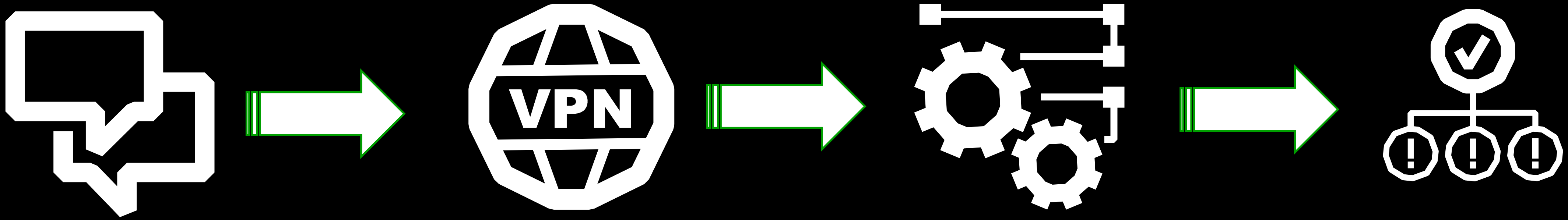
AI-Based Security Management delivered via Cloud

How modern AI and cloud-based analytics tools increase efficiency and uncover modern credential-based attacks.

Felix Blanke | Senior Manager, Sales Engineering, Europe

DAY 3
HUMANS STILL
THINK I'M LOST

Cyber Attack: Timeline



The answer?

“There are only two types of companies: those that have been hacked and those that don’t know they have been hacked.”

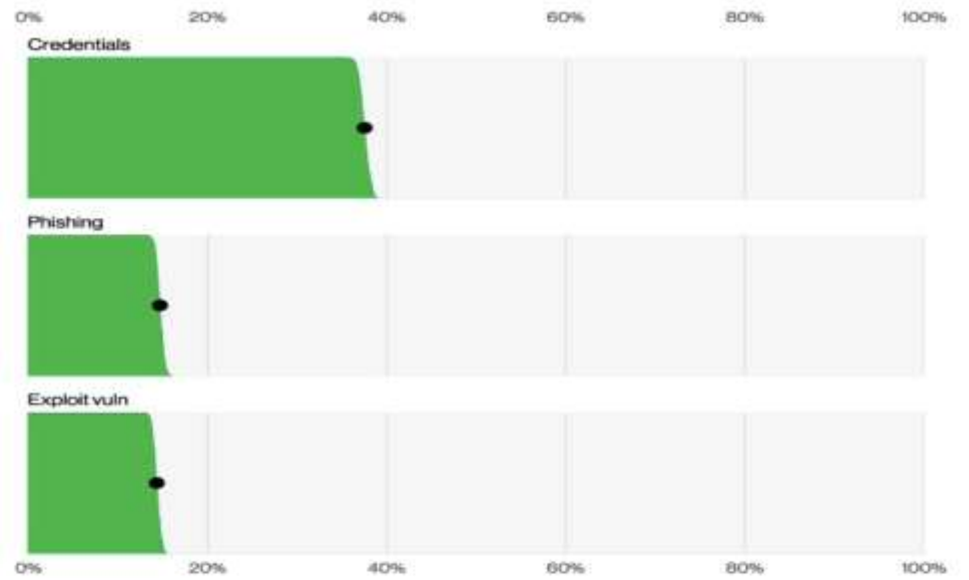


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

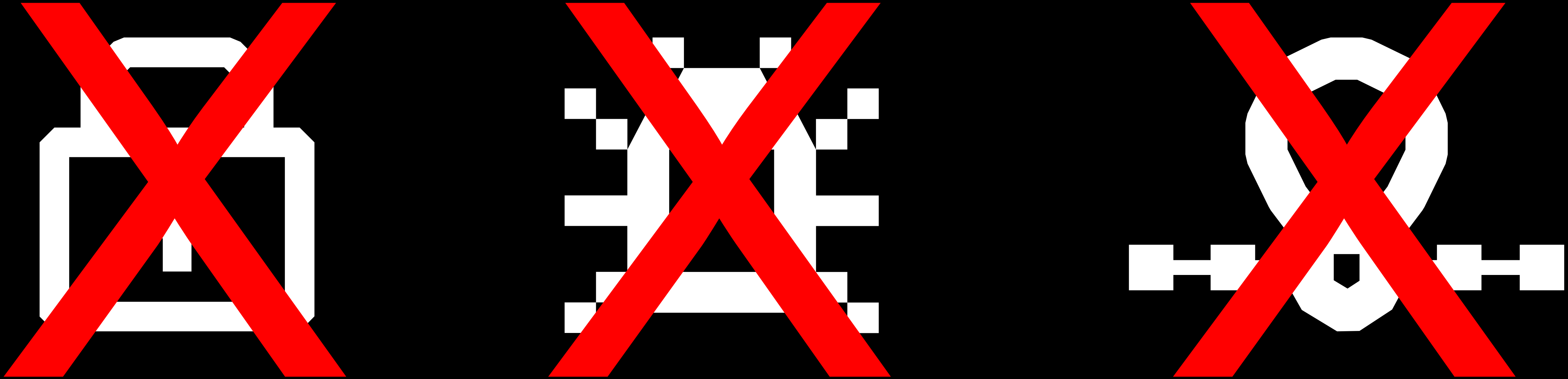
Source: DBIR 2024 by Verizon → https://www.verizon.com/business/resources/reports/dbir/

It's all about the creds™

Ralph Pisani

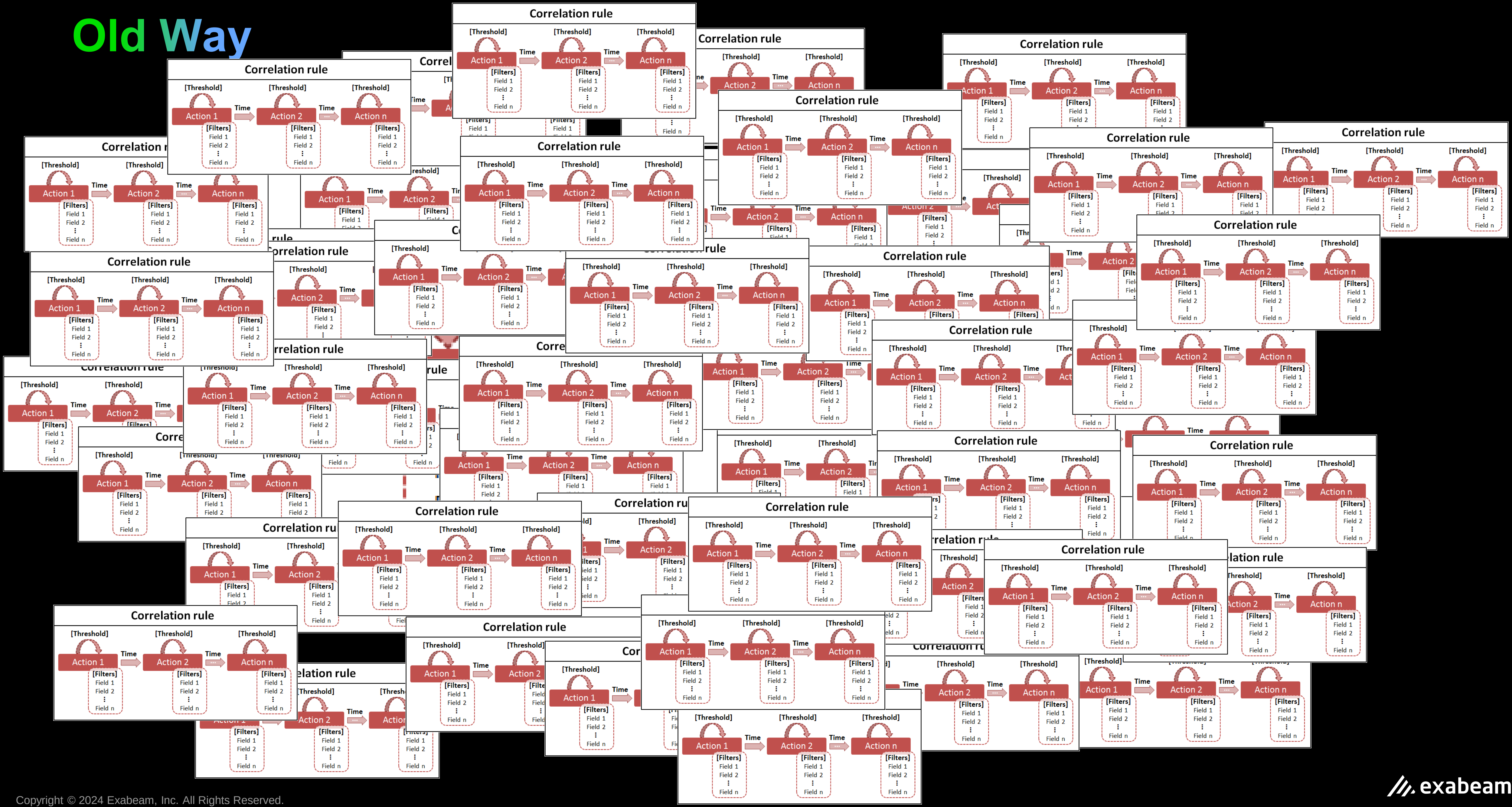
What are companies doing about it today?

How to detect credential based attacks?



VS.

Old Way

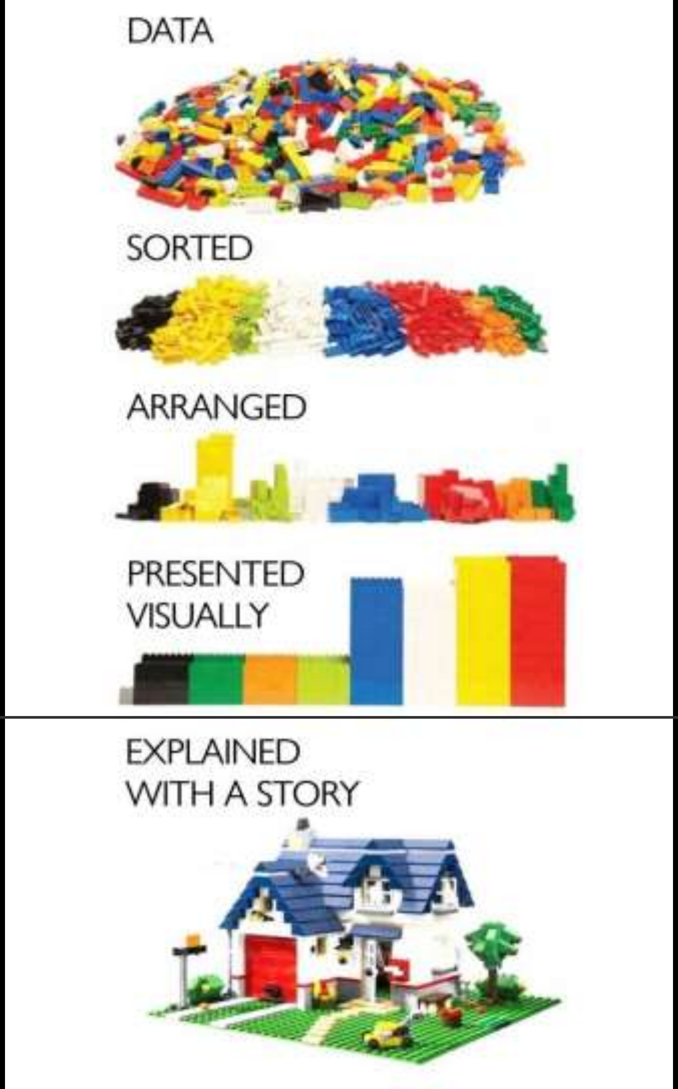


exabeam

Old Way / Challenges

- Can only detect known patterns
- Tons of false positives
- Very time intensive to fine tune
- Very time intensive to expand
- No automation in terms of investigation work

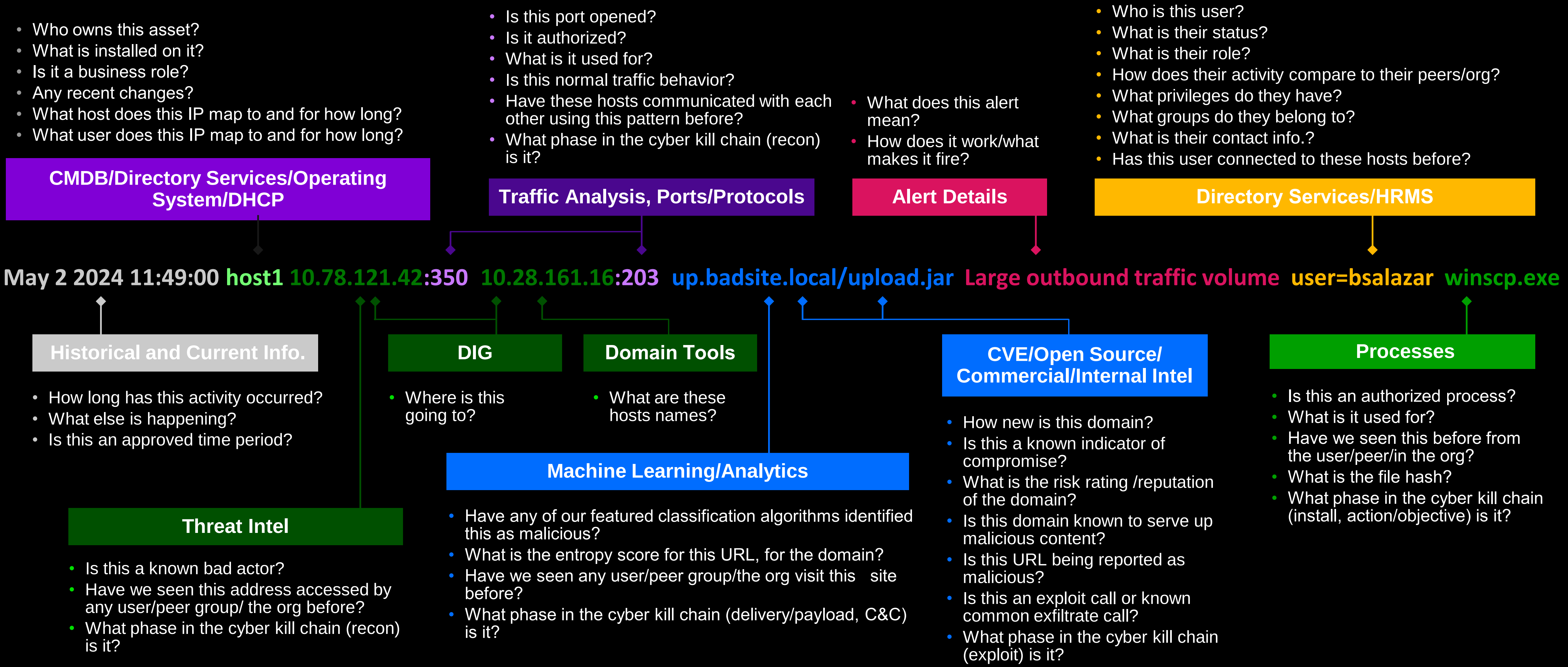
The New Way



Old Way

New Way

What Are the Right Questions?



May 2 2024 11:49:00 host1 10.78.121.42:350 10.28.161.16:203 up.badsite.local/upload.jar Large outbound traffic volume user=bsalazar winscp.exe

CMDB/Directory Services/Operating System/DHCP

- Who owns this asset?
- What is installed on it?
- Is it a business role?
- Any recent changes?
- What host does this IP map to and for how long?
- What user does this IP map to and for how long?

Traffic Analysis, Ports/Protocols

- Is this port opened?
- Is it authorized?
- What is it used for?
- Is this normal traffic behavior?
- Have these hosts communicated with each other using this pattern before?
- What phase in the cyber kill chain (recon) is it?

Alert Details

- What does this alert mean?
- How does it work/what makes it fire?

Directory Services/HRMS

- Who is this user?
- What is their status?
- What is their role?
- How does their activity compare to their peers/org?
- What privileges do they have?
- What groups do they belong to?
- What is their contact info.?
- Has this user connected to these hosts before?

Historical and Current Info.

- How long has this activity occurred?
- What else is happening?
- Is this an approved time period?

DIG

- Where is this going to?

Domain Tools

- What are these hosts names?

Threat Intel

- Is this a known bad actor?
- Have we seen this address accessed by any user/peer group/ the org before?
- What phase in the cyber kill chain (recon) is it?

Machine Learning/Analytics

- Have any of our featured classification algorithms identified this as malicious?
- What is the entropy score for this URL, for the domain?
- Have we seen any user/peer group/the org visit this site before?
- What phase in the cyber kill chain (delivery/payload, C&C) is it?

CVE/Open Source/ Commercial/Internal Intel

- How new is this domain?
- Is this a known indicator of compromise?
- What is the risk rating /reputation of the domain?
- Is this domain known to serve up malicious content?
- Is this URL being reported as malicious?
- Is this an exploit call or known common exfiltrate call?
- What phase in the cyber kill chain (exploit) is it?

Processes

- Is this an authorized process?
- What is it used for?
- Have we seen this before from the user/peer/in the org?
- What is the file hash?
- What phase in the cyber kill chain (install, action/objective) is it?

exabeam

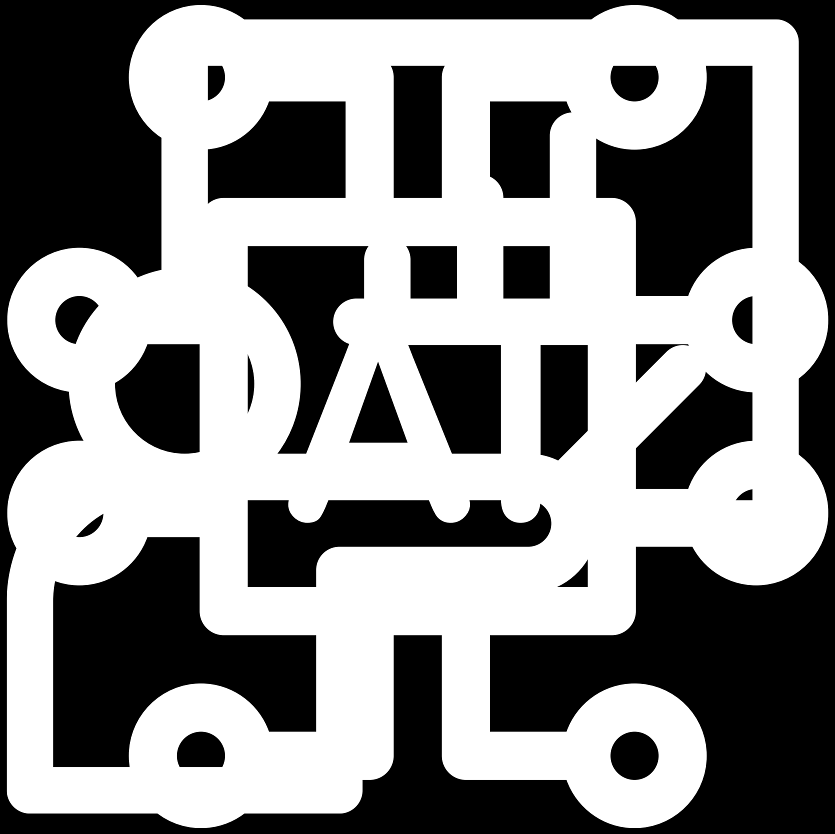
New Way / Advantages

- Learns behavior of users
- Way more acurate given every user has its own baseline
- Fine tunes automatically
- By definition no false positives
- Can detect “unknowns”
- Automates big part of the investigation by answerig all those questions automatically

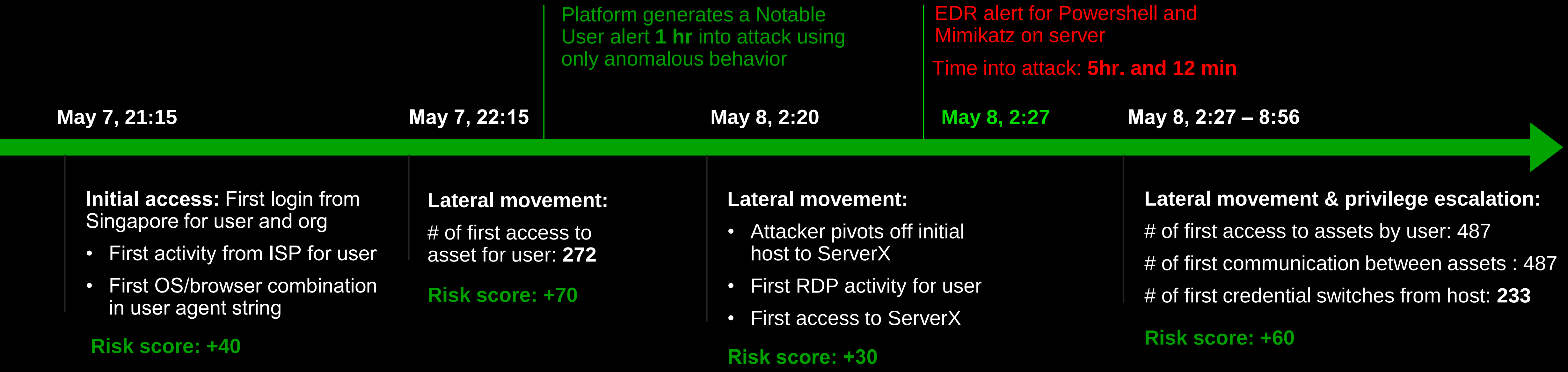
What could those numbers refer to?

12%	Detection
62%	Triage & Investigation
26%	Incident Response

Investigation Automation



Looking at the complete Picture of a *Compromised Insider* Incident



May 7, 21:15

Initial access: First login from Singapore for user and org

- First activity from ISP for user
- First OS/browser combination in user agent string

Risk score: +40

May 7, 22:15

Lateral movement:

# of first access to asset for user: **272**

Risk score: +70

Platform generates a Notable User alert **1 hr** into attack using only anomalous behavior

May 8, 2:20

Lateral movement:

- Attacker pivots off initial host to ServerX
- First RDP activity for user
- First access to ServerX

Risk score: +30

EDR alert for Powershell and Mimikatz on server

Time into attack: **5hr. and 12 min**

May 8, 2:27

May 8, 2:27 – 8:56

Lateral movement & privilege escalation:

# of first access to assets by user: 487

# of first communication between assets : 487

# of first credential switches from host: **233**

Risk score: +60

What did we detect:

- Comprehensive and complete picture of the attack
- Details of abnormal user behavior and Lateral Movement
- Compromised Credentials connecting on the VPN from Singapore
- Assets affected: **759**
- Number of credentials switched: **234**
- notepad.exe running out of an abnormal directory C:\\PerfLogs\
- Detailed timeline of activities and assets

Outcomes enabled by Us

- Remediation of the entire threat
- Led to resetting all 234 credentials
- Informed the need to preform AV scans of all assets involved
- Helped review all users as assets to identify abnormal activities
- Insights helped decision to clean up ServerX

Thank You

exabeam™