Watchers on the Wall

How to Safely Share Content with Wildlings on a Multi-Tenant Platform

SCREENERS.COM
BY SHIFT

SafeStream

Alex Nauda
CTO, SHIFT

Edan Shekar
Senior Security Engineer, SHIFT

Our Realm

Dozens of content owners
- Majors
- Independents
- Service providers and vendors

...forced to cooperate to defend themselves

Screeners application
- Thousands of viewers, mainly press
- Web and Apple TV front ends
- Admin web UI for PR teams to manage it all
- Multi-cloud

Content ripe for piracy
- Many popular shows
- In their final form

Decent Controls

- Passwordless Login
  - No password to compromise
- Visual Watermark
  - Deter against leaks
- Forensic Watermark
  - Track when we need to

Plus...

The Wall

- MFA
- Geofencing
- VPN
- Hardened Devices
- Encryption all over
- Pen Tests
- Appsec Scans
- Vulnerability Management
- Audits
- Code Review
- Training
- Testing

But...

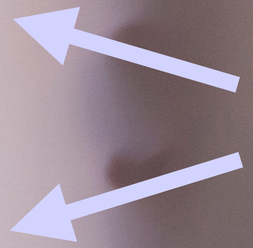
We Must Go Beyond the Wall

Into the haunted forests

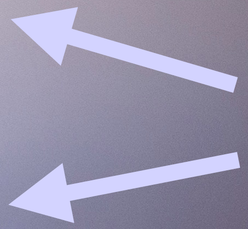
- We have to share content
- On the open internet
- Where pirates are kings
- And everyone gets hacked

Five Threats to Consider

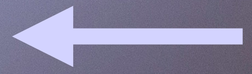
1. Authorized user leaks content
   - Accidentally by over sharing
   - Accidentally through carelessness
   - On purpose by screencapping
2. Attacker compromises authorized user
   - Probably phishes their email
3. Attacker breaks into application
   - May be an authorized user or not
4. Attacker breaks into infrastructure
5. Social engineering / inside job



User Credentials



Break-ins



Employee Credentials

Watchers on the Wall

Monitoring as a general purpose compensating control

Flexible

- Can be applied to many threat models

Can start small

- Build up to more sophistication

Includes humans

- Leverages our paranoia and judgment

Good toolsets available

Example 1

Anomalous Activity Monitoring

Addresses authorized users' use of our systems

User Credentials

Inputs:

- Client side UI tracking
- Server side request tracking
  - Authentication
  - Playback
- Video QoS tracking data

Example 1 - Anomalous Activity Monitoring

- Analyze typical user activity

- Set threshold alerts
  - Number of locations
  - Number of devices
  - Number of views per time period
  - etc.

- Investigate alarms using an SOP
  - But also your brain

- Correlate with session tracking and replay tools

- Spot check on an ongoing basis

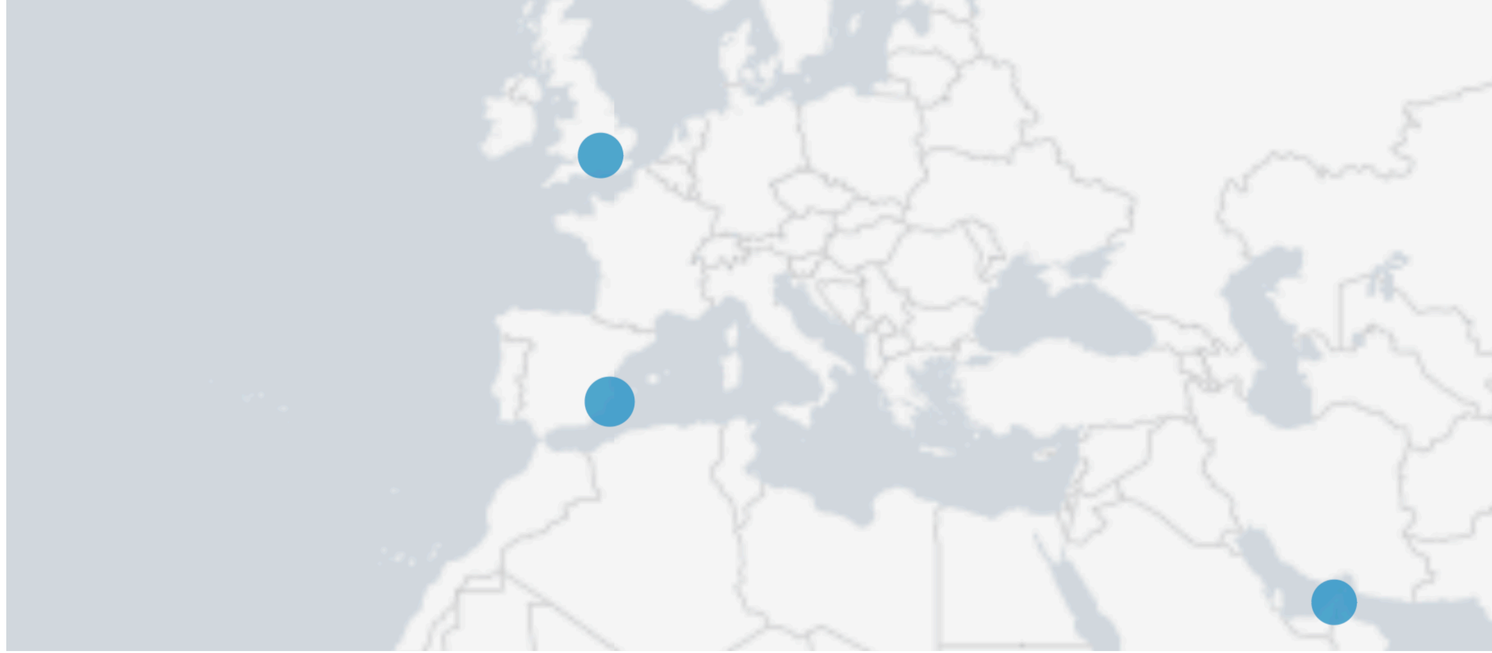
Example 1 - Anomalous Activity Monitoring

Alert: Users exceeding location threshold (Real time)

EmailRequestingLink	ContentProvider	NumberOfLinksRequested
[redacted]@[redacted].com	[redacted]	4
[redacted].com		5
[redacted].com		4
[redacted]om		5
[redacted]@gmail.com		4
[redacted].com		4
[redacted]@gmail.com		4
[redacted].com		4

strf_time	stall_span_minutes	watermarked_by_email	ip_address	ip_user_type	City	Region	Country	video_id	total_noticable_stalls	total_delay_seconds	delay_rate
07-23-2018 3:49 PM	15.5235	tr[redacted]@gmail.com	[redacted].189	college	Baltimore	Maryland	United States	bfb160ed-263f-4964-8089-ccd52a1d2c25	25	126.187	0.135480
07-23-2018 3:56 AM	3.11368	ro[redacted]@latimes.com	[redacted].35	residential	Los Angeles	California	United States	0946c39e-5926-4895-9bf0-0af35ee4bf0e	2	1.567	0.008388
07-23-2018 4:45 PM	0.000	[redacted]film@gmail.com	[redacted].5	residential	Southbridge	Massachusetts	United States	c5baf7c1-5dfb-482b-827b-d11cc37a9b35	1	1.227	
07-23-2018 5:13 AM	21.82228	[redacted]@tangmp.com	[redacted].6	residential	Los Angeles	California	United States	04b13bc2-9b37-4423-b5b5-36db2d8358d3	26	160.544	0.122615
07-23-2018 5:24 PM	0.000	le[redacted]@gmail.com	[redacted].218	residential	Elmhurst	New York	United States	927a38ec-39fc-41c8-bfb8-8022125c75db	1	2.088	
07-23-2018 5:39 PM	0.000	so[redacted]@condenast.com	[redacted].113	residential	Stamford	Connecticut	United States	bfb160ed-263f-4964-8089-ccd52a1d2c25	1	0.593	
07-23-2018 5:41 PM	46.64187	si[redacted]@sky.de	[redacted].19	residential	Munich	Bavaria	Germany	31007afc-efd3-4598-bfb4-82375363f3b2	8	52.557	0.018780
07-23-2018 5:59 PM	16.84778	w[redacted]@gmail.com	[redacted].130	residential	London	Ontario	Canada	2f41d8ec-f723-42dd-b809-0e59b9d3401a	2	17.916	0.017723

Example 1 - Anomalous Activity Monitoring



Activity Reviewed:

USER: [redacted]@[redacted].com

Previous observations:

First request for magic link sent 11/12/2018. No content viewed until 11/16/2018. User is a top viewer. User has records of viewing from 2 devices in tandem, one on a cellular network. 3 IPs, 3 devices, 2 regions.

Current observations:

No new activity from this user since initial observation. User will remain flagged for further observation.

>>>Flagged for further observation.

Example 1 - Anomalous Activity Monitoring

Results

- Be vigilant
- We do find suspicious activity
- Some activity is legit but looks very suspicious
  - Certain VPNs
  - Client machines in public cloud
- Requires constant improvement

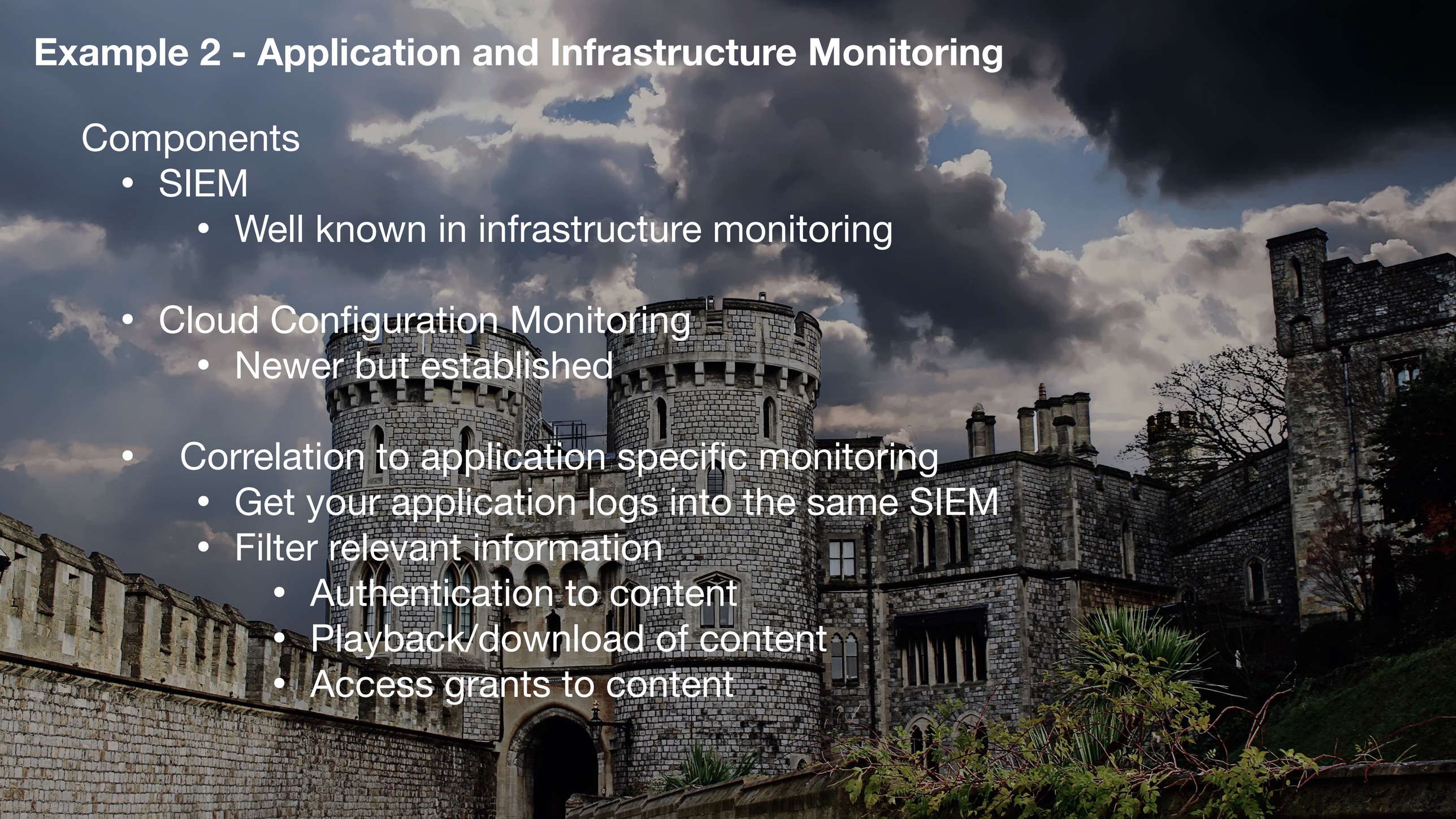
Example 2

Application and Infrastructure Monitoring

Addresses attempts at unauthorized access to our systems

Break-ins

Example 2 - Application and Infrastructure Monitoring



Components

- SIEM
  - Well known in infrastructure monitoring
- Cloud Configuration Monitoring
  - Newer but established
- Correlation to application specific monitoring
  - Get your application logs into the same SIEM
  - Filter relevant information
    - Authentication to content
    - Playback/download of content
    - Access grants to content

Example 2 - Application and Infrastructure Monitoring

Overview

LIVE MODE [From Panel]

Activity by Source Location

Last 30 Days

Total Login Failures

Last 30 Days

138

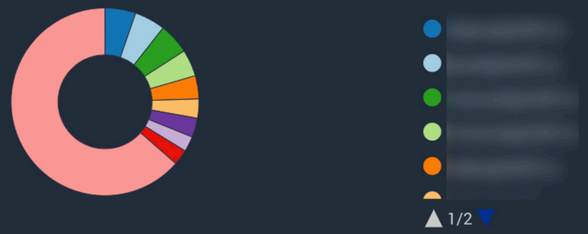
Top Login Failure Reasons

Last 30 Days

#	eventName	login_failure_type	login_type	eventCount
1	login_verification	passed		130
2	login_challenge	passed		5
3	login_verification	incorrect_answer_entered		3

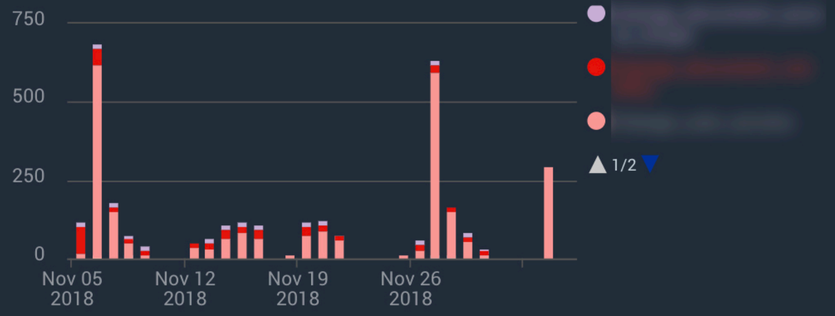
Logins from Multiple IPs

Last 30 Days



ACL Changes

Last 30 Days



Login Failures by User

Last 30 Days

Logins from Multiple IPs

Last 30 Days

#	email	DistinctIPs	LoginCount
1		8	69

Top Event Name by Event Type

Last 30 Days

#	eventType	eventName	eventCount	_rank
1	DOMAIN_SETTINGS		1	1

Top Apps

Last 30 Days

Example 2 - Application and Infrastructure Monitoring

Amazon GuardDuty - Overview

LIVE MODE | Last 30 Days

Guard Duty Threat Map

Last 30 Days

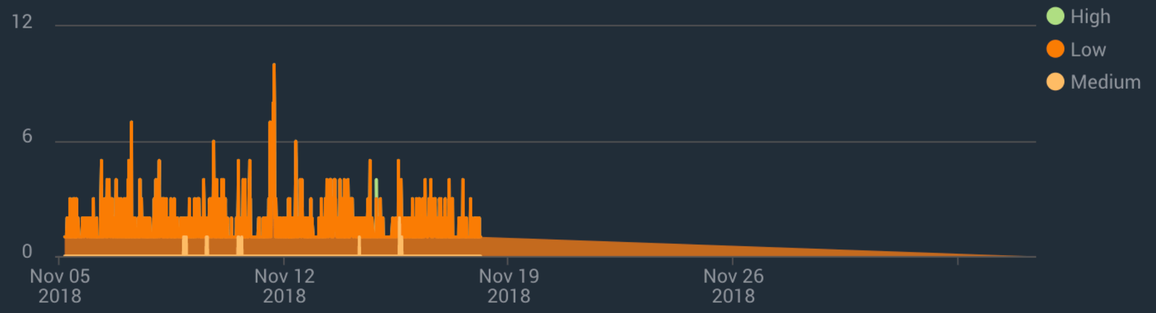
High Severity Threats Table

Last 30 Days

#	Time	accountID	region	ResourceType	description	link
1	12/03/2018 10:57:00 AM -0500		us-east-1	EC2		https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:search=i-
2	11/14/2018 9:35:00 PM -0500		us-east-1	EC2		https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:search=i-
3	11/14/2018 9:11:00 PM -0500		us-east-1	EC2		https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:search=i-
4	11/14/2018 8:45:00 PM -0500		us-east-1	EC2		https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:search=i-

Severity Trend

Last 30 Days



Threats by ThreatPurpose, ResourceType, ThreatName

Last 30 Days

#	ThreatPurpose	ResourceType	ThreatName	count
1	Recon	EC2	PortProbeUnprotectedPort	3,785
2	UnauthorizedAccess	EC2	SSHBruteForce	43
3	UnauthorizedAccess	IAMUser	UnusualASNCaller	33
4	Behavior	EC2	NetworkPortUnusual	5
5	Trojan	EC2	DNSDataExfiltration	4
6	Recon	EC2	Portscan	1

Threats by IP

Last 30 Days

Severity and AccountID

Last 30 Days

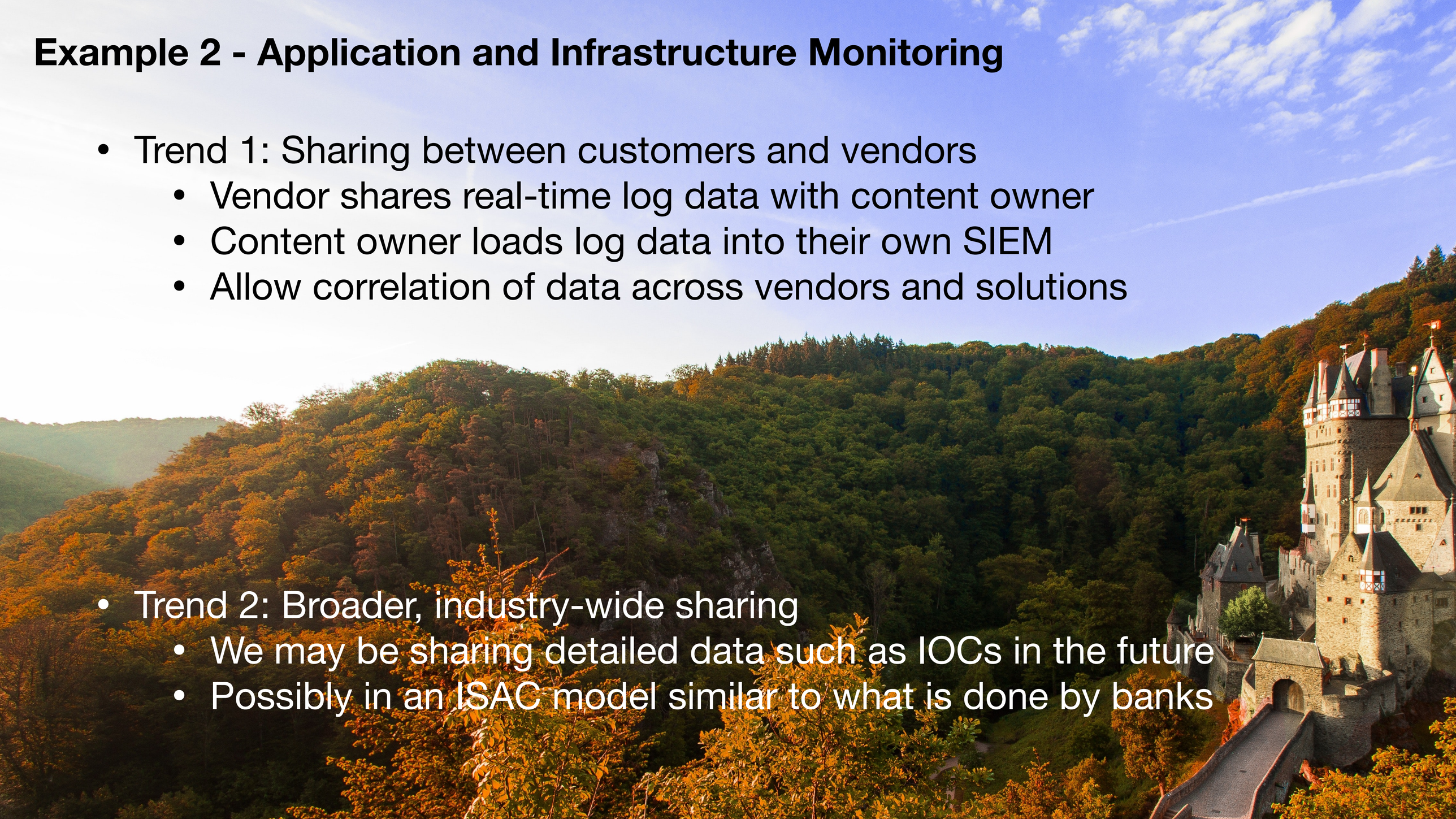
Severity and Region

Last 30 Days

Severity and ResourceType

Example 2 - Application and Infrastructure Monitoring

- Trend 1: Sharing between customers and vendors
  - Vendor shares real-time log data with content owner
  - Content owner loads log data into their own SIEM
  - Allow correlation of data across vendors and solutions



- Trend 2: Broader, industry-wide sharing
  - We may be sharing detailed data such as IOCs in the future
  - Possibly in an ISAC model similar to what is done by banks

Example 3

Controlling Internal Use

Addresses employees' use of our systems

Employee Credentials

Example threats

- Compromised endpoint (malware)
- Compromised employee credentials

Challenge -
Provide enterprise grade security, operating as a small company who is a vendor to large enterprises

Example 3 - Controlling Internal Use

Simplify - Settle on one simple, trainable tool for each control

- Password vault with sharing
- Identity Management
- SSO authentication
- VPN
- Patch management
- Anti-malware

Tiered privilege requires tiered controls

- Privileged access users get more controls
  - Deeper background checks and competence vetting
  - More frequent endpoint scans
  - Higher severity alerts in the case of any anomaly
  - Retraining right away when it changes

Example 3 - Controlling Internal Use

Details | Refresh details | Edit details

Name: alex_nauda-mbp13
Model: MacBook Pro
Serial: [redacted]
Warranty: Apple
Tags: BOS OWN
Auto tags: Mac devices
Owner: Set an owner

SM Agent

Up to date: Yes

OS

Version: OS X 10.14
Uptime: 23h 33m 55s
Last user: -

Security

Encryption: Enabled
-
Firewall: -
Login required: Yes
Auto login: Disabled
Screen lock: Enabled
Screen lock delay: 9 minutes
Security policies: filevault | login_req | firewall | jumpcloud

Management

Settings: up-to-date
Enrollment date: 12:58 Jun 20 2017

Storage

/dev/disk1s1:	143.4 GB / 931.5 GB	15%
/dev/disk1s2:	67.1 MB / 931.5 GB	0%
/dev/disk1s4:	3.0 GB / 931.5 GB	0%

Network

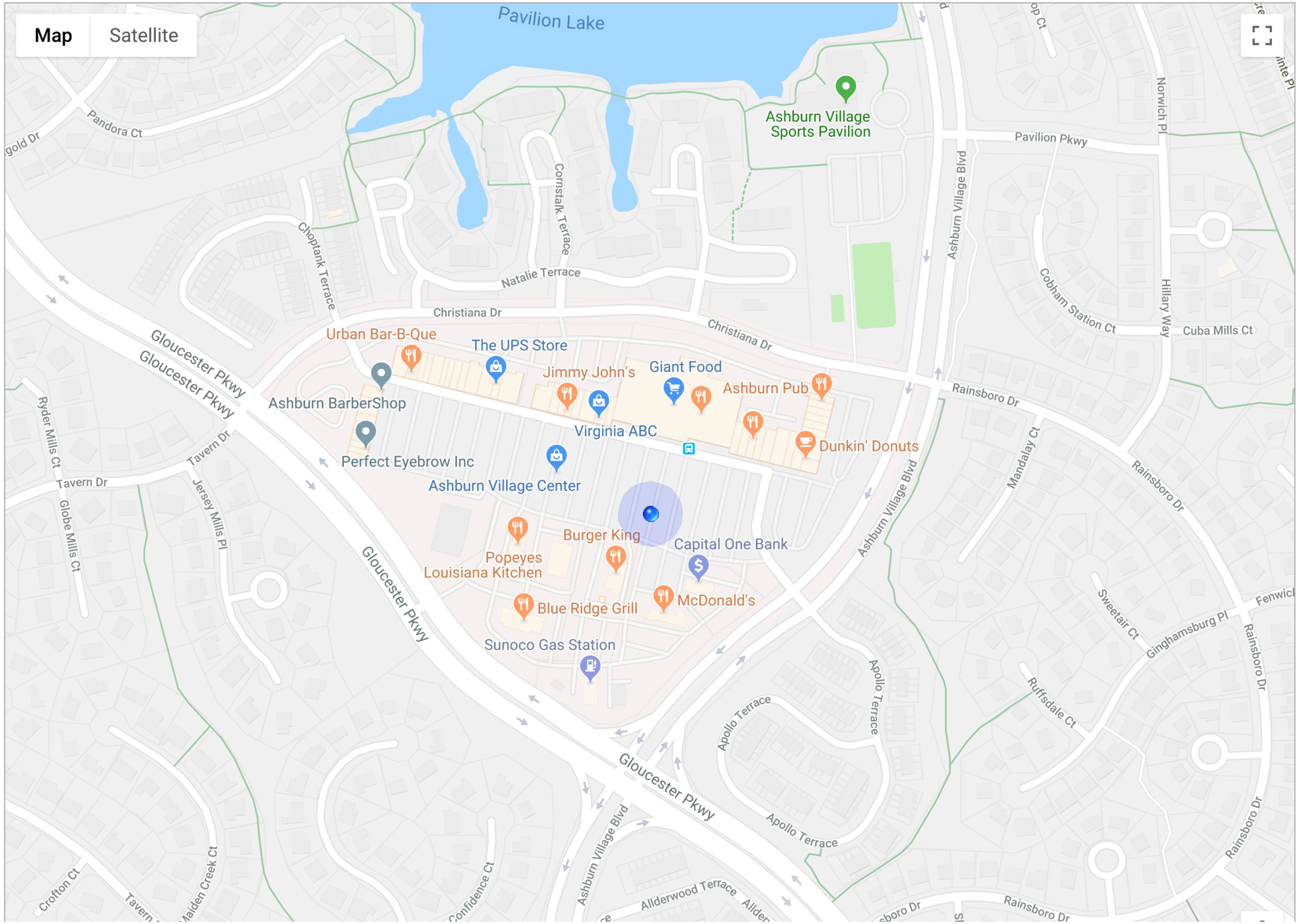
LAN IP: [redacted]
Public IP: [redacted]
Wireless adapter: Airport Extreme
Bluetooth MAC: [redacted]

Online status | ▶ Check-in now

Agent last online: Dec 04 2018 14:50

Approximate location | Refresh location

Ashburn, VA (via IP, updated about 3 hours ago)



Example 3 - Controlling Internal Use

Dashboard | Analysis | Outbreak Control | Management | Accounts | Search

Dashboard

Compromise Events (Default) | Reset | New Filter

Dashboard | Inbox | Overview | Events

Time Period | 14 days | Refresh All | Auto-Refresh

0% compromised

Inbox Status

0 Require Attention | 0 In Progress | 0 Resolved

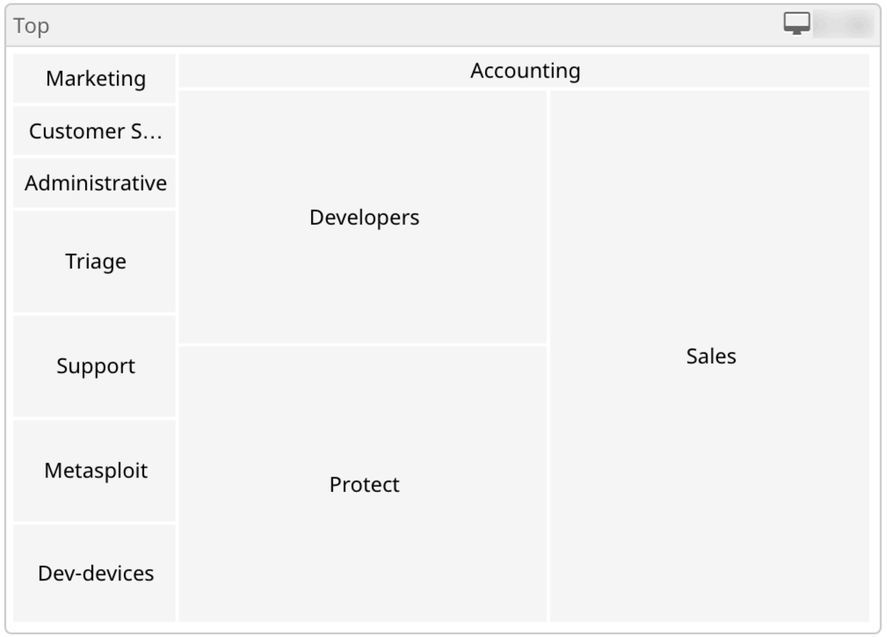
Cognitive Threat Analytics

unresolved threats
0

Compromises

Inbox

Top

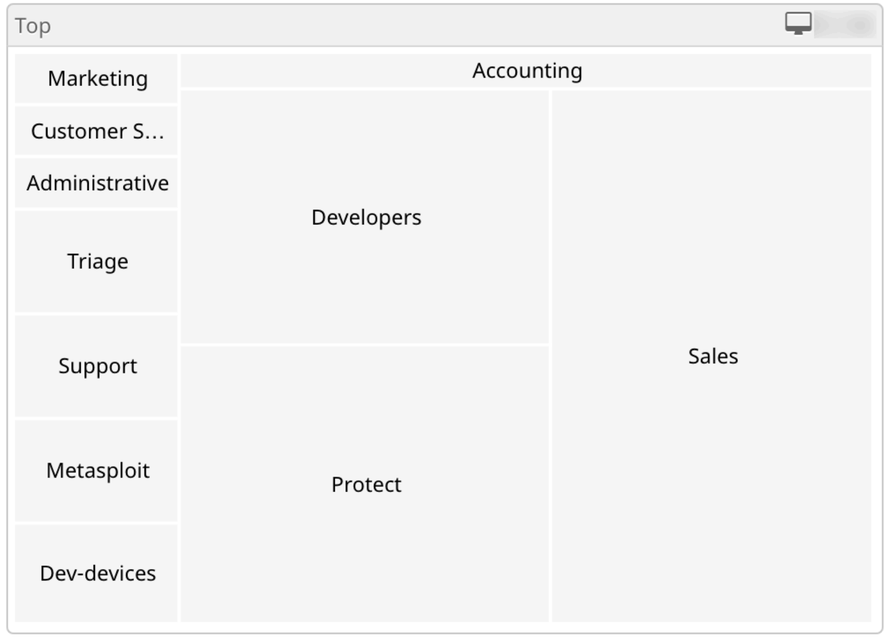


20 21 22 23 24 25 26 27 28 29 30 1 2 3 4
NOV DEC

Quarantined Detections

Quarantine Events

Top



20 21 22 23 24 25 26 27 28 29 30 1 2 3 4
NOV DEC

Vulnerabilities

View

Top

Threat Grid Analysis

0 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

2.26 Million Files Scanned
40.2 Thousand Network Connections Logged

Connectors

Example 3 - Controlling Internal Use

Trends

- Good security with less impedance
  - Hardware MFA (e.g. YubiKey) and/or biometrics (e.g. TouchID)
  - GCP Identity Aware Proxy as a potential alternative to VPN

- New techniques become available every 6 months or so
  - Keep up with the news
  - Evaluate techniques as they emerge and are adopted
  - If something works, implement it fast

Thank You

Questions?

Thank you to the photoghraphers who made their work available under permissive licenses for uses like this presentation

Simon Matzinger
Pedro Figueras
Jordan Stimpson
Tim Mossholder
PhotoMIX Ltd.

Tom Swinnen
Eberhard Grossgasteiger
Luka Siemiopnov
werner22brigitte
TheDigitalArtist

Pascal Trichter
Mali Maeder
Manfred Richer
fbhk
myeviajes

SHIFT