differ

VEROSINT

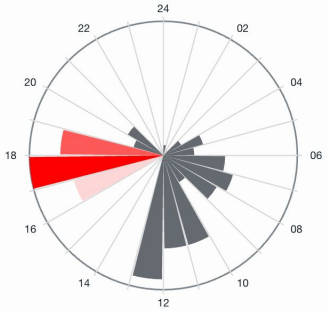
User behaviors



Expanding Nodes	7
Account	1
Email	1
IP Address	40
Print	7

Circadian Rhythm

Hourly activity, averaged over 30 days before the last seen event



Typical Activity
Outlier Activity

Outlier Activity indicates unusual account activity relative to other accounts in this workspace.

Location History

Activity over 30 days before the last seen event

Successful
Failed

- Locations
- ISPs, VPNs used
- Circadian rhythm
  - also weekday vs. weekend
- Number of events
- User agents
  - versions

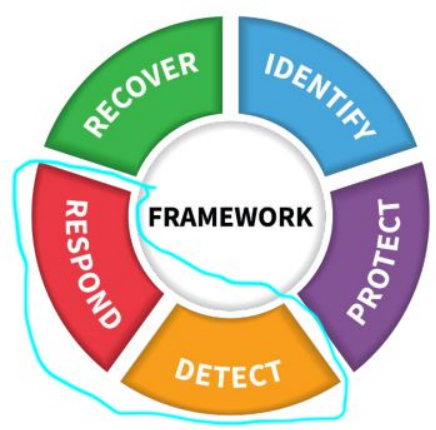
VEROSINT

Other facets

- Entity types
  - managed vs. unmanaged
  - human vs. non-human / AI agent
- Business context
  - normal vs. unexpected
  - CIAM vs. Enterprise
  - different applications - different contexts
  - single vs. multiple Identity Providers

VEROSINT

What concerns does ITDR address?



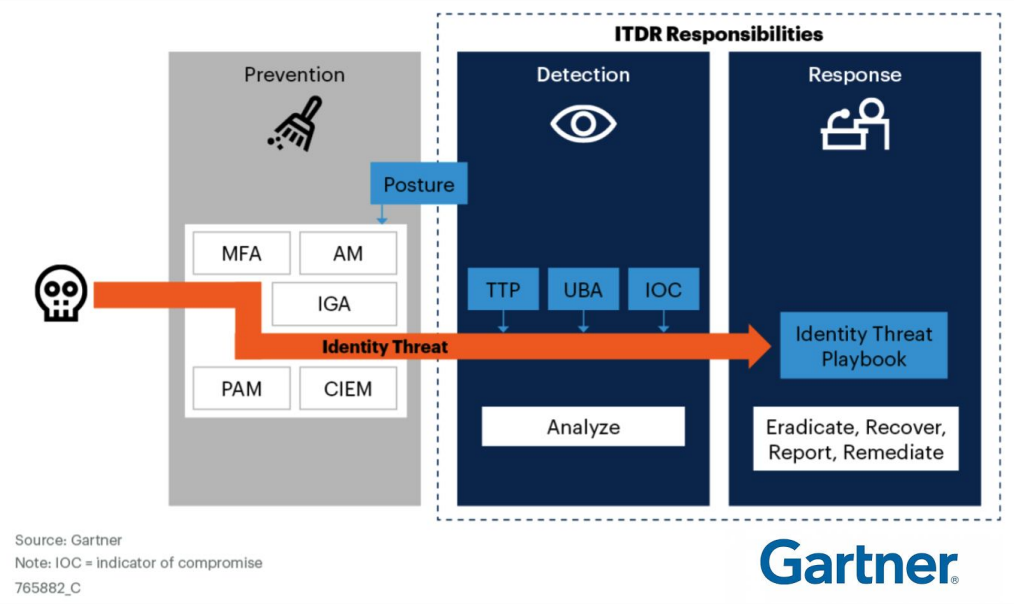
- ITDR: Identity Threat Detection & Response
- Threat **detection**:
  - ITDR solutions monitor user activity and access patterns to identify suspicious behavior that may indicate a threat.
- Threat **investigation**:
  - When a threat is detected, ITDR systems help investigate the incident, including identifying the source, scope, and impact.
- Threat **response**:
  - ITDR solutions can automate responses to threats, such as blocking access, disabling accounts, or alerting security teams.
- With a focus on **identity**:
  - Unlike other threat detection and response solutions (EDR, XDR, MDR), ITDR specifically focuses on the identity domain, which is often the entry point for many cyberattacks.

Image credit: NIST

VEROSINT

ITDR Illustrated

Modern cybercriminal tools & tactics circumvent traditional IAM prevention



- Detect indicators of attack by monitoring for TTPs
- Detect the moment an account is compromised by knowing what is normal for every user

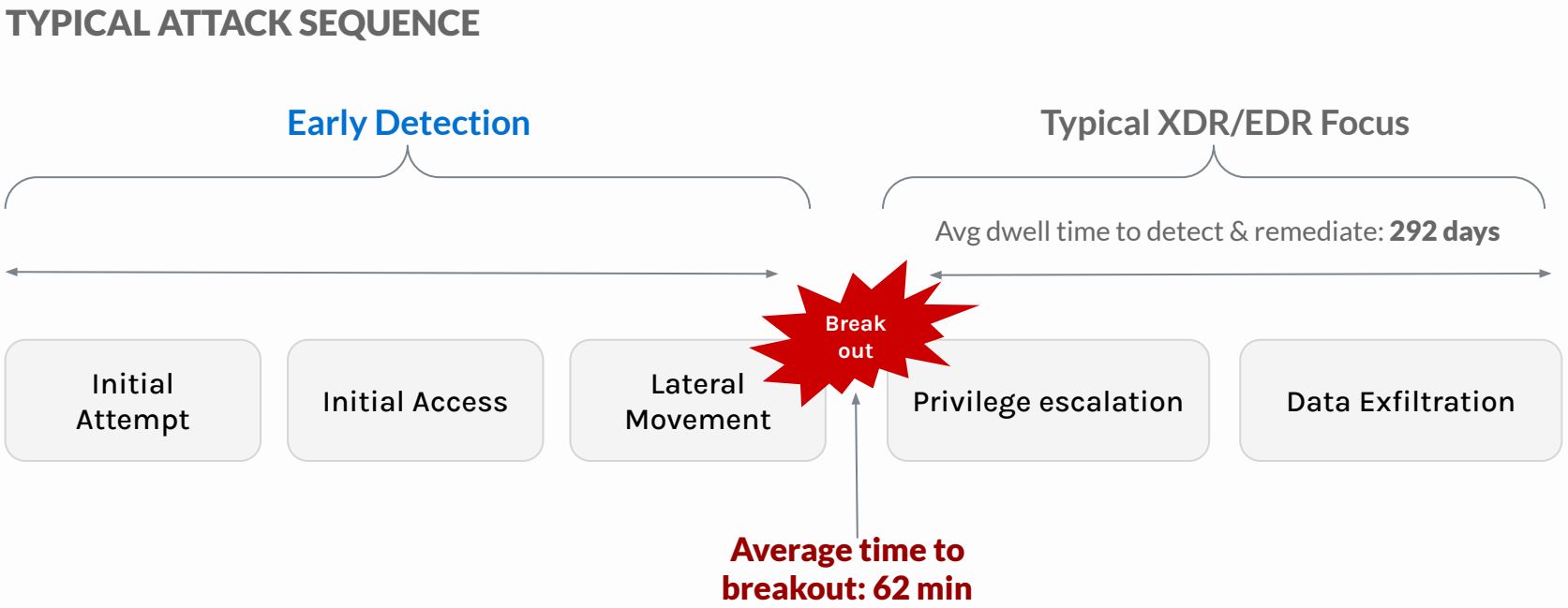
VEROSINT

Endpoint Detection & Response vs. ITDR

	EDR	ITDR
Scope	monitor, secure endpoints	identity-based threats across platforms, environments, systems
Data collected	process execution, file access, network traffic	user activity logs, access management logs
Threat visibility	endpoint activities, user devices	identity-based threats, privileged user behavior, access attempts, auth patterns
Incident response	threats at endpoint level	user behaviors across environments

VEROSINT

Contrasting ITDR and XDR/EDR



VEROSINT

Cybercriminals Don’t Break In, They Log In

- Credential Stuffing
- Account Takeover
- Session Sharing
- Stolen Credentials
- Brute Force Attacks
- MFA Fatigue Attack
- Suspicious IPs
- Insider Threats
- Unusual Device Use
- Impossible Travel
- Circadian Rhythm
- MFA Location Mismatch

VEROSINT

Detection, Prevention, Response

Prevent

Do we block all malicious activity?
Do we prevent access to malicious actors only?

Detect

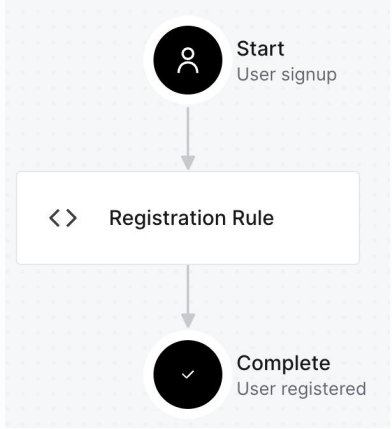
Can we identify new threats, risks?
Behaviors shifting, changing?

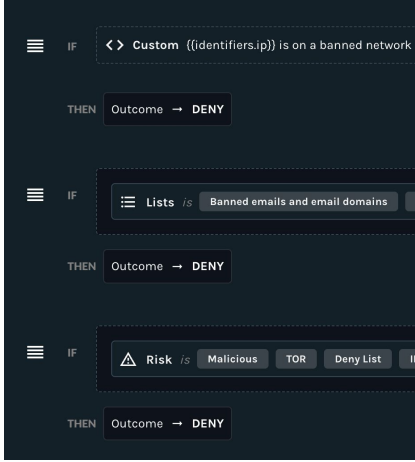
Respond

Actions - block user, terminate sessions
Should we block new threats, risks?
Handling the unexpected
Automated vs. manual

VEROSINT

Prevention - Example





Sign up attempt

Application

Risky?
Location, ToD, Device, etc.

ITDR

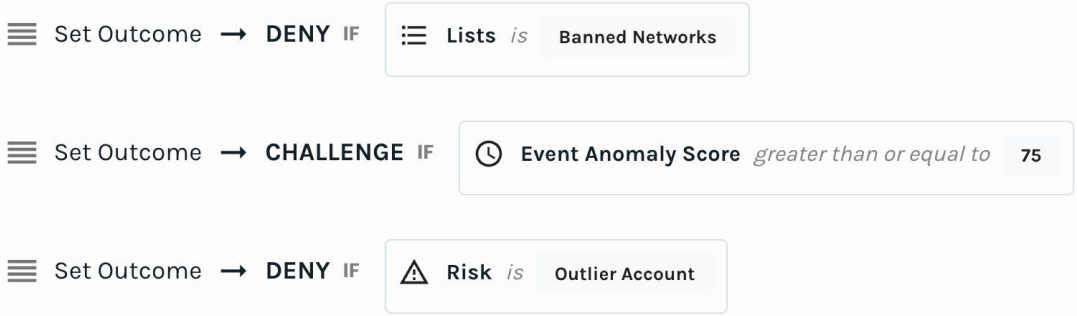
Deny

Deny
Challenge
Allow

VEROSINT

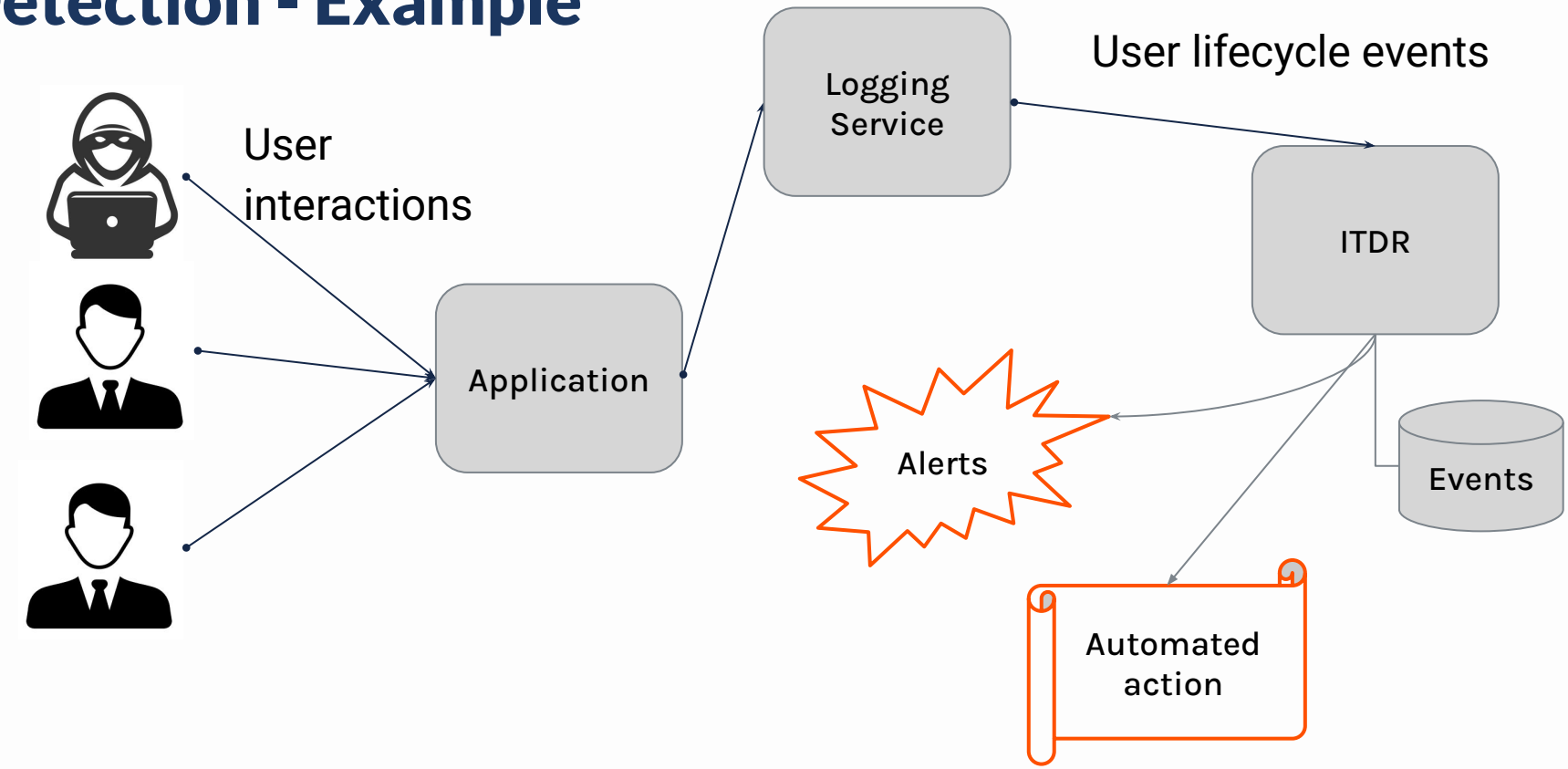
Preventing

- Rules to block unwanted traffic, allowing legitimate traffic
- Goldilock principle
  - block too much - lose potential legitimate business
  - block too little - business loss due to illegitimate activities
- Going beyond allow/deny
  - step-up authentication (e.g. MFA)
  - prompting (e.g. CAPTCHA)



VEROSINT

Detection - Example



VEROSINT

Detection - Analogy

Without ITDR

With ITDR

Image credit: Reddit

VEROSINT

Detection - Phases

User Actions

1. Log in
2. Use App
3. (sometimes)
   change password
   change email
4. (maybe) log out

Application Logs Events

ITDR Processes Events

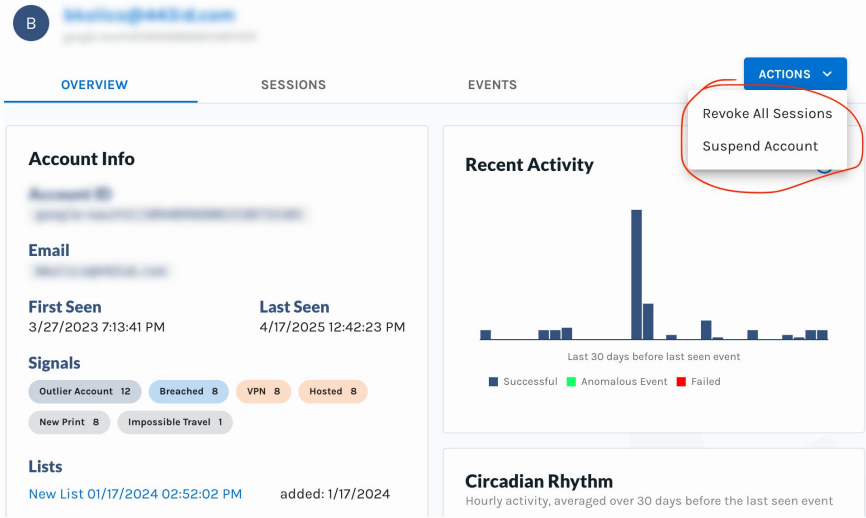
- Event enrichment
  - IP - location, country, VPN,
  - Email - breach, free/business
  - User Agent - obsolete, bot
  - Phone - DNO
- Building profile, trends
  - unusual in context
- Detecting emerging threats

Image credit: Reddit

VEROSINT

Responding

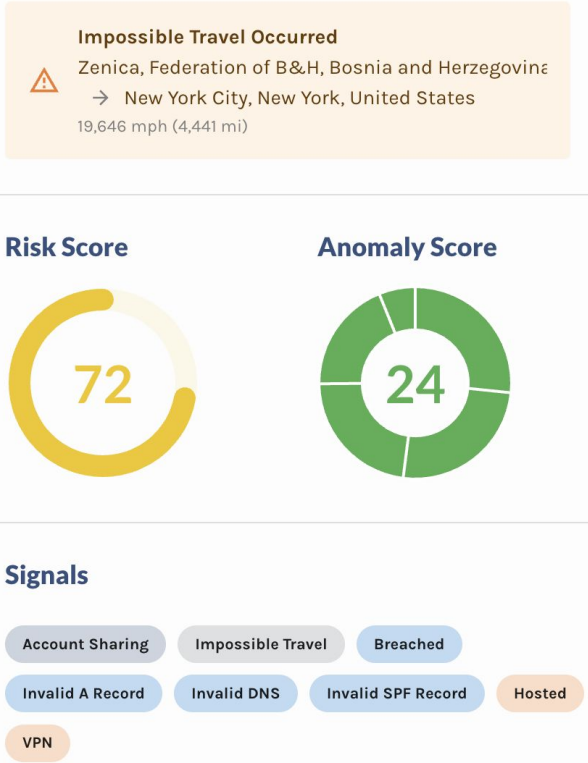
- Playbooks
  - manual / automated
- Actions
  - blocking, suspending users, sessions
  - revising prevention rules



VEROSINT

Threats vs. Risks

- Risks ~ events that could possibly indicate malicious behavior
  - IP is a Tor exit node
  - IP was involved in malicious activity
  - IP is not residential IP (and not a VPN)
  - Email is disposable
  - Email appears in a breach
  - User agent is obsolete
  - User agent is a bot
  - etc.



VEROSINT

Threats vs. Risks - cont’d

- Threats ~ specific, identified attacks on accounts / identities
  - account takeover
  - impossible travel
  - credential stuffing
  - session sharing
  - MFA location mismatch
  - multiple accounts
  - etc.

VEROSINT

Threat: Impossible Travel

- Definition
  - successful subsequent authentication events from separate locations that is impossible for the same person to execute
- Challenges:
  - location accuracy
  - VPN use
  - Relays (iCloud, Edge VPN)
    - even on same physical device - Safari vs. non-Safari
  - there is a 3rd dimension
- Cause:
  - likely leaked or breached credentials

VEROSINT

Threat: Credential Stuffing

- Definition
  - many failed login attempts - and few successful - typically in a short period of time from a small set of locations against a large number of accounts
- Challenges:
  - large volume of events
- And:
  - could lead to account takeover
  - could also trip impossible travel alerts

VEROSINT

Threat: Credential Stuffing

Dec 31 - Credential Stuffing Attack Credential Stuffing

12/31/2024 3:50:18 AM - 1/2/2025 10:25:26 PM

Accounts

5
TAKEOVERS

4,306
FAILED TAKEOVERS

3,892,910
NONEXISTENT ACCOUNTS

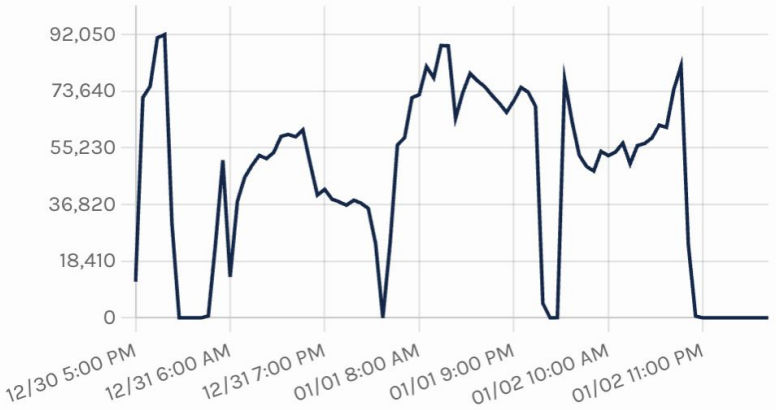
ATTACK ORIGINATION

462,535 IPs across **107 countries**

ATTACK SIZE & SCOPE

3,897,221 attempts in **2** days, **18** hr, **35** min, **8** sec

Total Events



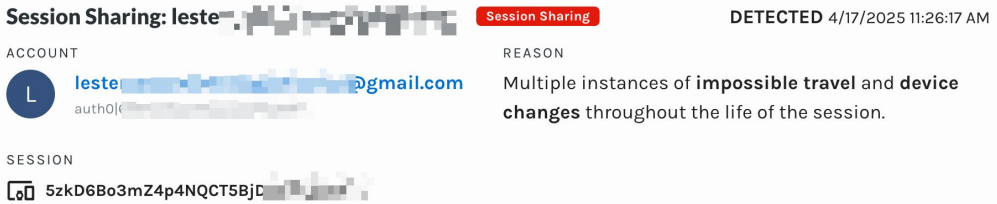
SEE MORE

RESOLVE

VEROSINT

Threat: Session Sharing

- Definition
  - limited validity access tokens shared between multiple users likely at different locations to access the same application
- How?
  - Chrome Extensions exist to facilitate this (or just use Chrome DevTools)
- Why?
  - circumvent login restrictions



VEROSINT

Other Detection Techniques

- Device fingerprinting
  - browsers - may require browser extensions or custom libraries
  - not limited to browsers
- Honeypots
  - cheap way to detect malicious activity
- Canary Accounts
  - for example, a user who should never be seen in production

VEROSINT

Surprises

- The share of automated traffic on the internet (~half)
- Amount of traffic from IPv6 addresses
  - some 5G ISPs only use IPv6
  - size of IPv6 networks assigned to end users
- Windows XP is still used
- Lookalike domains: smilesllc@outlokk.com

VEROSINT

Just for Fun

- Default prefix length of IPv6 networks?
- Homoglyphs
  - charlie@someagency.com - can you spot the homoglyph?
- Can you guess the application using this user agent string?

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1)
AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1
Safari/601.2.4 facebookexternalhit/1.1 Facebot Twitterbot/1.0
```


VEROSINT

Answers

- Default prefix length of IPv6 networks?
  - **/64** (!)
- Homoglyphs
  - charlie@someagency.com - can you see it now?: **c**harlie@someagency.com
- Can you guess the application using this user agent string?

  ```
  Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1)
  AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1
  Safari/601.2.4 facebookexternalhit/1.1 Facebot Twitterbot/1.0
  ```

  The answer: **Messages app on iOS**

VEROSINT

Resources

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- Newsletters
  - Risky Business - risky.biz
  - TL;DR security - tldrsec.com
- T-Pot honeypot - https://github.com/telekom-security/tpotce
- Homoglyph fun - https://www.dcode.fr/homoglyphs-homographs-generator

Thank You

www.imprivata.com
bertold.kolics@imprivata.com