GUARDIAN

TECHNOLOGIES

AGENDA

- Team Member Introductions
- Scenario
- Suggestion
- Demo's
- Q&A

Michael Roberts

- Cybersecurity Professional/Air Force Veteran.
- In senior year pursuing Bachelors in Computer Science. Committed to continuous learning.
- Skilled in Automation using tools such as Bash, Powershell, Python.
- Experience supervising others in aircraft troubleshooting of F-16's

GUARDIAN

TECHNOLOGIES

Christen Reinhart

Ready to embark on a mission-driven career in cybersecurity fueled by a profound commitment to safeguarding the integrity, security, and efficiency of vital IT systems. With over a decade of experience, I've honed a versatile skill set and gained significant expertise spanning system administration, network management, satellite communications, and cybersecurity.

GUARDIAN

TECHNOLOGIES

Thierry Tran

- US Army Veteran
- Pursuing B.S. in Computer Science at SNHU, proficient in Python, Java, C++, MQL and SQL.
- Inspired by a friend's success in Cybersecurity, enrolled in Code Fellow to specialize in the field
- Hobbies include soccer, watching movies, and traveling

GUARDIAN

TECHNOLOGIES

Edwin Pretel

- Army veteran, with a lifelong passion for technology, transitioned from industrial painting to excelling in tech troubleshooting at call centers during COVID.
- Motivated by an IT specialist advice, pursued further education in IT, now focusing on certification.
- Combines disciplined military work ethic with hands-on tech problem-solving skills, aiming for a career in IT.

SCENARIO

Client Overview:

- Guardian Technologies, a cybersecurity leader, focuses on fortifying digital defenses and ensuring organizational resilience against cyber threats.
- Our mission is to empower businesses with innovative solutions, maintaining the highest cybersecurity standards.

Key Focus:

Guardian Technologies emphasizes proactive security measures, innovation, and maintaining the highest cybersecurity standards to safeguard digital assets.

Project Objectives:

- Threat Model: Create a comprehensive DFD for AWS threat identification and prioritized defense.
- Enhanced Detection: Deploy tools like Splunk and Zeek for increased visibility in AWS.
- IDS Rules: Fine-tune IDS rules to detect suspicious network traffic effectively.
- Detective Controls: Implement controls on the web server for monitoring and preventing unauthorized access.

Specific Goals:

- Develop a comprehensive threat model DFD and perform a STRIDE analysis for AWS vulnerabilities.
- Deploy additional threat detection tools to enhance visibility across the environment.
- Configure IDS rules and implement detective controls to improve AWS infrastructure defense.
- Actively observe and document adversarial actions, collecting evidence to understand adversary tactics.
- Develop scripted automation for proactive detection and alerts on adversarial activity.

Guardian Technologies

GUARDIAN

TECHNOLOGIES

DEMO - Splunk

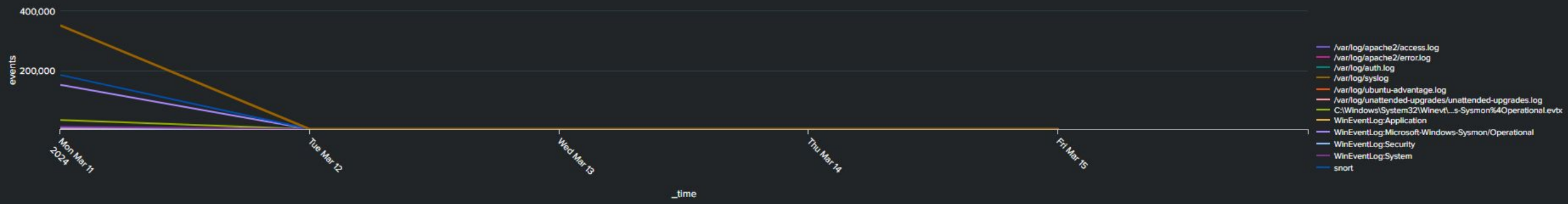
Mon-Fri Traffic on AWS

Edit Export ▾ ...

This is a collection of events and traffic generated by all instances on AWS compiled into readable graphs.

Sources Accessed from Mar 11th - Mar 15th

All sources



Sysmon Activity from Different Hosts

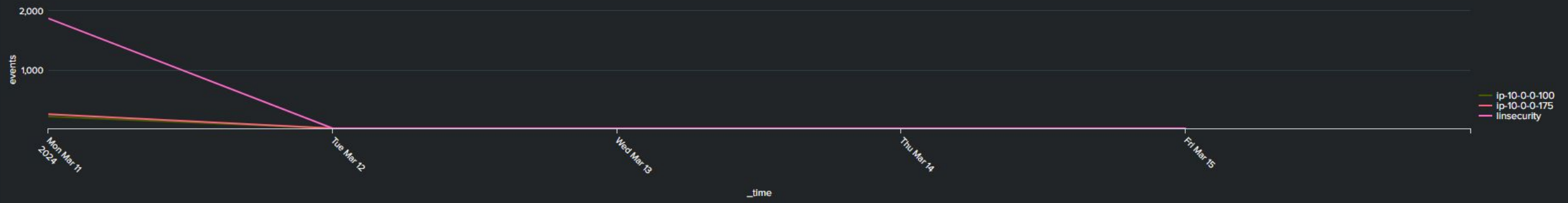
Different Hosts

/var/log/auth.log activity

Linux Login Activity: Hosts per event

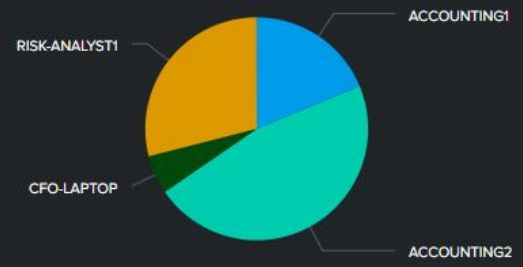
/var/log/auth.log activity

Linux Login Activity: Hosts per event



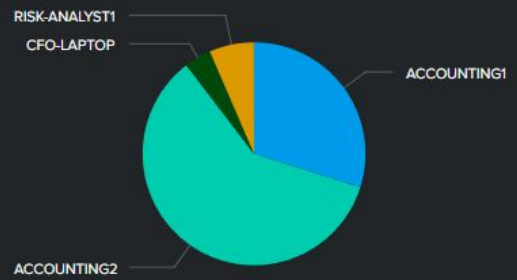
Windows Security Event Code: 4624

Successful Logins to Windows Machines/Host



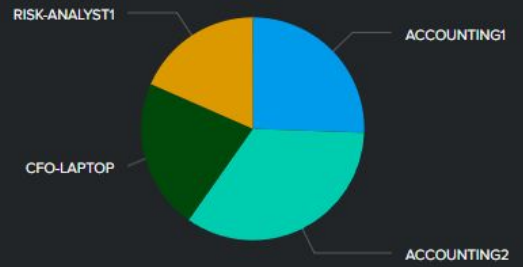
Windows Security Event Code: 4625

Failed Logins to Windows Machines/Host



Windows Security Event Code: 4672

Attempted Login to Administrator Equivalent User Account



Windows Security Event Code: 5379

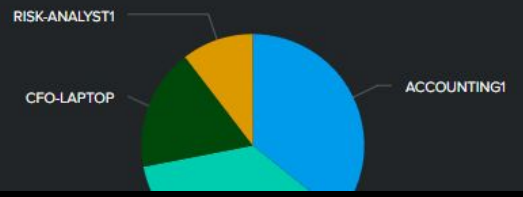
Someone is trying to read credentials in WCM

Microsoft Windows Sysmon Event Code: 22

DNS query was performed on machine

Windows System Events

Windows Machines System Event Log Activity/Host. click to refine search.

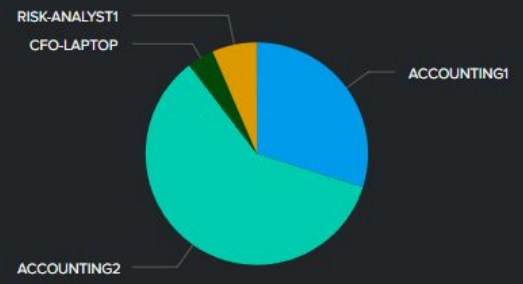


Windows Security Event Code: 4624

Successful Logins to Windows Machines/Host

Windows Security Event Code: 4625

Failed Logins to Windows Machines/Host

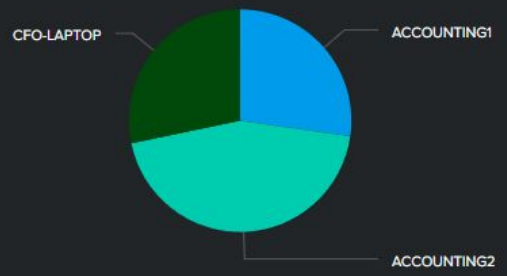


Windows Security Event Code: 4672

Attempted Login to Administrator Equivalent User Account

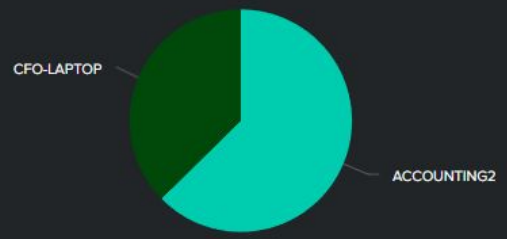
Windows Security Event Code: 5379

Someone is trying to read credentials in WCM



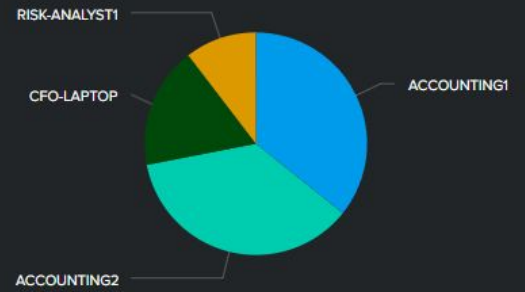
Microsoft Windows Sysmon Event Code: 22

DNS query was performed on machine



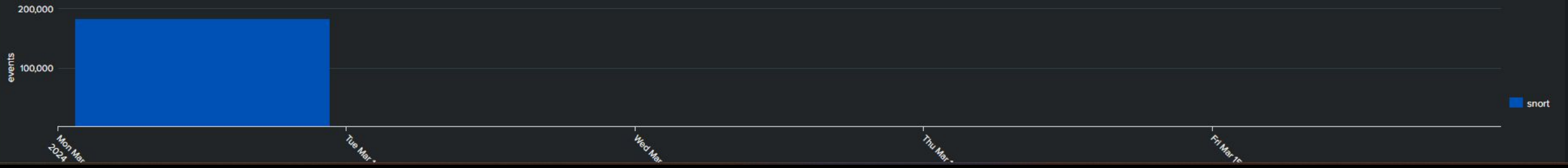
Windows System Events

Windows Machines System Event Log Activity/Host. click to refine search.



Snort Traffic

Capturing all traffic from every instance. click to refine search for strings

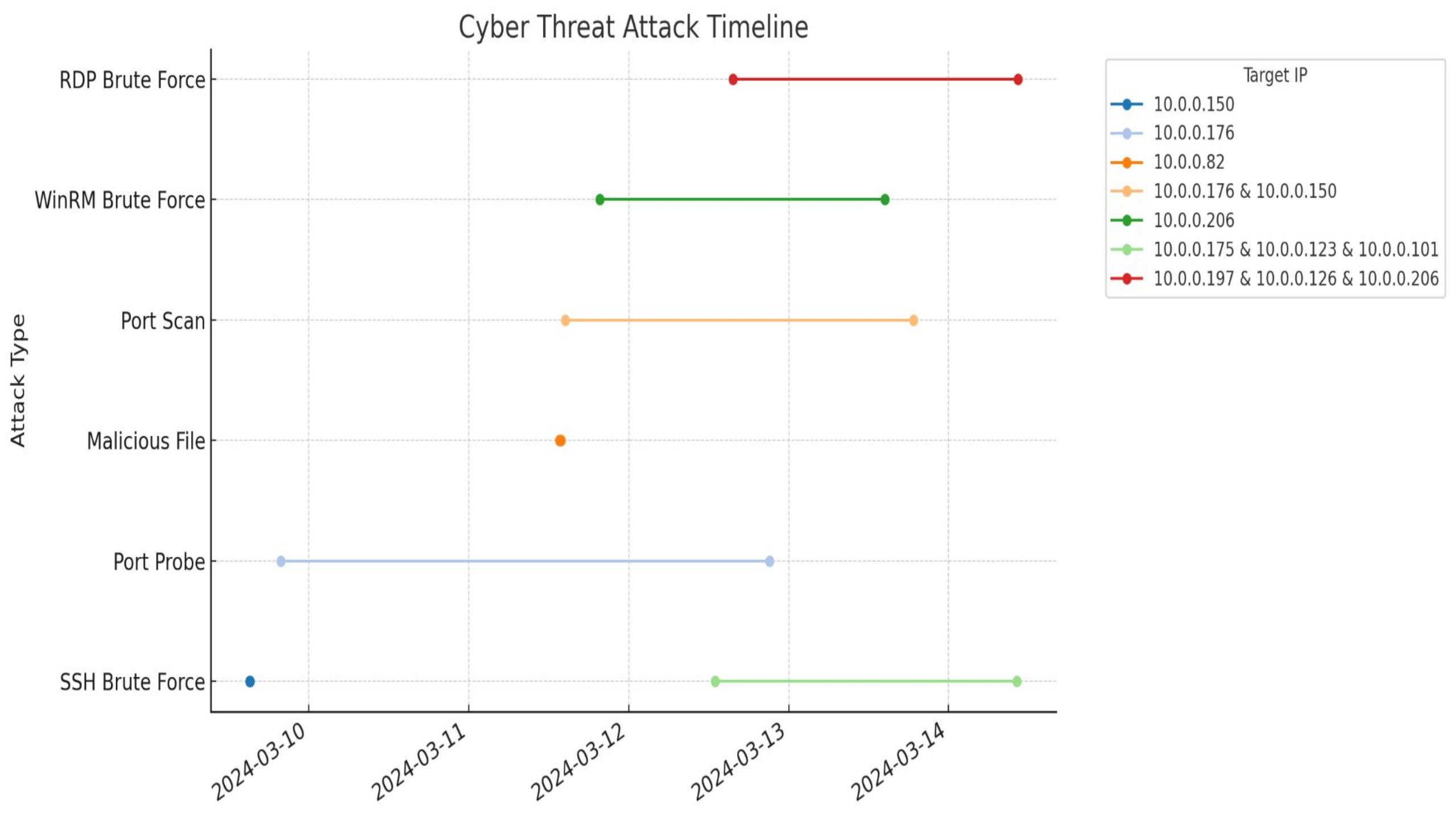


i	Time	Event
>	3/12/24 5:39:01.000 PM	Mar 12 17:39:01 ip-10-0-0-175 CRON[36620]: pam_unix(cron:session): session opened for user root by (uid=0) host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:20.000 PM	Mar 12 17:38:20 ip-10-0-0-175 sshd[36611]: Connection closed by invalid user people1 10.0.0.176 port 52190 [preauth] host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:20.000 PM	Mar 12 17:38:20 ip-10-0-0-175 sshd[36605]: Connection closed by invalid user 123456s 10.0.0.176 port 52176 [preauth] host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:20.000 PM	Mar 12 17:38:20 ip-10-0-0-175 sshd[36610]: Connection closed by invalid user pollita 10.0.0.176 port 52186 [preauth] host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:20.000 PM	Mar 12 17:38:20 ip-10-0-0-175 sshd[36600]: Connection closed by invalid user jonny 10.0.0.176 port 52150 [preauth] host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:19.000 PM	Mar 12 17:38:19 ip-10-0-0-175 sshd[36602]: Connection closed by invalid user allyson 10.0.0.176 port 52166 [preauth] host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:19.000 PM	Mar 12 17:38:19 ip-10-0-0-175 sshd[36598]: Connection closed by invalid user miguel1 10.0.0.176 port 52120 [preauth] host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:19.000 PM	Mar 12 17:38:19 ip-10-0-0-175 sshd[36604]: Connection closed by invalid user 1blood 10.0.0.176 port 52168 [preauth] host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:19.000 PM	Mar 12 17:38:19 ip-10-0-0-175 sshd[36610]: Failed password for invalid user pollita from 10.0.0.176 port 52186 ssh2 host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:19.000 PM	Mar 12 17:38:19 ip-10-0-0-175 sshd[36611]: Failed password for invalid user people1 from 10.0.0.176 port 52190 ssh2 host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:19.000 PM	Mar 12 17:38:19 ip-10-0-0-175 sshd[36608]: Connection closed by invalid user sexy01 10.0.0.176 port 52184 [preauth] host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:18.000 PM	Mar 12 17:38:18 ip-10-0-0-175 sshd[36608]: Failed password for invalid user sexy01 from 10.0.0.176 port 52184 ssh2 host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:18.000 PM	Mar 12 17:38:18 ip-10-0-0-175 sshd[36604]: Failed password for invalid user 1blood from 10.0.0.176 port 52168 ssh2 host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24 5:38:18.000 PM	Mar 12 17:38:18 ip-10-0-0-175 sshd[36605]: Failed password for invalid user 123456s from 10.0.0.176 port 52176 ssh2 host = ip-10-0-0-175 source = /var/log/auth.log sourcetype = auth-too_small
>	3/12/24	Mar 12 17:38:18 ip-10-0-0-175 sshd[36602]: Failed password for invalid user allyson from 10.0.0.176 port 52166 ssh2

DEMO - GuardDuty

DEMO - Lambda

DEMO - Incident Response Report


Cyber Threat Attack Timeline
Attack Type
RDP Brute Force
WinRM Brute Force
Port Scan
Malicious File
Port Probe
SSH Brute Force
2024-03-10
2024-03-11
2024-03-12
2024-03-13
2024-03-14
Target IP
10.0.0.150
10.0.0.176
10.0.0.82
10.0.0.176 & 10.0.0.150
10.0.0.206
10.0.0.175 & 10.0.0.123 & 10.0.0.101
10.0.0.197 & 10.0.0.126 & 10.0.0.206

SOLUTIONS

Threat Model Development

Collaborate on constructing a comprehensive DFD to identify attack vectors and prioritize defensive measures.

Enhanced Threat Detection

Deploy additional tools (Splunk and Zeek) to boost visibility across the AWS environment.

Configuration of IDS Rules

Fine-tune IDS rules for an improved defensive posture, with a focus on detecting suspicious network traffic.

Implementation of Detective Controls

Implement controls on the web server hosting SimCorp's application to monitor and prevent unauthorized access.

Adversarial Activity Observation

Actively observe adversarial actions, collecting evidence of scanning, TTPs, and IOCs for informed defensive strategies.

Thank You!

Guardian Technologies
Marco Vazquez
Roger Huba
TAs
Colleagues in cohort

Guardian Technologies Github


QUESTIONS ?