UC Davis SOC

Jeff Rowe, Shannen McKenna, Conrad Carter, Rasilind Berks, Angela Appiah

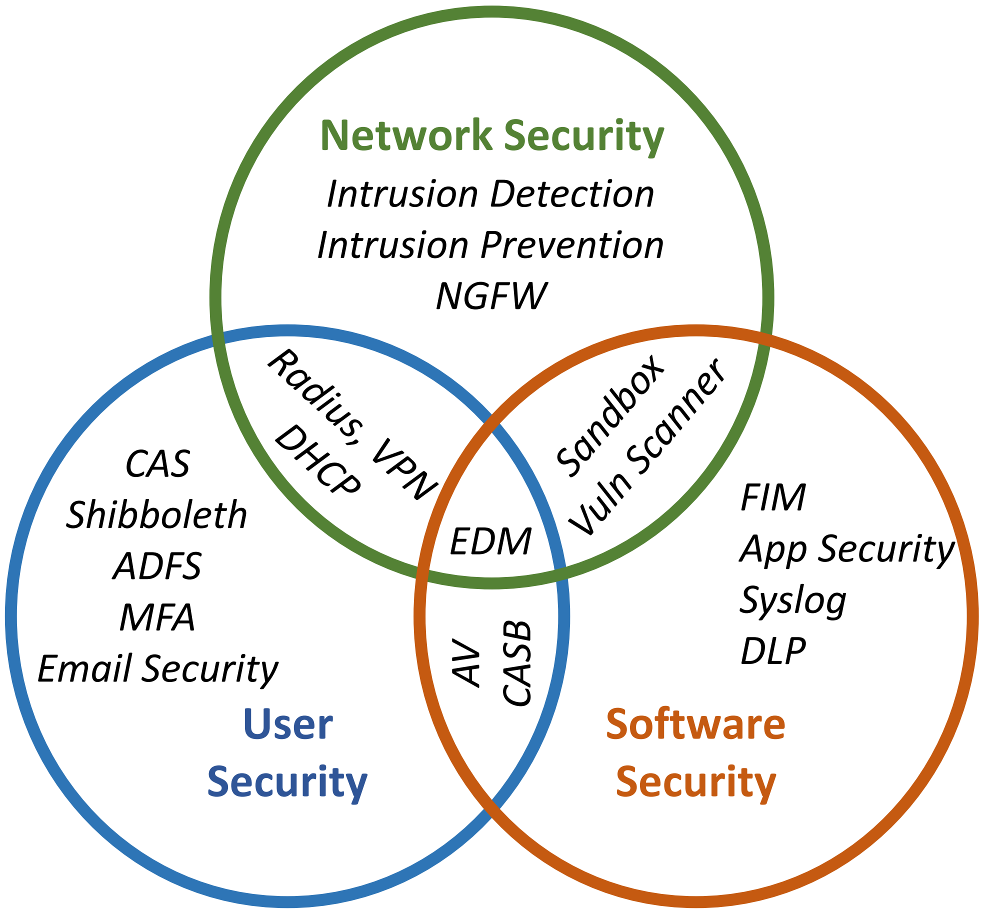
11/8/2022

UC Davis IT Environment

- 5000 servers
- 55,000 clients
- 170,000 user accounts
- High-value research
- Student Health Center (HIPAA)
- 120 credit card merchants (PCI)
- DoD funded research
- PG&E substation
- Police, Fire, USDA
- Airport (KEDU)
- Personal residences
- *Open access policies*
- *Massively distributed federated IT governance*

Security Operations at UC Davis

UCD SOC Technology Portfolio



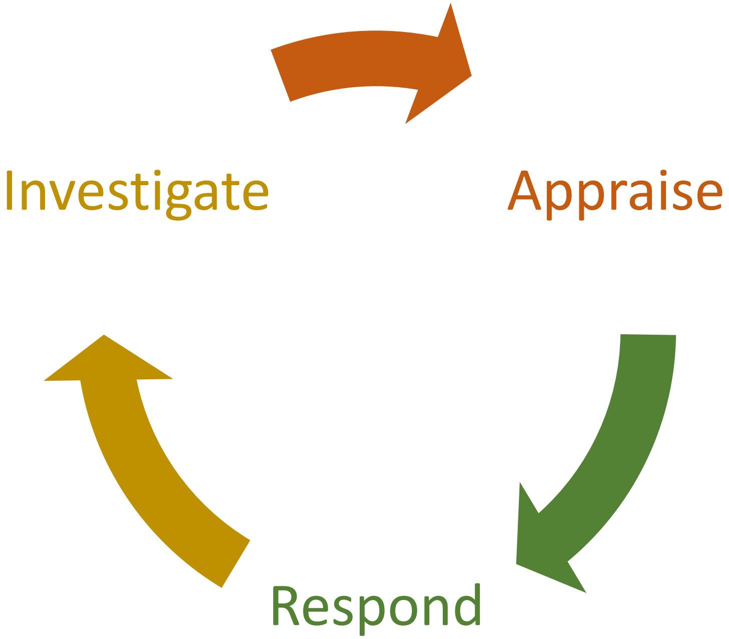
- Domain-specific technology.
- Overlap technology that links core domains.
- All these system generate event streams. Currently 10,000 events/sec and growing.

SOC workflows are about managing this information flow

Security Operations Information Flow Categories

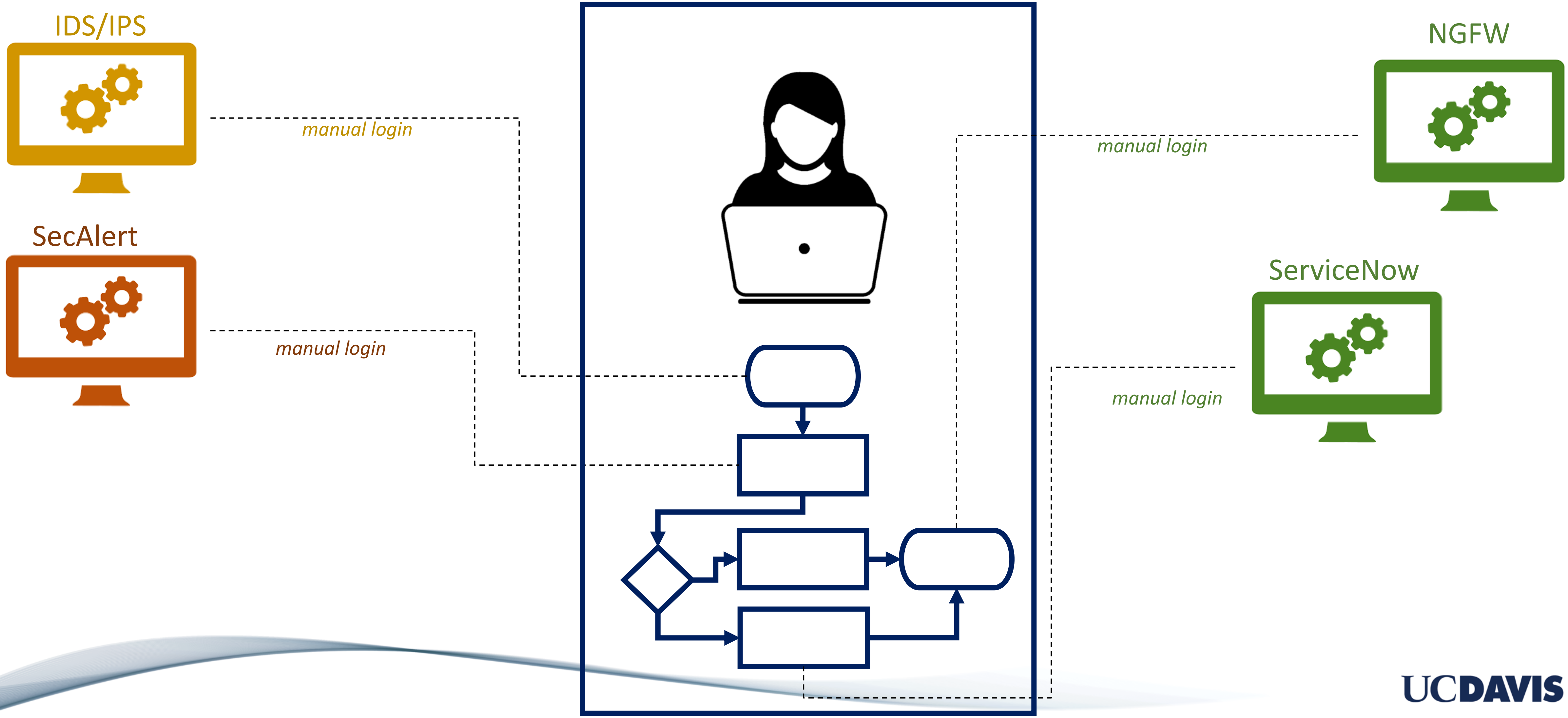
- Events *(Input)*
  - Time-series data streams generated by SOC tech portfolio
  - Used for manual and automated investigation
  - Cross domain technology enables aggregation and correlation
- Configuration *(Static Parameters)*
  - Relatively static system state and configuration
  - Used to improve correlation with semantic enrichment
  - Provides context for risk-based appraisal and reporting
- Directives *(Output)*
  - Actions taken in response to investigation and appraisal
  - Used to move systems from insecure to secure states
  - Implements Incident Response

Abstract Security Operations Workflow



- Events
  - Data streams generated by system operations
- Configuration
  - Current system state and value
- Directives
  - Actions taken in response to investigation outcome

SOC Workflow Process



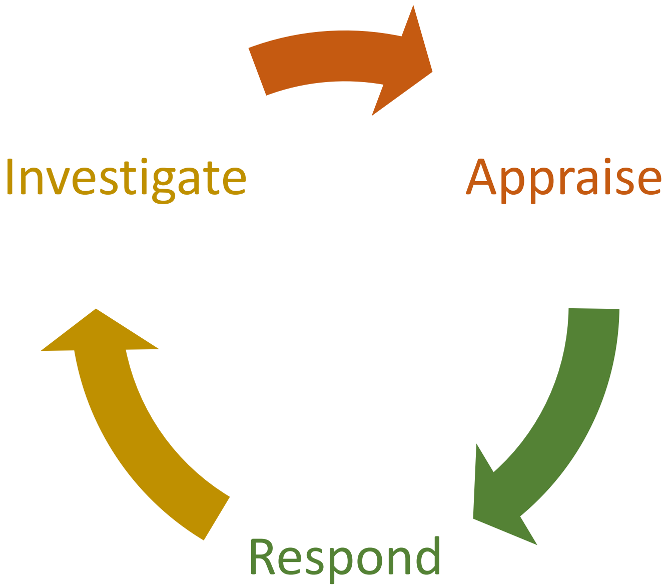
Automating Security Operations

“In chess, sometimes the machine wins and sometimes the Grand Master wins. But a machine assisted amateur can beat them both.”

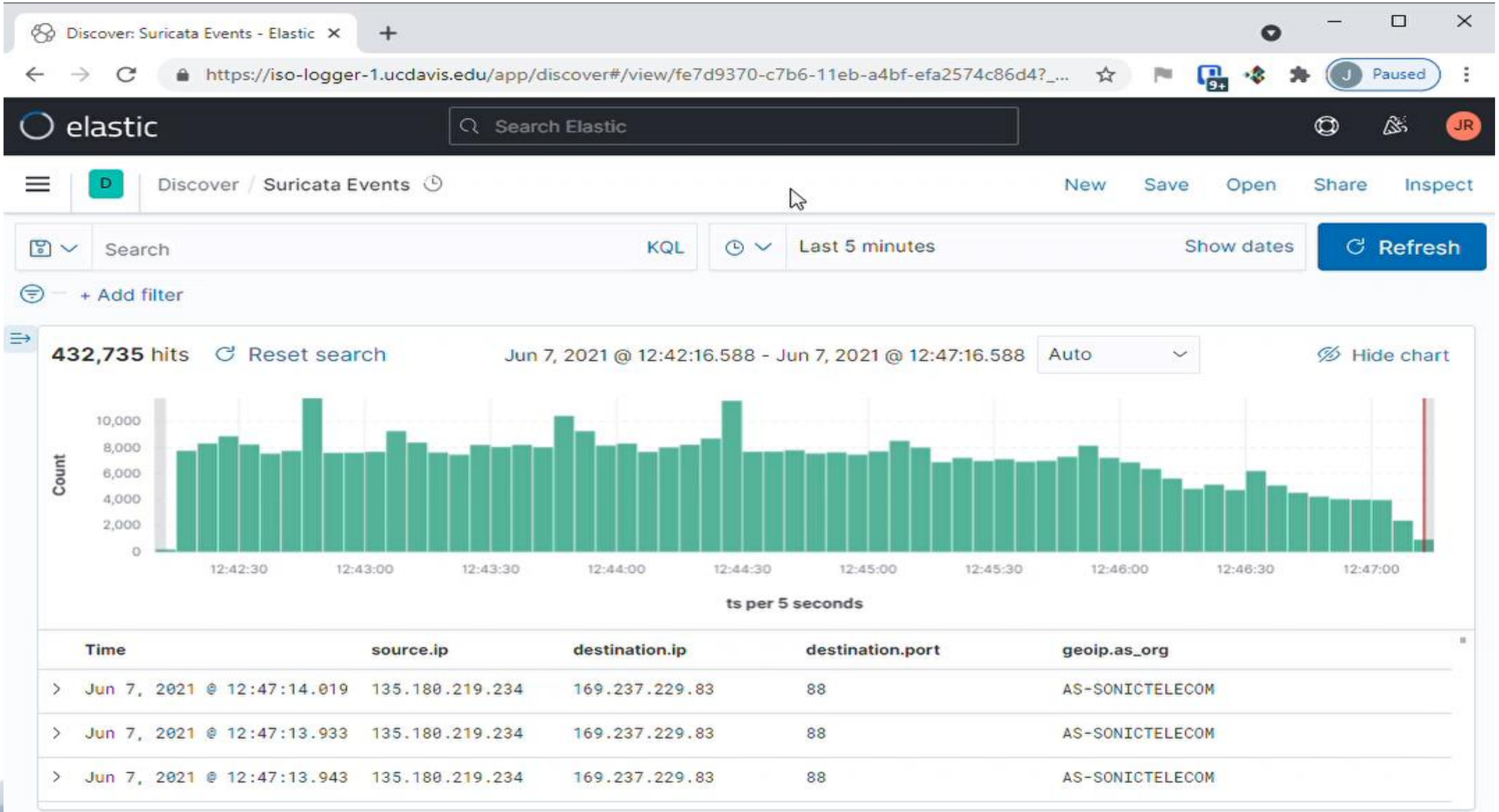
- *Bennett Bertenthal, IU Prof. of Cognitive Science*

Leapfrog the SEIM and implement SOAR

- Automate, automate, automate.
- APIs instead of portals and dashboards.
- Standalone scripting vs. Software Engineering
- Use custom ML analytics to assist in security operations workflows

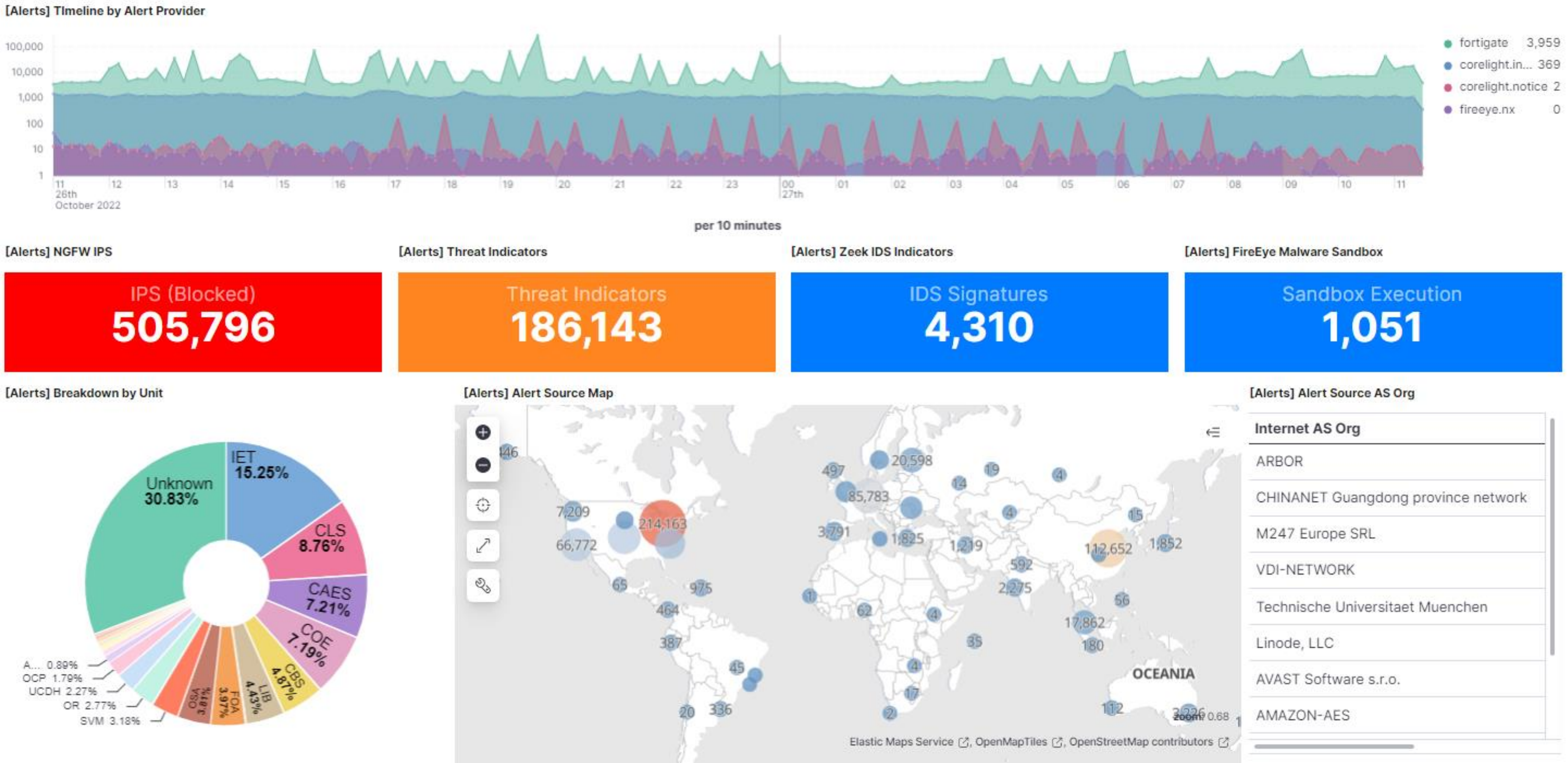


We have raw data events.



Time	source.ip	destination.ip	destination.port	geoip.as_org
Jun 7, 2021 @ 12:47:14.019	135.180.219.234	169.237.229.83	80	AS-SONICTELECOM
Jun 7, 2021 @ 12:47:13.933	135.180.219.234	169.237.229.83	80	AS-SONICTELECOM
Jun 7, 2021 @ 12:47:13.943	135.180.219.234	169.237.229.83	80	AS-SONICTELECOM

24 Hours of UC Davis Security Alerts



[Alerts] TImeline by Alert Provider

[Alerts] NGFW IPS

IPS (Blocked)
505,796

[Alerts] Threat Indicators

Threat Indicators
186,143

[Alerts] Zeek IDS Indicators

IDS Signatures
4,310

[Alerts] FireEye Malware Sandbox

Sandbox Execution
1,051

[Alerts] Breakdown by Unit

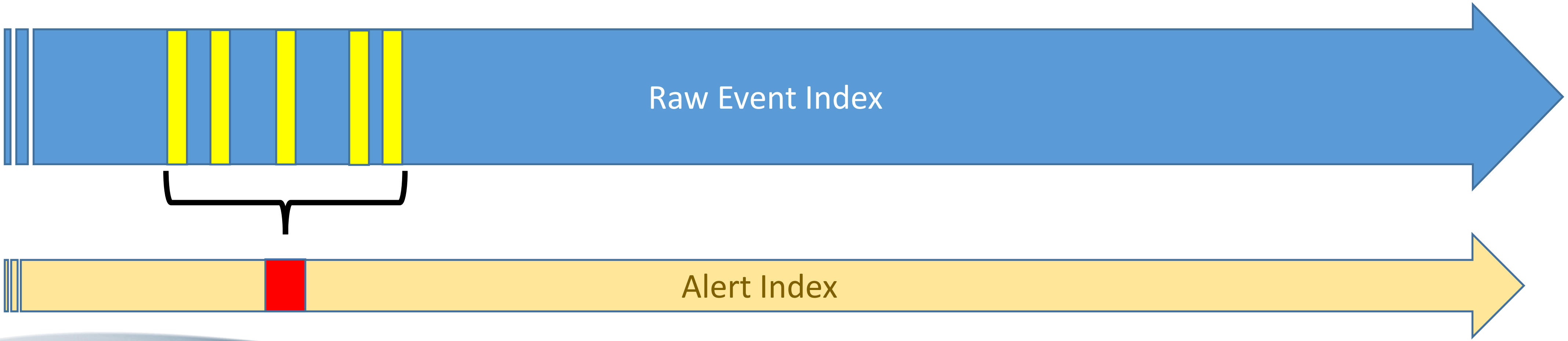
[Alerts] Alert Source Map

[Alerts] Alert Source AS Org

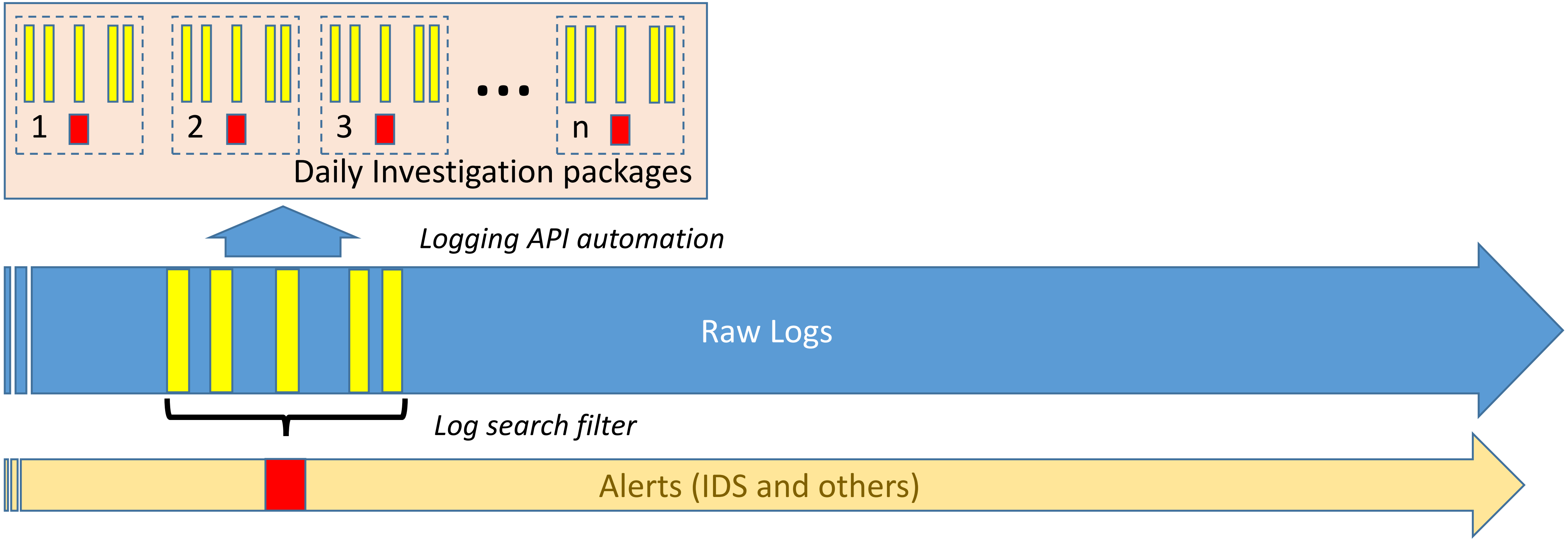
Internet AS Org
ARBOR
CHINANET Guangdong province network
M247 Europe SRL
VDI-NETWORK
Technische Universitaet Muenchen
Linode, LLC
AVAST Software s.r.o.
AMAZON-AES

Automating Alert Investigations

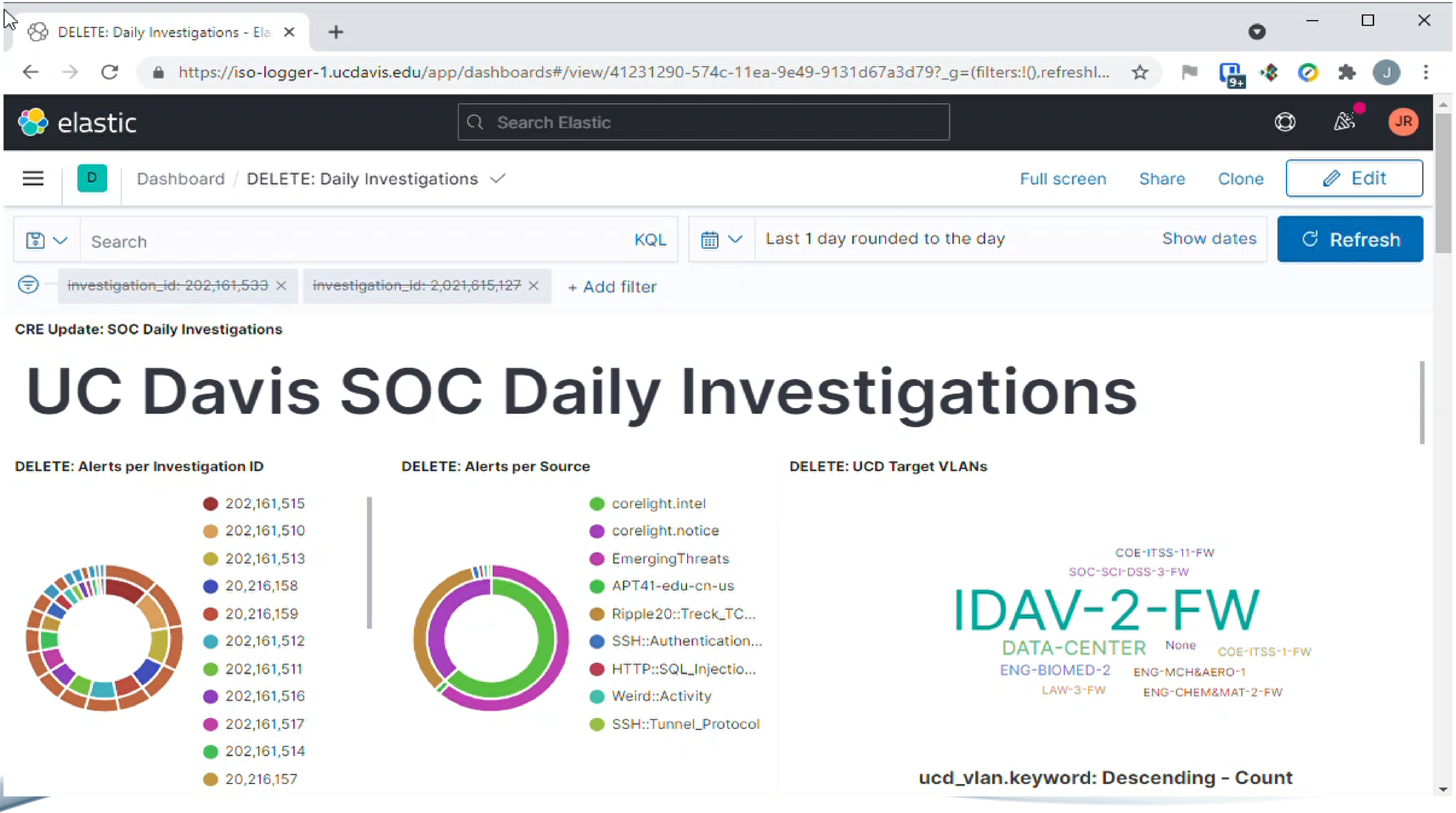
- Packaging Security Investigations
  - Alert stream provides pointers into the raw event stream (TCP conn, protocol decode, host logs)
  - Bracket connection events matching alert features.
  - Use Elastic REST API to automate alert ***filtering***, connection ***matching and aggregation***, and ***investigation packaging***.



UCDAVIS


1
2
3
…
n
Daily Investigation packages
Logging API automation
Raw Logs
Log search filter
Alerts (IDS and others)

Daily Investigation Process



CRE Update: SOC Daily Investigations

UC Davis SOC Daily Investigations

DELETE: Alerts per Investigation ID

DELETE: Alerts per Source

DELETE: UCD Target VLANs

ucd_vlan.keyword: Descending - Count

SOC Analytics

Outbound Encrypted Data Flow

The Problem

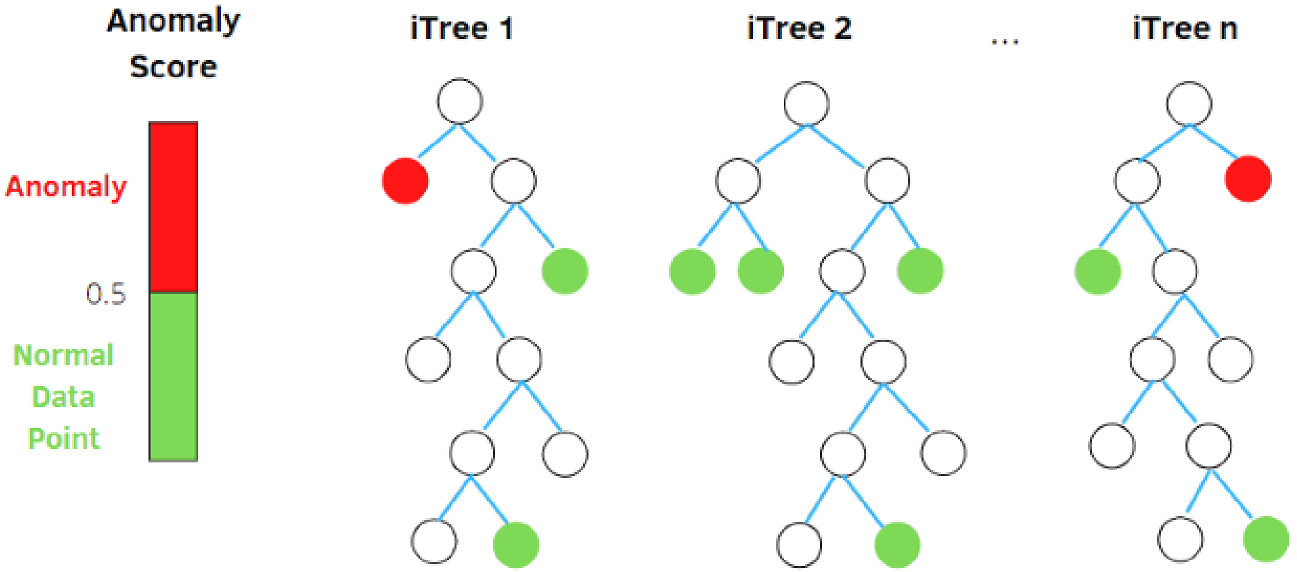
- What data leaves UC Davis?
- The lion’s share of network traffic is TLS encrypted.
- Large data transfers off-campus are normal.
- How to identify irregular data outflows from UCD to external clients?

Approach:

- Use all fields in the connection log (Bro/Zeek/Corelight conn.log) to identify anomalies: resp_ip_bytes, duration, ASN org, location, …
- Apply ***Isolation Forest*** AI algorithm to score anomalous connections.
- High anomaly score connections are added to the alert index for SOC investigation.

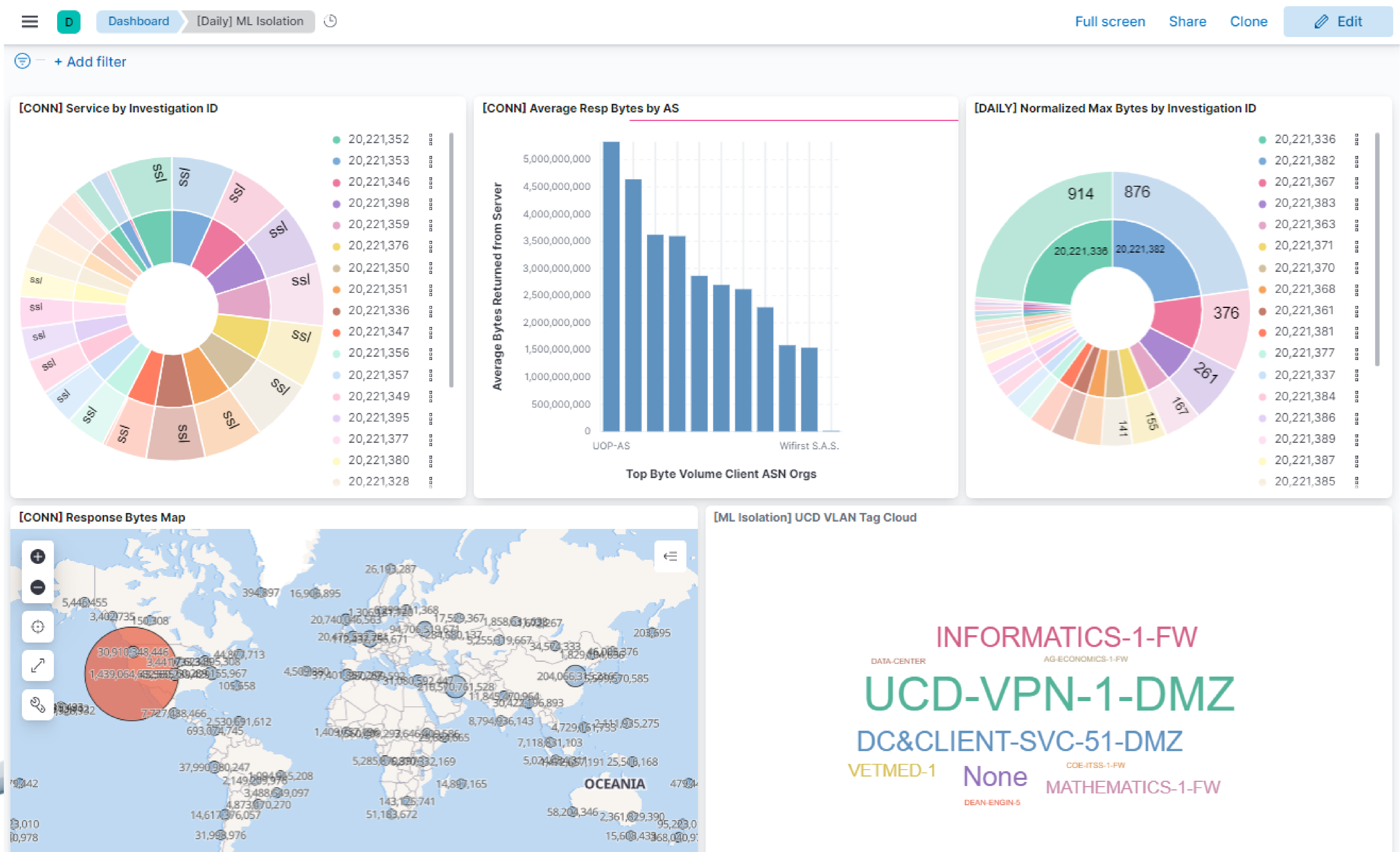
Isolation "Score"

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}}$$



Criteria for “Unusual”

UCDAVIS


D
Dashboard
[Daily] ML Isolation
Full screen
Share
Clone
Edit
+ Add filter
[CONN] Service by Investigation ID
ssl
20,221,352
20,221,353
20,221,346
20,221,398
20,221,359
20,221,376
20,221,350
20,221,351
20,221,336
20,221,347
20,221,356
20,221,357
20,221,349
20,221,395
20,221,377
20,221,380
20,221,328
[CONN] Average Resp Bytes by AS
Average Bytes Returned from Server
5,000,000,000
4,500,000,000
4,000,000,000
3,500,000,000
3,000,000,000
2,500,000,000
2,000,000,000
1,500,000,000
1,000,000,000
500,000,000
0
UOP-AS
Wifirst S.A.S.
Top Byte Volume Client ASN Orgs
[DAILY] Normalized Max Bytes by Investigation ID
914
876
20,221,336
20,221,382
376
261
167
155
141
20,221,336
20,221,382
20,221,367
20,221,383
20,221,363
20,221,371
20,221,370
20,221,368
20,221,361
20,221,381
20,221,377
20,221,337
20,221,384
20,221,386
20,221,389
20,221,387
20,221,385
[CONN] Response Bytes Map
26,103,287
394,897
16,906,895
5,446,455
3,402,735
150,308
30,910,348,446
7,727,188,466
2,530,691,612
693,074,745
105,658
44,877,713
203,695
17,529,367
34,574,333
204,066,315
11,845,470,964
30,422,196,893
8,794,936,143
4,729,161,753
7,118,831,103
37,990,380,247
14,887,165
143,125,741
51,183,672
14,617,476,057
31,998,976
58,204,346
2,361,829,390
OCEANIA
[ML Isolation] UCD VLAN Tag Cloud
INFORMATICS-1-FW
DATA-CENTER
AG-ECONOMICS-1-FW
UCD-VPN-1-DMZ
DC&CLIENT-SVC-51-DMZ
VETMED-1
None
COE-ITSS-1-FW
MATHEMATICS-1-FW
DEAN-ENGIN-5

Why are we doing this?

Notable Cyber-security Incidents at UC

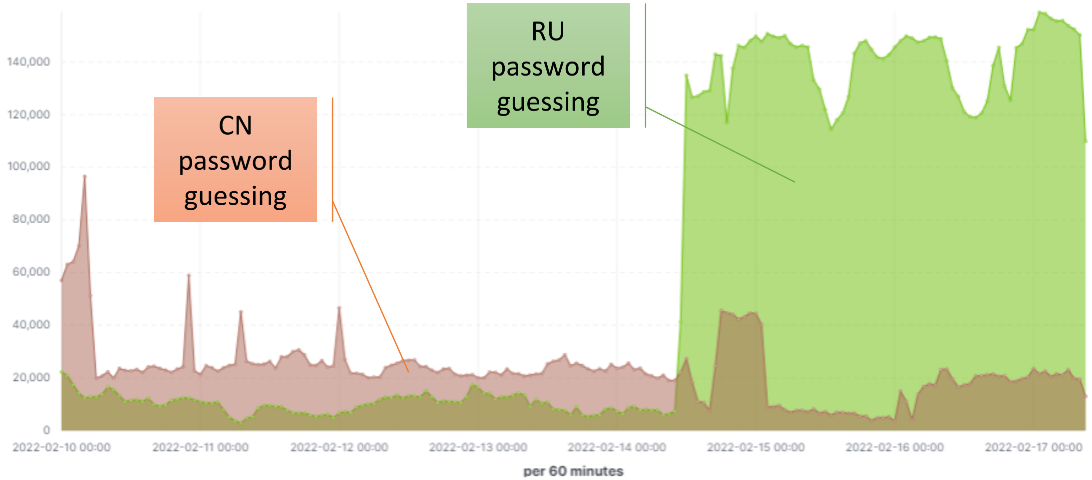
- UCSF Ransomware
  - Affected a large and influential research group (not clinical)
  - All computing resources encrypted and held for ransom
  - UC paid ~$1M for the encryption keys to recover years of research
- UCOP Accellion Breach
  - File transfer service used by the UC Office of the President hacked
  - The software had an unpatched vulnerability
  - Attackers obtained UC personnel private information and threatened release unless a ransom was paid

Ransomware Conditions are Ripe at UC Davis

- Move to remote work has left 100s of UCD systems exposed
- One device breached can lead to widespread compromise
- Installation of malicious “bot” programs remotely trigger widespread ransomware
- Many UCD computers are not managed by IT professionals and have unpatched critical software vulnerabilities.

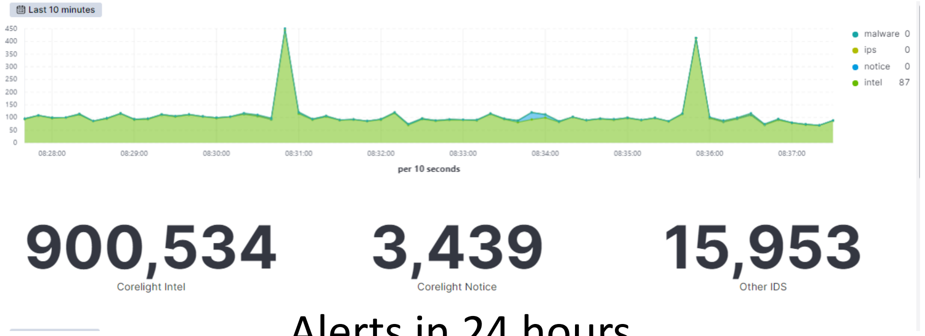
How do we know? Internet traffic behavior.

- Collect network logs at the campus Internet border
- 1B connections per day
- Remote Work Exposure
  - 3.5M failed Remote Desktop connections from RU per day. Matches CISA notice.
  - 0.5M failed secure shell from CN per day
  - They will guess correctly eventually
- Multiple Cyber-intrusion detection systems
- Intrusion attempts
  - ~1M connections per day from known bad sites
  - 20k/day of obvious malicious behavior
- ISO SOC performs ~50 detailed investigations per day



CN password guessing

RU password guessing



900,534
Corelight Intel

3,439
Corelight Notice

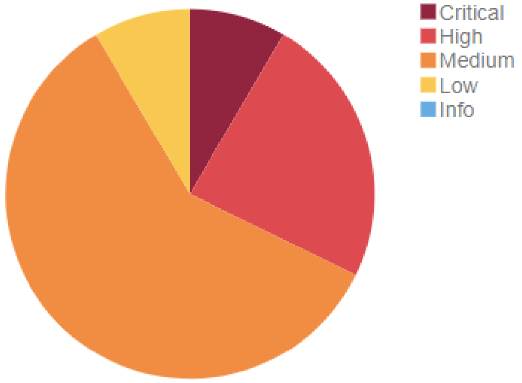
15,953
Other IDS

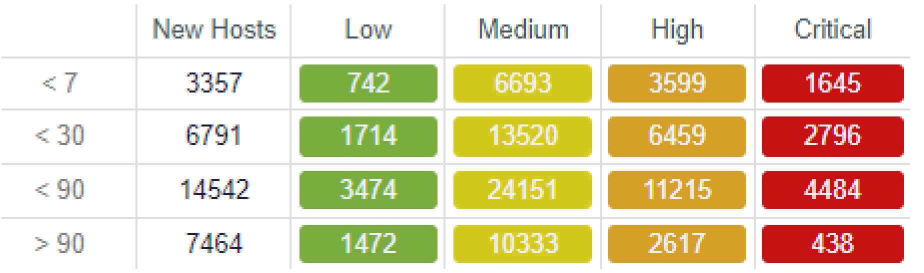
Alerts in 24 hours

UCDAVIS

How do we know? Vulnerability scanning.

- Search the entire campus daily for software vulnerabilities
  - 5000 critical vulnerabilities
  - 12k high
  - 35k medium
- Patching these systems is our highest priority
- New vulnerabilities are announced every day
  - 1/3 of critical vulnerabilities are less than 7 days old
  - Half are less than 30 days old.
  - 10% have been present for more than 3 months.





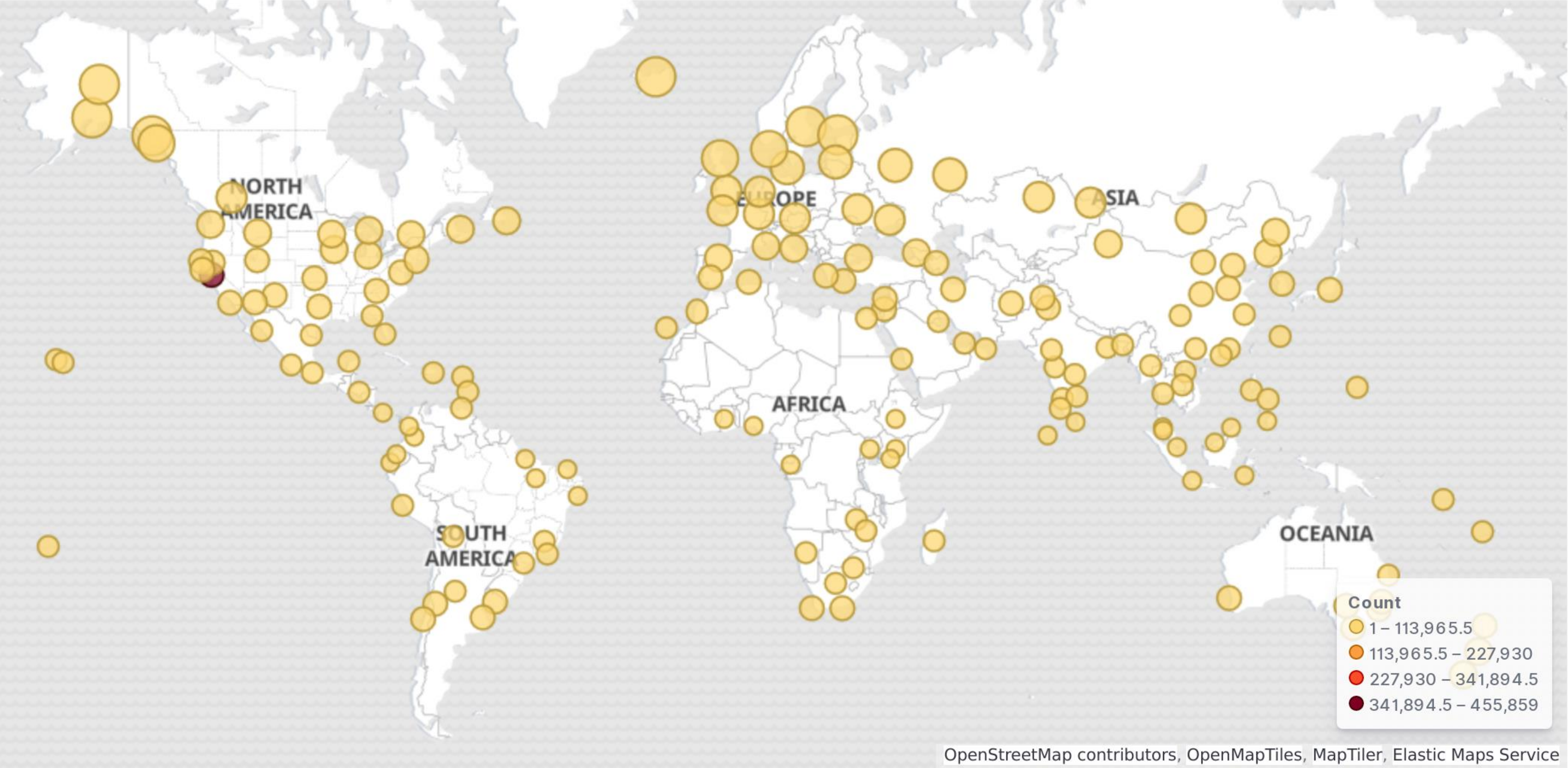
	New Hosts	Low	Medium	High	Critical
< 7	3357	742	6693	3599	1645
< 30	6791	1714	13520	6459	2796
< 90	14542	3474	24151	11215	4484
> 90	7464	1472	10333	2617	438

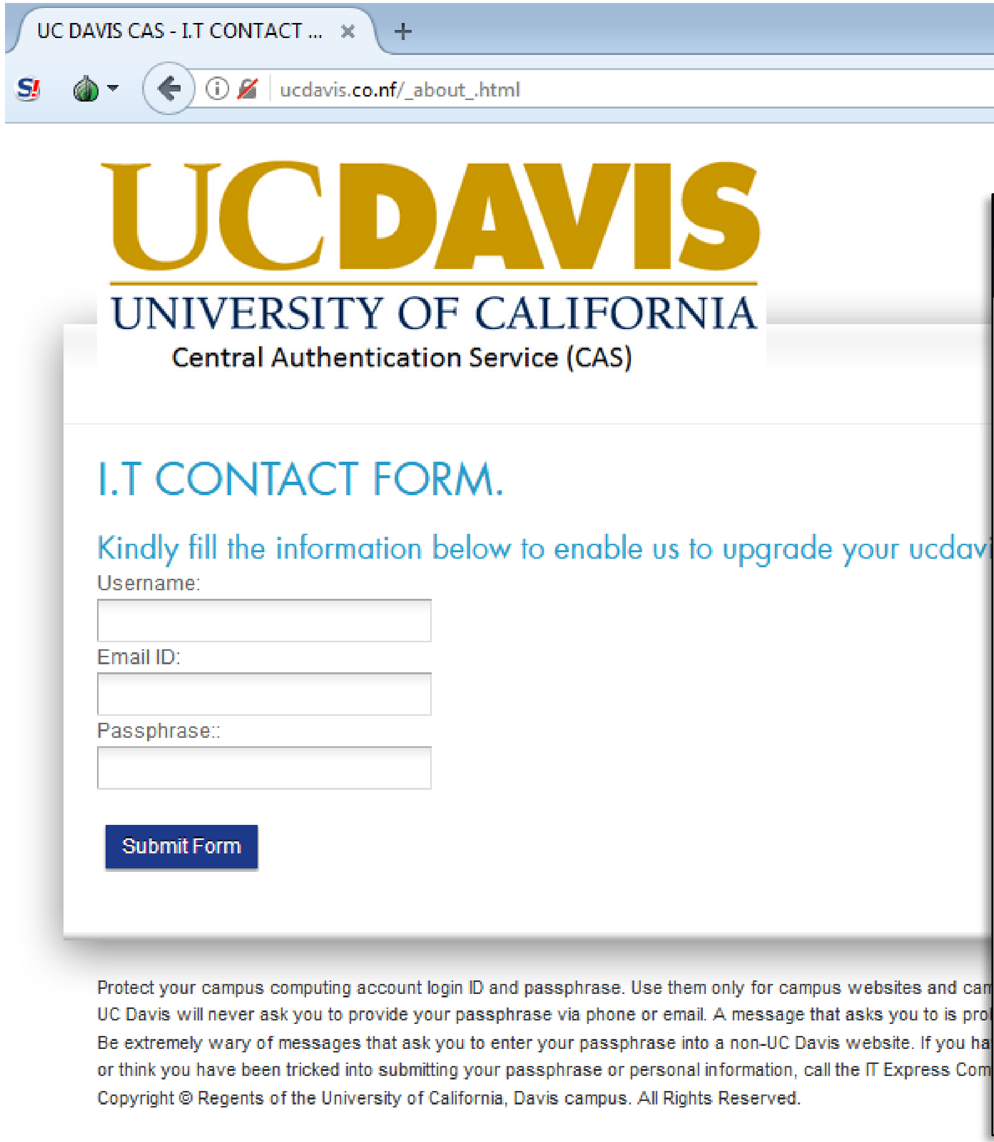
UCDAVIS

UCD Computing Account Security

The UCD SOC’s Eternal Struggle

UCDAVIS


NORTH AMERICA
EUROPE
ASIA
AFRICA
SOUTH AMERICA
OCEANIA
Count
● 1 – 113,965.5
● 113,965.5 – 227,930
● 227,930 – 341,894.5
● 341,894.5 – 455,859
OpenStreetMap contributors, OpenMapTiles, MapTiler, Elastic Maps Service



UCDAVIS
UNIVERSITY OF CALIFORNIA
Central Authentication Service (CAS)

I.T CONTACT FORM.

Kindly fill the information below to enable us to upgrade your ucdavi

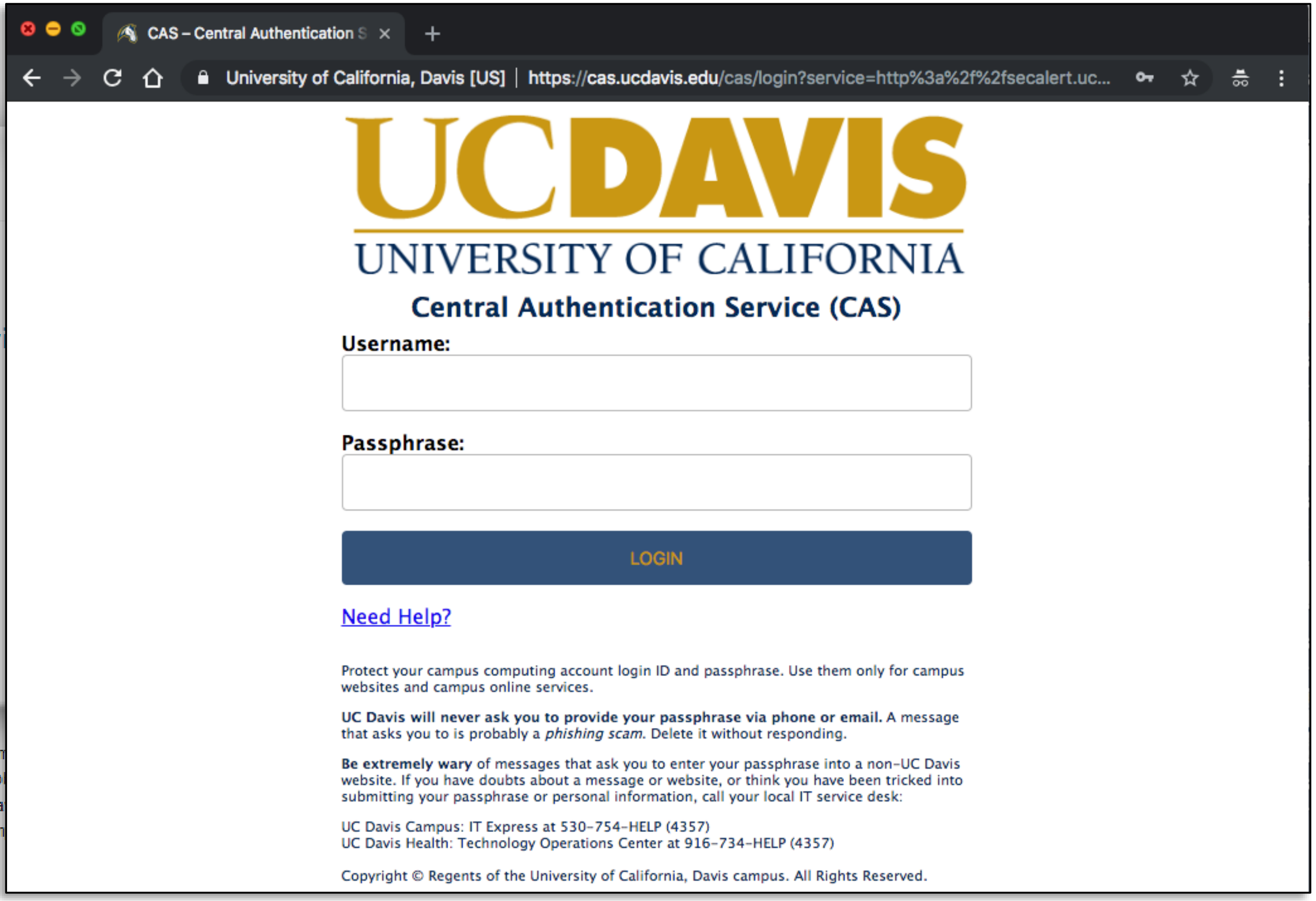
Username:

Email ID:

Passphrase::

Submit Form

Protect your campus computing account login ID and passphrase. Use them only for campus websites and cam
UC Davis will never ask you to provide your passphrase via phone or email. A message that asks you to is pro
Be extremely wary of messages that ask you to enter your passphrase into a non-UC Davis website. If you ha
or think you have been tricked into submitting your passphrase or personal information, call the IT Express Com
Copyright © Regents of the University of California, Davis campus. All Rights Reserved.


CAS – Central Authentication S
University of California, Davis [US]
https://cas.ucdavis.edu/cas/login?service=http%3a%2f%2fsecalert.uc...

UCDAVIS
UNIVERSITY OF CALIFORNIA
Central Authentication Service (CAS)

Username:

Passphrase:

LOGIN

Need Help?

Protect your campus computing account login ID and passphrase. Use them only for campus websites and campus online services.

UC Davis will never ask you to provide your passphrase via phone or email. A message that asks you to is probably a *phishing scam*. Delete it without responding.

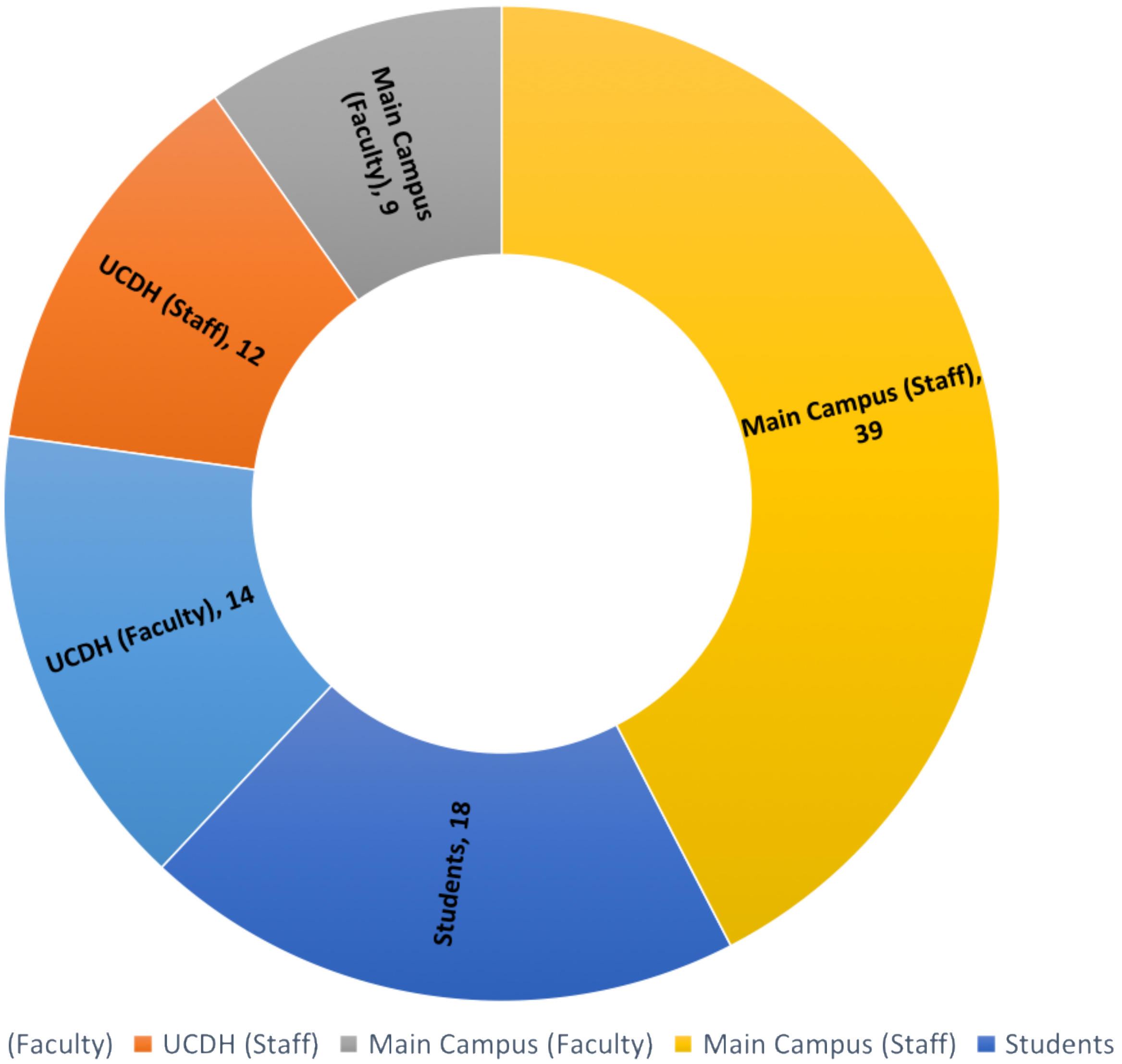
Be extremely wary of messages that ask you to enter your passphrase into a non-UC Davis website. If you have doubts about a message or website, or think you have been tricked into submitting your passphrase or personal information, call your local IT service desk:

UC Davis Campus: IT Express at 530-754-HELP (4357)
UC Davis Health: Technology Operations Center at 916-734-HELP (4357)

Copyright © Regents of the University of California, Davis campus. All Rights Reserved.

```
===================================================
============xX USER ID N PASS Xx======
E-mail ID  : tsjones
Password : Y87n%trsP3*lq+
============xX LOGIN CHECK Xx=====
IP : 105.112.22.2 | SOLID ST+NE : 1:22:40:pm || Thu-05-Apr-2022
===================================================
```

Phished UCD Population Breakdown



UCDAVIS

The Black Axe Hacker Group

- Started as a college fraternity in Nigeria.
- Quasi-religious cult.
- Does not use technically sophisticated computer hacks.
- Very skilled at large scale social-engineering (human deception).
- Rapidly adapt to defensive countermeasures.
- Targets university environments.

https://www.wired.com/story/nigerian-email-scammers-more-effective-than-ever/

Google: “black axe wired”

What can we do? Make UCD a less attractive victim

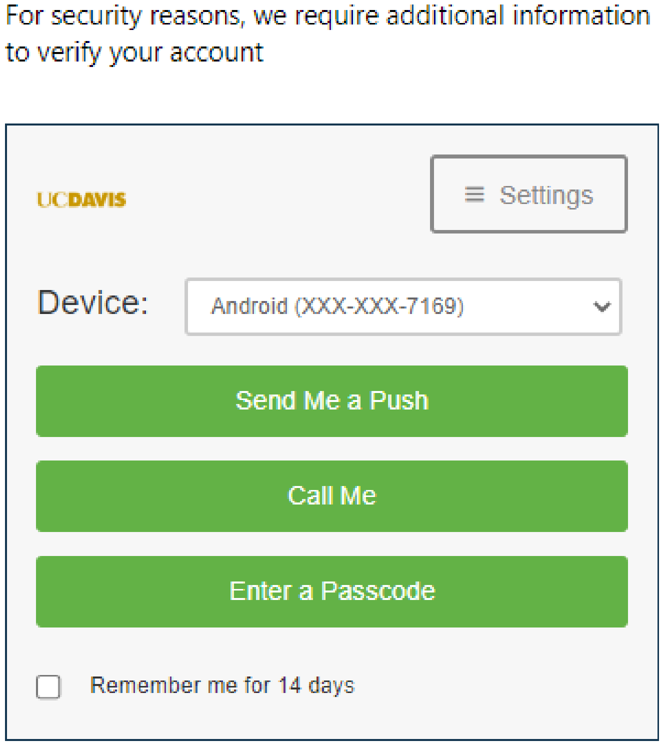
What the ISO SOC is doing.

- Duo MFA everywhere. Even remote access workstations.
- Refine UC Davis specific network threat detection (ML based)
- Reduce blind spots
  1. Gain visibility into lateral movement between workstations/servers
  2. Instrument devices to find malware execution on important systems
  3. Share information with external partners to reveal malicious actors
- Implement Email security 2.0
- Identity-based networking (Net v4)

ISO Top Cyber-security Recommendations

1. Duo MFA Hygiene
   - MFA has been a game changer for UC Davis. Large scale computing account compromise has disappeared
   - Our adversaries react
     - MFA Exhaustion – Send 100's of MFA cellphone push messages. Users accept to silence their phone
     - MFA Mimic – Credential phishing tells users to expect a Duo push even without a request.
   - Make sure that you accept Duo pushes only after you have requested.

Duo cellphone push messages should only follow a send request



For security reasons, we require additional information to verify your account

Device: Android (XXX-XXX-7169)

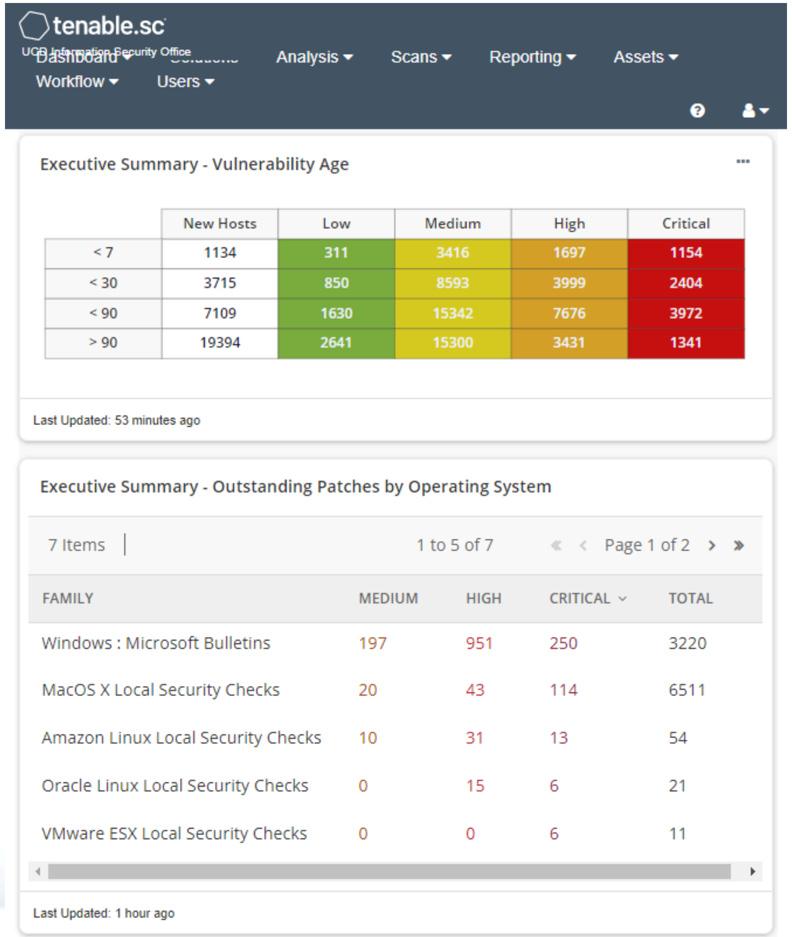
□ Remember me for 14 days

ISO Top Cyber-security Recommendations

ISO SOC scanning shows 1000's of high and critical vulnerabilities on campus greater than 90 days old

2. Don't make it easy – Patch
    - NSA claims that nation state breaches usually exploit 2+ year old vulnerabilities.
    - CISA publishes an actively exploited vulnerability list.

      https://www.cisa.gov/known-exploited-vulnerabilities-catalog
    - The ISO SOC scans for these weekly.
    - 98% cannot be identified by network scanning.
    - Host agent or privileged account scanning is key. The ISO SOC can assist.



Executive Summary - Vulnerability Age

	New Hosts	Low	Medium	High	Critical
< 7	1134	311	3416	1697	1154
< 30	3715	850	8593	3999	2404
< 90	7109	1630	15342	7676	3972
> 90	19394	2641	15300	3431	1341

Last Updated: 53 minutes ago

Executive Summary - Outstanding Patches by Operating System

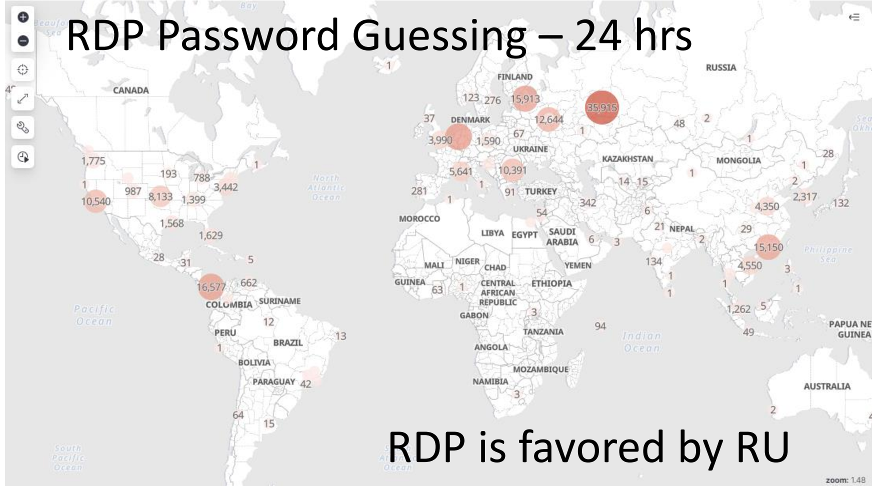
7 Items | 1 to 5 of 7 « ‹ Page 1 of 2 › »

FAMILY	MEDIUM	HIGH	CRITICAL	TOTAL
Windows : Microsoft Bulletins	197	951	250	3220
MacOS X Local Security Checks	20	43	114	6511
Amazon Linux Local Security Checks	10	31	13	54
Oracle Linux Local Security Checks	0	15	6	21
VMware ESX Local Security Checks	0	0	6	11

Last Updated: 1 hour ago

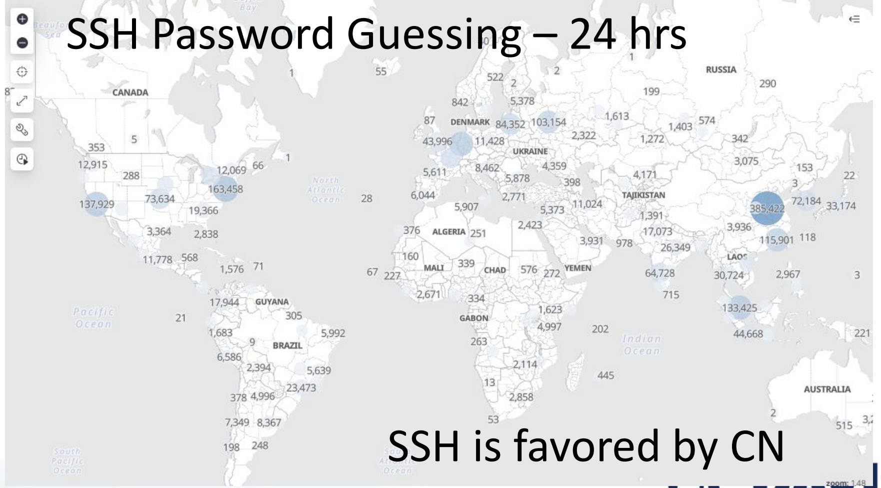
ISO Top Cyber-security Recommendations

3. Protect remote interactive services
   - Large numbers of remote access services were enabled following COVID work-from-home
   - Includes RDP, SSH and VNC (Mac and Linux RDP)
   - Massive password guessing campaigns target these services
   - A single device joined to campus Active Directory exposes all campus accounts.
   - Deny Internet access to these services – use a VPN with Duo MFA



RDP Password Guessing – 24 hrs

RDP is favored by RU



SSH Password Guessing – 24 hrs

SSH is favored by CN

Conclusion

- The UC Davis SOC actively prevents, detects and responds to malicious cyber attacks daily
- Automation is helping the UC Davis SOC cope with the large investigation workload
- The most common (and most serious) breach attempts are non-technical
- The entire UC Davis community must remain vigilant.

Next Steps

- Refine UC Davis specific automated network threat analytics (ML).
- Reduce blind spots
    1. Gain visibility into lateral movement between workstations/servers
    2. Instrument devices to find malware execution on important systems
    3. Share information with external partners to reveal malicious actors
- Implement Email security 2.0
- Identity-based networking (Net v4)

Questions? *<jbrowe@ucdavis.edu>*