STAGE 1: SANS 20 Framework Overview

The 20 critical security controls include the following:

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Cyber attackers will typically scan address spaces waiting for new and unprotected IT assets to be added to the system. The first control encourages companies to use an inventory discovery tool to automatically log and track all devices that exist in the company's IT infrastructure.

Use of AI:

- AI can assist in automatically discovering and tracking hardware assets by analyzing network traffic, logs, and device fingerprints

Business Impact:

- Ensures that all hardware assets are known and managed, reducing the risk of unauthorized devices accessing the network. This control helps in preventing potential security breaches and maintaining the integrity of the IT infrastructure.

Critical Control 2: Inventory of Authorized and Unauthorized Software

SANS encourages companies to include authorized and unauthorized software in their IT asset inventory database. Most cyber-attacks are carried out using a combination of social engineering, phishing emails and, vulnerabilities — Java, Adobe Flash and Acrobat, Firefox and Chrome plugins, 0-day client-side / browser vulnerabilities.

Use of AI:

- AI can be utilized for software inventory management by identifying and categorizing installed applications on endpoints and servers.

Business Impact:

- Helps in managing and controlling software licenses, reducing costs and ensuring compliance. It also mitigates the risk of unapproved or vulnerable software being used within the organization.

SANS Critical Control 3: Secure Configurations

Control 3 focuses on ensuring companies set up and install the proper security configurations on all workstations, laptops, servers, and mobile devices. Individuals can use a configuration review scanner and authenticated scans to monitor the security of their operating systems automatically and make sure they aren't affected by malware.

Use of AI:

- AI can enhance vulnerability assessment by prioritizing vulnerabilities based on risk, helping organizations focus on the most critical issues.

Business Impact:

- Identifies and addresses vulnerabilities proactively, reducing the likelihood of successful cyberattacks. This control helps in safeguarding sensitive data, maintaining customer trust, and avoiding financial losses associated with data breaches.

Critical Control 4: Continuous Vulnerability Assessment and Remediation

The fourth control focuses on the value of continuous vulnerability management and remediation. Many companies will only scan their assets for potential vulnerabilities every three to six months, which may be the bare minimum for compliance purposes. Still, SANS urges companies to monitor their assets continuously. Hackers are waiting for potential vulnerabilities to pop up online

Use of AI:

- AI-driven analytics can monitor and detect unusual or unauthorized administrative activities, providing early warning of potential insider threats.

Business Impact:

- Minimizes the risk of insider threats and unauthorized access, protecting critical systems and data. This control helps in maintaining the confidentiality and integrity of sensitive information.

Critical Control 5: Malware Defenses

Malware remains a dangerous threat to organizations of all sizes. Companies can use the last vulnerability management software to automatically scan assets for malware before it can spread to other parts of the network.

Use of AI:

- AI can assist in ensuring secure configurations by automatically analyzing and verifying device configurations against security best practices.

Business Impact:

- Ensures that devices and systems are configured securely, reducing the risk of exploitation. This control helps in preventing unauthorized access, data breaches, and system disruptions.

Critical Control 6: Application Software Security

Web and mobile applications can often be the weakest link in the security chain. This control encourages companies to install web application firewalls to protect these applications while including them in the VRM scanning process.

Use of AI:

- AI can be employed to analyze large volumes of security logs, identifying patterns or anomalies indicative of potential security incidents.

Business Impact:

- Enhances the ability to detect and respond to security incidents promptly. This control aids in investigating and mitigating security breaches, minimizing the impact on operations and reputation.

Critical Control 7: Wireless Device Control

Wireless networks and the devices that use them often lack the necessary security protocols to ward off a potential attack. Control 7 outlines the ways in which organizations can test, monitor, and analyse their wireless networks for potential vulnerabilities while encrypting sensitive information and setting administrative privileges.

Use of AI:

- AI-based threat detection can enhance email and web security by identifying malicious content, phishing attempts, and other cyber threats

Business Impact:

- Guards against phishing attacks, malware, and other email/web-based threats, protecting sensitive information and maintaining the trust of customers and partners

Critical Control 8 and 9: Data Recovery Capability & Security Skill Assessment

Control 8 refers to an organization's ability to recover data in the event of a breach or attack. This often includes storing a secure backup outside of the company's IT system.

Control 9 refers to an organization's ongoing security training program and security skill improvement. Employees need to regularly improve their skills to keep up with the latest trends in cyber security.

Use of AI:

- AI-driven malware detection tools can improve the ability to identify and mitigate malware by analyzing behavior, heuristics, and known patterns.

Business Impact:

- Reduces the risk of malware infections, which can lead to data loss, operational disruptions, and reputational damage. This control helps in safeguarding business continuity.

Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

This control speaks to the importance of setting security configurations for network devices, including internet routers, which often lack the necessary cyber security protections.

Use of AI:

- AI can assist in monitoring network traffic to identify and block unauthorized or malicious protocols and services.

Business Impact:

- Minimizes the attack surface, making it harder for adversaries to exploit vulnerabilities. This control helps in preventing unauthorized access and maintaining the confidentiality and availability of services.

Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services

Control 11 focuses on limiting access to network ports, protocols, and other services. The latest VRM software will analyze production systems for unauthorized ports, protocols, and services while blocking unauthorized users using the application firewall.

Use of AI:

- AI can enhance data protection by monitoring and analyzing user behavior to detect unusual access patterns or potential data breaches.

Business Impact:

- Reduces the risk of security vulnerabilities in software applications, protecting against data breaches and potential financial losses. This control contributes to the overall security of software products and systems.

Critical Control 12: Controlled Use of Administrative Privileges

This control deals with an organization’s ability to track and control the use of administrative privileges.

Use of AI:

- AI can assist in ensuring secure configurations by analyzing and validating the settings of network devices for compliance with security policies.

Business Impact:

- Safeguards sensitive data from unauthorized access or disclosure, protecting the organization from regulatory fines, legal liabilities, and damage to its reputation.

Critical Control 13: Boundary Défense

Boundary defences are cybersecurity tools that automatically differentiate networks based on their trustworthiness such as firewalls, intrusion detection and prevention systems, web content filtering, network access controls, routers/switches, and proxy servers that can help organizations prevent attacks.

Use of AI:

- AI-driven intrusion detection and prevention systems can strengthen boundary defenses by identifying and blocking malicious traffic at network perimeters.

Business Impact:

- Ensures that network devices are configured securely, reducing the risk of unauthorized access and network-based attacks. This control contributes to the overall security of the organization's IT infrastructure.

Critical Controls 14 and 15: Audit Logs and Controlled Access

Control 14 refers to audit logs for firewalls, network devices, servers, and hosts. They are usually the only way to determine whether the host has been compromised. The logs need to be aggregated, safeguarded, and correlated with other relevant security events.

Control 15 deals with controlling access to data from people with the appropriate need to know, based on their level in the organization. This can help organizations prevent sensitive information from falling into the wrong hands.

Use of AI:

- AI can play a role in data loss prevention by monitoring and classifying sensitive data and enforcing policies to prevent unauthorized access or transmission.

Business Impact:

- Enhances the organization's ability to detect and block malicious network traffic at the perimeter, reducing the risk of cyberattacks and protecting critical assets.

Critical Control 16: Account Monitoring and Control

This control talks about the need to the protect privileged user and administrative accounts. Automatic scanning tools will automatically identify potential access control vulnerabilities, including expired or weak passwords and outdated lockout policies.

Use of AI:

- AI can help in implementing role-based access controls and dynamically adjusting access privileges based on user behavior and context.

Business Impact:

- Helps in preventing data breaches by implementing controls to protect sensitive information, thereby avoiding financial losses, reputational damage, and legal consequences.

Critical Controls 17, 18 and 19: Data Loss Prevention, Incident Response and Management, Secure Network Engineering

These controls focus on how companies can prevent potential data breaches, improve their incident response times, and avoid permanent data loss.

Use of AI:

- AI can enhance wireless security by detecting and responding to unauthorized or anomalous wireless access attempts.

Business Impact:

- Minimizes the risk of unauthorized access to sensitive information, protecting confidentiality and maintaining trust with customers and stakeholders.

Critical Control 20: Penetration Tests and Red Team Exercises

The last control talks about the importance of penetration testing and how companies can hire ethical hackers to conduct simulated attacks on the system without disrupting operations. The organization can then patch the system before a real attack occurs.

Use of AI:

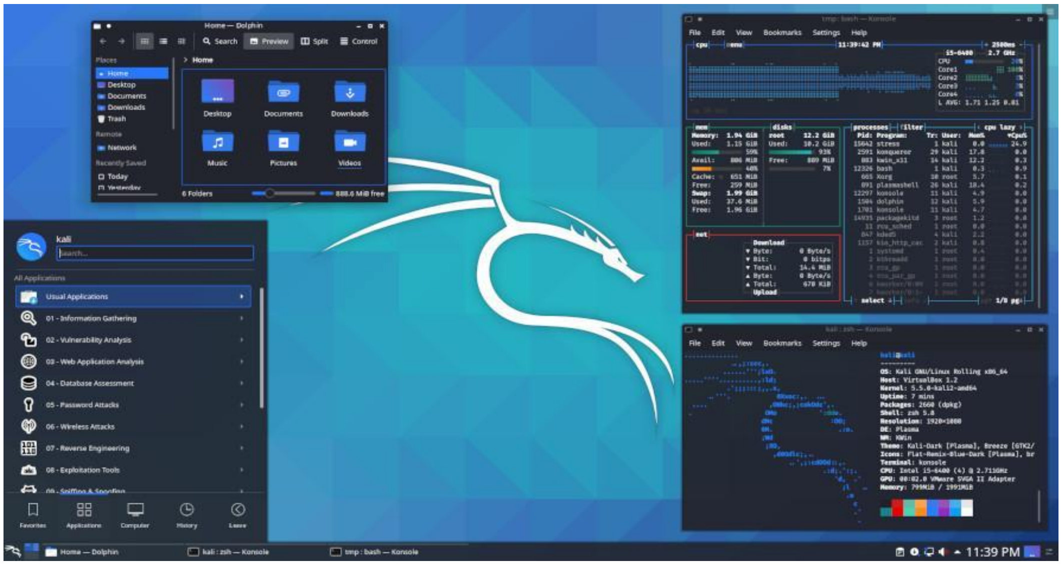
- AI can be integrated into the software development lifecycle to identify and mitigate security vulnerabilities in code and dependencies.

Business Impact:

- Identifies and addresses security weaknesses through simulated attacks, improving the organization's overall cybersecurity resilience. This control helps in proactively strengthening defenses and avoiding the financial and reputational impact of successful cyberattacks.

Cybersecurity simulation tools or platforms that demonstrate AI-driven threat identification

1. Kali Linux:



```
cpu   menu                11:39:42 PM                      2500ms
                                                 i5-6400    2.7 GHz
                                                 CPU                 20%
                                                 Core1              100%
                                                 Core2                0%
                                                 Core3                2%
                                                 Core4                0%
                                                 L AVG: 1.71 1.25 0.81

mem                    disks                 processes  filter         cpu lazy
Memory:   1.94 GiB     root      12.2 GiB     Pid: Program:       Tr: User:  Mem%   Cpu%
Used:     1.15 GiB     Used:     10.2 GiB   15642 stress           1 kali    0.0   24.9
                59%                   93%    2591 konqueror       29 kali   17.8    0.0
Avail:     806 MiB     Free:      809 MiB     883 kwin_x11        14 kali   12.2    0.3
                40%                    7%   12326 bash             1 kali    0.3    0.9
Cache:     651 MiB                            665 Xorg            10 root    5.7    0.1
Free:      259 MiB                            891 plasmashell     26 kali   18.4    0.2
Swap:     1.99 GiB                          12297 konsole         11 kali    4.9    0.0
Used:     37.6 MiB                           1504 dolphin         12 kali    5.9    0.0
Free:     1.96 GiB                           1701 konsole         11 kali    4.7    0.0
                                            14935 packagekitd      3 root    1.2    0.0
net                                            11 rcu_sched        1 root    0.0    0.0
               Download                       847 kded5            4 kali    2.2    0.0
               ▼ Byte:       0 Byte/s        1157 kio_http_cac     2 kali    0.0    0.0
               ▼ Bit:          0 bitps          1 systemd          1 root    0.4    0.0
               ▼ Total:     14.4 MiB            2 kthreadd         1 root    0.0    0.0
               ▲ Byte:       0 Byte/s           3 rcu_gp           1 root    0.0    0.0
               ▲ Total:      670 KiB            4 rcu_par_gp       1 root    0.0    0.0
               Upload                           6 kworker/0:0H     1 root    0.0    0.0
                                                7 kworker/0:1-     1 root    0.0    0.0
                                              select                          1/0 pg
```

```
kali@kali
---------
OS: Kali GNU/Linux Rolling x86_64
Host: VirtualBox 1.2
Kernel: 5.5.0-kali2-amd64
Uptime: 7 mins
Packages: 2660 (dpkg)
Shell: zsh 5.8
Resolution: 1920x1080
DE: Plasma
WM: KWin
Theme: Kali-Dark [Plasma], Breeze [GTK2/
Icons: Flat-Remix-Blue-Dark [Plasma], br
Terminal: konsole
CPU: Intel i5-6400 (4) @ 2.711GHz
GPU: 00:02.0 VMware SVGA II Adapter
Memory: 799MiB / 1991MiB
```

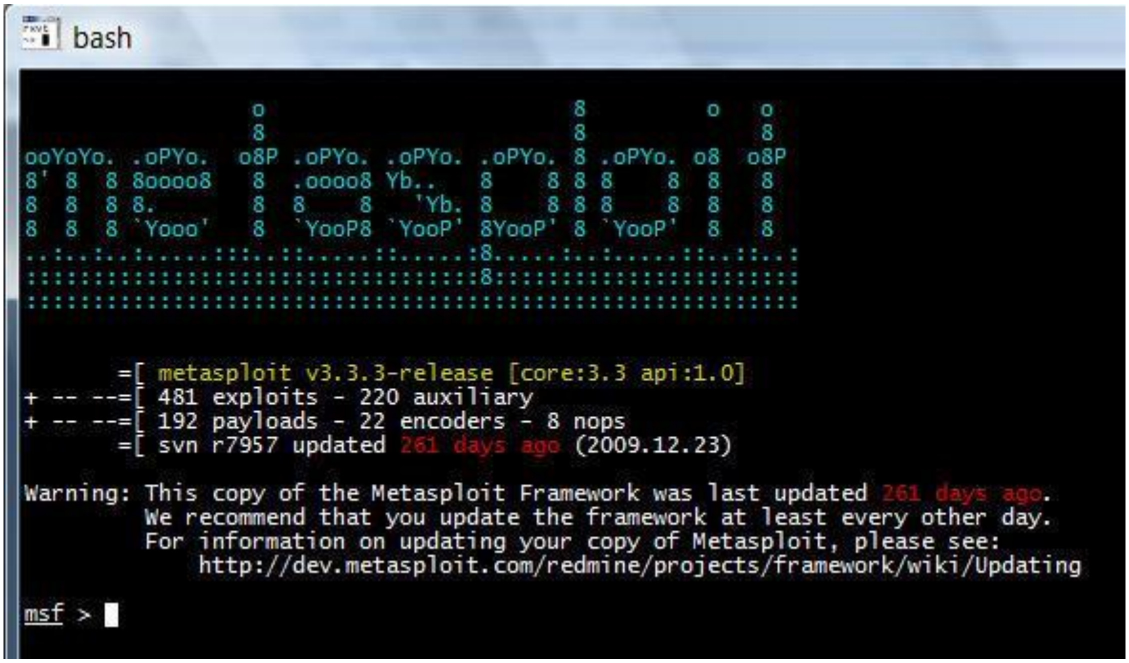
Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering

- It has 600+ Penetration testing and network security tools pre-installed.
- It is completely free and open source. So you can use it for free and even contribute for its development.
- It supports many languages.
- Great for those who are intermediate in Linux and have their hands on Linux commands.
- Could be easily used with Raspberry Pi.

2. Metasploit:

The world’s most used penetration testing framework

Knowledge is power, especially when it’s shared. A collaboration between the open source community and Rapid7, Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness; it empowers and arms defenders to always stay one step (or two) ahead of the game.

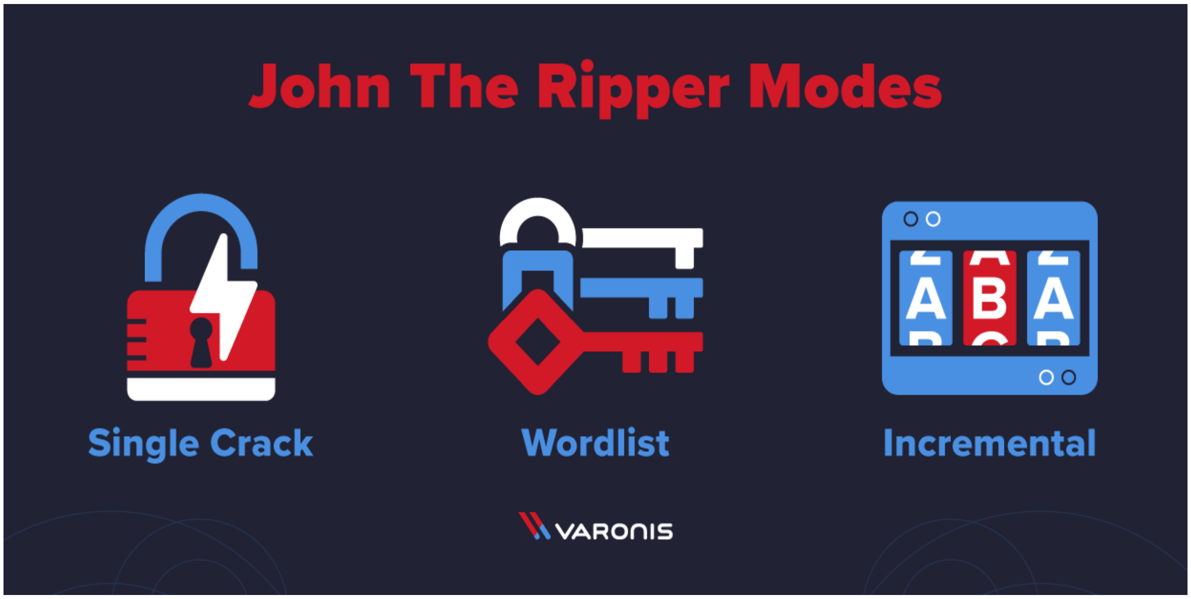


```
                 o                       8         o   o
                 8                       8             8
ooYoYo. .oPYo.  o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8  o8P
8' 8  8 8oooo8   8  .oooo8 Yb..   8    8 8 8    8  8   8
8  8  8 8.       8  8    8   'Yb. 8    8 8 8    8  8   8
8  8  8 `Yooo'   8  `YooP8 `YooP' 8YooP' 8 `YooP'  8   8
..:..:..:.....::..::.....::.....:8.....:..:.....::..::..:
:::::::::::::::::::::::::::::::::8::::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


       =[ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --=[ 481 exploits - 220 auxiliary
+ -- --=[ 192 payloads - 22 encoders - 8 nops
       =[ svn r7957 updated 261 days ago (2009.12.23)

Warning: This copy of the Metasploit Framework was last updated 261 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             http://dev.metasploit.com/redmine/projects/framework/wiki/Updating

msf > 
```

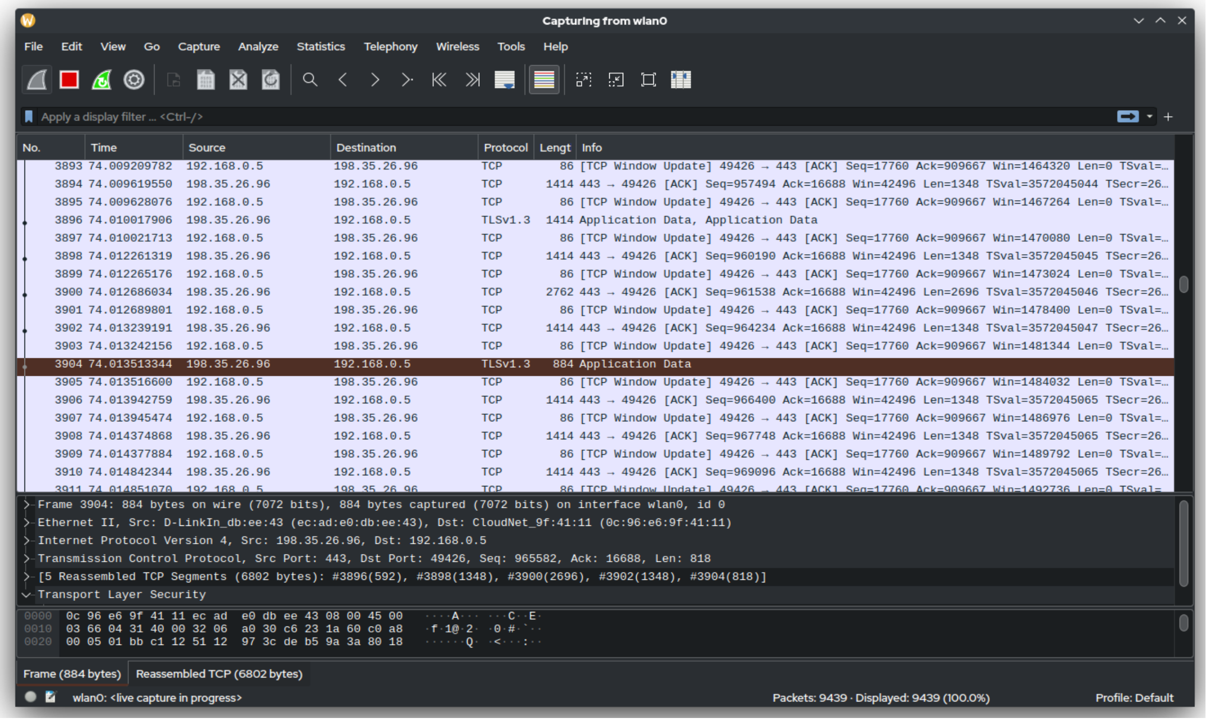
- Metasploit is the world’s leading open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits.
- The framework makes hacking simple for both attackers and defenders.
- The purpose of Metasploit is to help users identify where they are most likely to face attacks by hackers and proactively mend those weaknesses before exploitation by hackers.

3. John The Ripper:

- John the Ripper is an offline password cracking tool that was developed in 1996 by Openwall Project. It is notable for supporting a diversity of password formats.
- The tool is also notable for its ubiquity and accessibility. It's included in the default repositories for many Linux distributions, including Debian and Ubuntu, and installed by default in most penetration testing distributions, including Kali and BlackArch.
- John the Ripper isn't the most complicated tool, but as you'll see with some experimentation, it is a true workhorse for red teamers, blue teamers and auditors alike.



- Wireshark is an open-source network protocol analysis software program, widely considered the industry standard.
- A global organization of network specialists and software developers supports Wireshark and continues to make updates for new network technologies and encryption methods.



```
No.  Time         Source         Destination    Protocol Lengt Info
3893 74.009209782 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1464320 Len=0 TSval=…
3894 74.009619550 198.35.26.96   192.168.0.5    TCP      1414 443 → 49426 [ACK] Seq=957494 Ack=16688 Win=42496 Len=1348 TSval=3572045044 TSecr=26…
3895 74.009628076 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1467264 Len=0 TSval=…
3896 74.010017906 198.35.26.96   192.168.0.5    TLSv1.3  1414 Application Data, Application Data
3897 74.010021713 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1470080 Len=0 TSval=…
3898 74.012261319 198.35.26.96   192.168.0.5    TCP      1414 443 → 49426 [ACK] Seq=960190 Ack=16688 Win=42496 Len=1348 TSval=3572045045 TSecr=26…
3899 74.012265176 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1473024 Len=0 TSval=…
3900 74.012686034 198.35.26.96   192.168.0.5    TCP      2762 443 → 49426 [ACK] Seq=961538 Ack=16688 Win=42496 Len=2696 TSval=3572045046 TSecr=26…
3901 74.012689801 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1478400 Len=0 TSval=…
3902 74.013239191 198.35.26.96   192.168.0.5    TCP      1414 443 → 49426 [ACK] Seq=964234 Ack=16688 Win=42496 Len=1348 TSval=3572045047 TSecr=26…
3903 74.013242156 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1481344 Len=0 TSval=…
3904 74.013513344 198.35.26.96   192.168.0.5    TLSv1.3   884 Application Data
3905 74.013516600 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1484032 Len=0 TSval=…
3906 74.013942759 198.35.26.96   192.168.0.5    TCP      1414 443 → 49426 [ACK] Seq=966400 Ack=16688 Win=42496 Len=1348 TSval=3572045065 TSecr=26…
3907 74.013945474 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1486976 Len=0 TSval=…
3908 74.014374868 198.35.26.96   192.168.0.5    TCP      1414 443 → 49426 [ACK] Seq=967748 Ack=16688 Win=42496 Len=1348 TSval=3572045065 TSecr=26…
3909 74.014377884 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1489792 Len=0 TSval=…
3910 74.014842344 198.35.26.96   192.168.0.5    TCP      1414 443 → 49426 [ACK] Seq=969096 Ack=16688 Win=42496 Len=1348 TSval=3572045065 TSecr=26…
3911 74.014851070 192.168.0.5    198.35.26.96   TCP        86 [TCP Window Update] 49426 → 443 [ACK] Seq=17760 Ack=909667 Win=1492736 Len=0 TSval=…
```

```
> Frame 3904: 884 bytes on wire (7072 bits), 884 bytes captured (7072 bits) on interface wlan0, id 0
> Ethernet II, Src: D-LinkIn_db:ee:43 (ec:ad:e0:db:ee:43), Dst: CloudNet_9f:41:11 (0c:96:e6:9f:41:11)
> Internet Protocol Version 4, Src: 198.35.26.96, Dst: 192.168.0.5
> Transmission Control Protocol, Src Port: 443, Dst Port: 49426, Seq: 965582, Ack: 16688, Len: 818
> [5 Reassembled TCP Segments (6802 bytes): #3896(592), #3898(1348), #3900(2696), #3902(1348), #3904(818)]
v Transport Layer Security
```

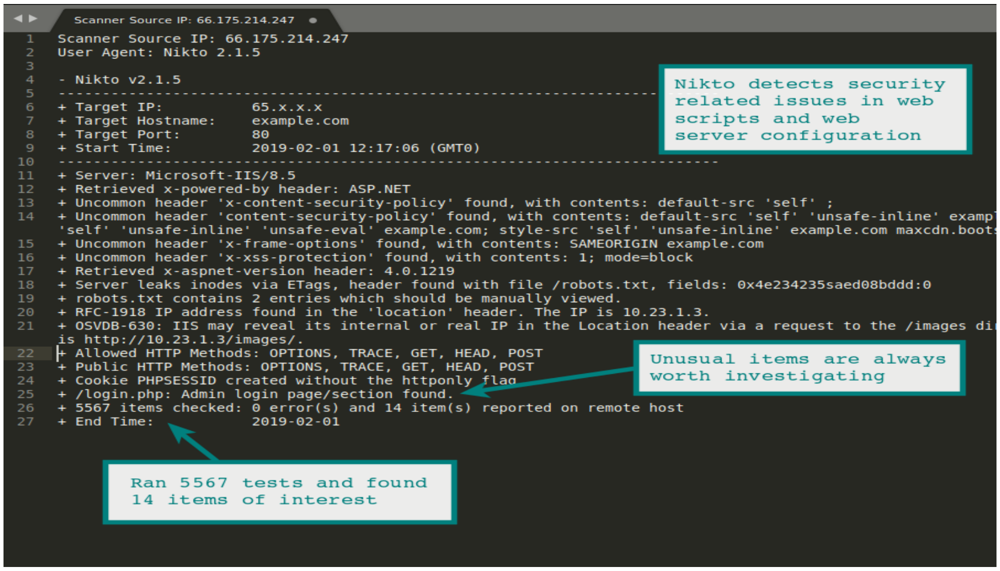
```
0000  0c 96 e6 9f 41 11 ec ad  e0 db ee 43 08 00 45 00   ····A···  ···C··E·
0010  03 66 04 31 40 00 32 06  a0 30 c6 23 1a 60 c0 a8   ·f·1@·2·  ·0·#·`··
0020  00 05 01 bb c1 12 51 12  97 3c de b5 9a 3a 80 18   ······Q·  ·<···:··
```

wlan0: <live capture in progress>   Packets: 9439 · Displayed: 9439 (100.0%)   Profile: Default

- Wireshark is a packet sniffer and analysis tool. It captures network traffic from ethernet, Bluetooth, wireless (IEEE.802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis.
- Wireshark can be used to understand how communication takes place across a network and to analyze what went wrong when an issue in communication arises

5. NIKTO:

- Nikto is an open source (GPL) web server scanner that performs vulnerability scanning against web servers for multiple items, including dangerous files and programs.
- Nitko checks for outdated versions of web server software. It also checks for server configuration errors and any possible vulnerabilities they might have introduced.
- Nikto can detect over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.
- It also checks for server configuration items such as the presence of multiple index files and HTTP server options, and will attempt to identify installed web servers and software.
- Scan items and plugins are frequently updated and can be automatically updated.



```
Scanner Source IP: 66.175.214.247
User Agent: Nikto 2.1.5

- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          65.x.x.x
+ Target Hostname:    example.com
+ Target Port:        80
+ Start Time:         2019-02-01 12:17:06 (GMT0)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.5
+ Retrieved x-powered-by header: ASP.NET
+ Uncommon header 'x-content-security-policy' found, with contents: default-src 'self' ;
+ Uncommon header 'content-security-policy' found, with contents: default-src 'self' 'unsafe-inline' examp
'self' 'unsafe-inline' 'unsafe-eval' example.com; style-src 'self' 'unsafe-inline' example.com maxcdn.boot
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN example.com
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
+ Retrieved x-aspnet-version header: 4.0.1219
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x4e234235saed08bddd:0
+ robots.txt contains 2 entries which should be manually viewed.
+ RFC-1918 IP address found in the 'location' header. The IP is 10.23.1.3.
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images di
is http://10.23.1.3/images/.
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Cookie PHPSESSID created without the httponly flag
+ /login.php: Admin login page/section found.
+ 5567 items checked: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2019-02-01
```

Nikto detects security related issues in web scripts and web server configuration

Unusual items are always worth investigating

Ran 5567 tests and found 14 items of interest

A case Study on SANS 20:

Problem :

"*It was one of those things like death and taxes. You're just going to have to pay your dues and do it a certain way. And then this came along and gave us the opportunity to solve two or three very challenging problems in a way that was much more satisfactory to our customers, helps us understand and protect our content and its usage and allows the frequent and consistent updates required by our industry and customers*."

- To solve these problems, the SANS Institute uses Content Controller. The new implementation allows SANS to centrally host their content in order to seamlessly deliver the latest, most accurate content and streamline license administration.

The results

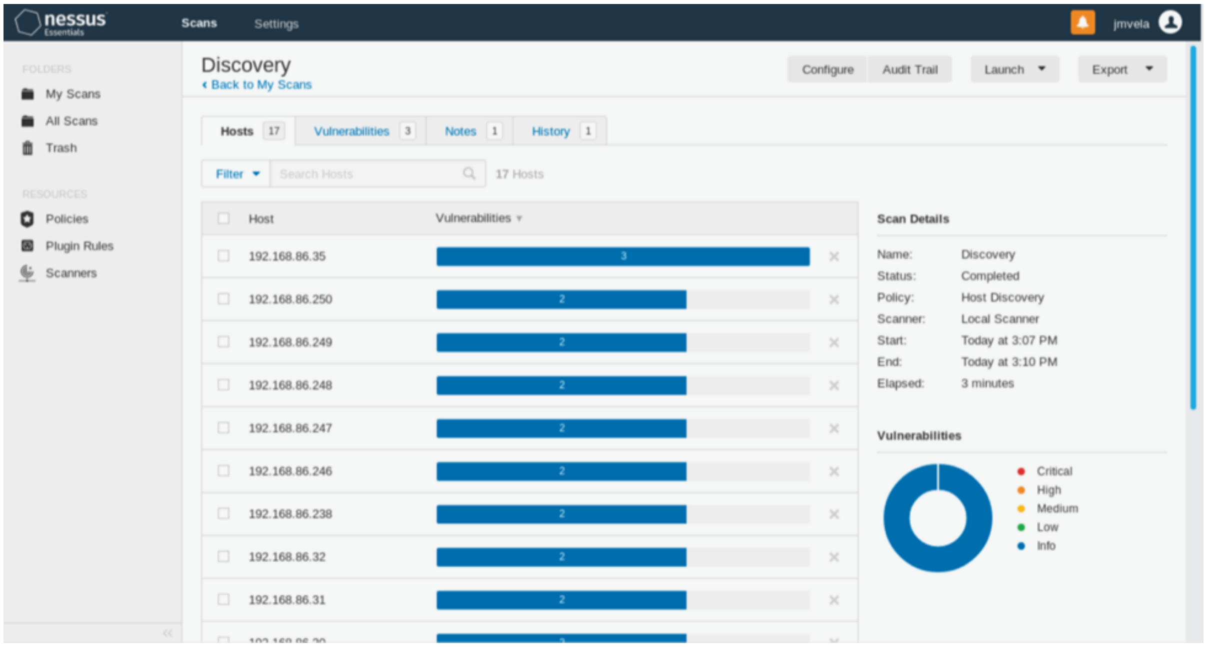
The partnership between the SANS Institute and Rustici Software allows SANS to successfully deliver upwards of one million training modules per week that can be easily updated and tracked. Since launching Content Controller, SANS has seen:

1. A 90% reduction in time spent updating existing content, saving $100,000 in employee costs per year.
2. A significant increase in revenues by ensuring customers are paying for the right number of learners.
3. Efficient deployment of 28 languages as a single course.
4. 70 LMSs across 600 customers supported with the ability to easily deploy to more.

Stage 2: Nessus Plugins & Threat Detections And Response

Nessus:-

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.



Discovery
‹ Back to My Scans

17 Hosts

Host	Vulnerabilities
192.168.86.35	3
192.168.86.250	2
192.168.86.249	2
192.168.86.248	2
192.168.86.247	2
192.168.86.246	2
192.168.86.238	2
192.168.86.32	2
192.168.86.31	2

Scan Details

Name:	Discovery
Status:	Completed
Policy:	Host Discovery
Scanner:	Local Scanner
Start:	Today at 3:07 PM
End:	Today at 3:10 PM
Elapsed:	3 minutes

Vulnerabilities

Plugin:-

A security plugin is a type of software that adds an extra layer of protection to a site by scanning for security issues. Plug-ins can also be called add-ons or extensions

Plugin Catalog Exploration:-

As information about new vulnerabilities is discovered and released into the general public domain, Tenable Research designs programs to detect them. These programs are named plugins and are written in the Nessus Attack Scripting Language (NASL). The plugins contain vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of the security issue. Tenable Research has published 200101 plugins, covering 81043 CVE IDs and 30943 Bugtraq IDs.

ID	Name	Product	Family	Severity
501853	Moxa (CVE-2023-5962)	Tenable OT Security	Tenable.ot	MEDIUM
187632	RHEL 8 : squid:4 (RHSA-2024:0046)	Nessus	Red Hat Local Security Checks	HIGH
187631	Wireshark 4.2.x < 4.2.1 Multiple Vulnerabilities (macOS)	Nessus	MacOS X Local Security Checks	HIGH
187630	Wireshark 4.2.x < 4.2.1 Multiple Vulnerabilities	Nessus	Windows	HIGH
187629	Oracle Linux 8 : thunderbird (ELSA-2024-0003)	Nessus	Oracle Linux Local Security Checks	HIGH
187628	Oracle Linux 8 : firefox (ELSA-2024-0012)	Nessus	Oracle Linux Local Security Checks	HIGH
187627	Ubuntu 22.04 LTS : OpenSSH vulnerabilities (USN-6565-1)	Nessus	Ubuntu Local Security Checks	HIGH
187626	Ubuntu 22.04 LTS : SQLite vulnerabilities (USN-6566-1)	Nessus	Ubuntu Local Security Checks	HIGH
187625	Wireshark 4.0.x < 4.0.12 Multiple Vulnerabilities	Nessus	Windows	HIGH
187624	Wireshark 4.0.x < 4.0.12 Multiple Vulnerabilities (macOS)	Nessus	MacOS X Local Security Checks	HIGH

Plugin Categories:-

The plugins are categorized according to the vulnerabilities

ACT_COMPLIANCE_CHECK - Non The plugins below are listed in the order they will run during the scan.
ACT_INIT - Sets KB values. Will not send network traffic. These plugins always run.

ACT_SCANNER - Port scanner or pings the target

ACT_SETTINGS - Sets KB values. May send traffic over the network. Cannot be disabled.

ACT_GATHER_INFO - Non-intrusive. Generally perform banner grab or send harmless packets to host.

ACT_ATTACK - non-intrusive action which would be considered as an attack by many IDSes.

ACT_MIXED_ATTACK - Non-intrusive if safe checks are enabled. May be intrusive if safe checks are disabled.

ACT_DESTRUCTIVE_ATTACK -intrusive local configuration check

ACT_DENIAL - Attempts to crash service

ACT_KILL_HOST - Attempts to crash host

ACT_FLOOD - Attempts to flood network

ACT_END - Executed last

Plugin Functionality Analysis:-

Plugin Workflow:-

Plugin Initialization: When Nessus starts up, it initializes the plugin framework. The framework loads all the plugins available in the plugin database.

Plugin Configuration: The user configures Nessus by selecting the specific plugins to be used in the scan. This configuration includes enabling or disabling specific categories or individual plugins.

Plugin Scanning: Once the configuration is set, Nessus performs a scan on the target system. It identifies vulnerabilities by using various plugins. Each plugin is responsible for scanning a specific aspect of the target system, such as open ports, outdated software, or weak configurations.

Plugin Activation: During the scan, Nessus activates each selected plugin according to its configuration. For instance, if a plugin is configured to search for specific vulnerabilities, it will be activated and executed on each target that meets the plugin's target criteria.

Plugin Execution: The activated plugin then performs the necessary tests and checks against the target system. It may send specific requests, execute scripts, or analyze network traffic to discover vulnerabilities.

Plugin Output: After executing, each plugin generates a report containing its findings. This report includes details about the vulnerabilities discovered, potential risks, severity levels, and recommended actions to mitigate or resolve the issues.

Plugin Reporting: Once the scan is complete, Nessus compiles all the plugin reports into a comprehensive vulnerability assessment report. This report provides an overview of the security posture of the scanned system and helps prioritize remediation efforts.

*The specific steps within this workflow depend on the plugin type and the target being scanned.

Feature Examination:

Analyzing the Contributions of Specific Plugin Features to Threat Identification.Plugin features play a crucial role in identifying and mitigating threats within systems. This article aims to evaluate the significance of specific features within plugins and their impact on threat identification.

I. Feature 1: Scripting Capabilities

Scripting capabilities within plugins enable advanced threat detection and prevention. These capabilities allow the execution of custom scripts to identify unique vulnerabilities. Examples of scripting capabilities include the ability to conduct specialized scans, parse specific logs, or perform targeted reconnaissance. However, it is important to consider potential vulnerabilities and limitations associated with scripting, such as script errors or potential false positives.

II. Feature 2: Exploitability Checks

Exploitability checks are essential for identifying vulnerabilities that can be exploited by threat actors. These checks help prioritize vulnerabilities based on their potential impact and ease of exploitation. Plugins that offer built-in exploitability checks can assess vulnerabilities against known exploits, reducing false positives and providing actionable results. Considering potential limitations and the need for up-to-date exploit databases is crucial when utilizing exploitability checks.

III. Feature 3: Protocol-Specific Detections

Protocol-specific detections focus on identifying threats that target specific communication protocols. Plugins with this feature leverage protocol-specific knowledge to conduct specialized scans to detect protocol-related vulnerabilities. Examples include plugins that detect vulnerabilities in web applications, email servers, or network protocols. It is important to consider the limitations, such as the need for appropriate protocol configurations and potential false negatives

- Features of the specific plugin

Siemens SIMATIC S7-400 Uncontrolled Recursion vulnerability (CVE-2022-47374):-

The remote OT asset is affected by a vulnerability. A vulnerability has been identified in SIMATIC PC-Station Plus (All versions), SIMATIC S7-400 CPU 412-2 PN V7 (All versions), SIMATIC S7-400 CPU 414-3 PN/DP V7 (All versions), SIMATIC S7-400 CPU 414F-3 PN/DP V7 (All versions), SIMATIC S7-400 CPU 416-3 PN/DP V7 (All versions), SIMATIC S7-400 CPU 416F-3 PN/DP V7 (All versions), SINAMICS S120 (incl. SIPLUS variants) (All versions < V5.2 SP3 HF15), SIPLUS S7-400 CPU 414-3 PN/DP V7 (All versions), SIPLUS S7-400 CPU 416-3 PN/DP V7 (All versions). The affected products do not handle HTTP(S) requests to the web server correctly. This could allow an attacker to exhaust system resources and create a denial of service condition for the device.

Exploitability Checks:

Purpose: Identify and assess vulnerabilities in the Siemens SIMATIC S7-400, particularly the CVE-2022-47374.

Analysis: Verify if the security plugin has specific exploitability checks for the CVE-2022-47374 vulnerability.Assess the accuracy and completeness of the exploitability checks to ensure proper identification of this specific issue.

Protocol-Specific Detections:

Purpose: Detect threats related to the Siemens SIMATIC S7-400 protocol and identify instances of uncontrolled recursion.

Analysis: Evaluate if the plugin includes protocol-specific detections for Siemens SIMATIC S7-400 vulnerabilities. Assess the depth of protocol analysis, specifically focusing on uncontrolled recursion as described in CVE-2022-47374.

Integration with Threat Intelligence:

Purpose: Leverage external threat intelligence to enhance detection capabilities, including knowledge about the CVE-2022-47374.

Analysis: Check if the plugin integrates with threat intelligence feeds that provide information on Siemens SIMATIC S7-400 vulnerabilities, including CVE-2022-47374.
Assess the timeliness and accuracy of updates from threat intelligence sources.

Testing Scenarios:

Conducting hands-on testing within a controlled environment is a practical approach to evaluating the performance of security plugins. Here are general testing scenarios that you can apply across a range of security plugins to observe their performance in detecting vulnerabilities and potential threats in a controlled environment:

Basic Vulnerability Scanning:

Scenario: Introduce outdated software versions and misconfigurations in the test environment.

Objective: Evaluate how each security plugin identifies and reports basic vulnerabilities in the system.

Exploitation Simulation:

Scenario: Attempt to exploit known vulnerabilities in the test environment.

Objective: Assess how each security plugin detects and prevents actual exploitation attempts.

Protocol-Specific Threats:

Scenario: Simulate network traffic with protocol-specific threats (e.g., SQL injection, buffer overflow).

Objective: Evaluate the capability of each security plugin to detect and mitigate threats specific to different protocols.

Malware Injection:

Scenario: Introduce malware into the controlled environment.

Objective: Test how quickly and accurately each security plugin identifies and responds to the threat.

Behavioral Analysis:

Scenario: Simulate abnormal behavior in the system, such as unauthorized access or data exfiltration.

Objective: Assess how well each security plugin can identify and alert on unusual activities indicating potential security threats.

Threat Intelligence Feed Integration:

Scenario: Integrate threat intelligence feeds with up-to-date information on emerging threats.

Objective: Evaluate the responsiveness of each security plugin to new threats and the accuracy of threat intelligence integration.

Simulated DDoS Attack:

Scenario: Simulate a Distributed Denial of Service (DDoS) attack on the network.

Objective: Evaluate each security plugin's capability to detect and mitigate DDoS attacks, including its ability to differentiate between legitimate and malicious traffic.

Insider Threat Simulation:

Scenario: Mimic insider threats by simulating activities with malicious intent.

Objective: Assess how well each security plugin can detect and respond to threats originating from within the organization.

Custom Scripting:

Scenario: Utilize custom scripts to simulate advanced attack scenarios.

Objective: Evaluate the flexibility and customization capabilities of each security plugin, particularly in handling complex and custom attack techniques.

Compliance Testing:

Scenario: Validate if each security plugin adheres to specific compliance standards (e.g., PCI DSS, HIPAA).

Objective: Ensure that each security plugin can identify and report on security measures required by regulatory standards.

Reporting and Analysis:

After conducting hands-on testing with the security plugins and simulating various threat scenarios, the analysis of the reports generated by these plugins is crucial for understanding their effectiveness. Here's a detailed breakdown of how to analyze the reports:

Comprehensiveness of Reports:

- Evaluate how well the reports cover the detected vulnerabilities, threats, and overall security posture of the environment.
- Check if the reports provide a comprehensive overview of identified vulnerabilities, potential threats, and security events.
- Assess the depth of information provided for each detected issue, including details on affected systems, severity levels, and recommended remediation steps.

Accuracy of Threat Identification:

- Assess the accuracy of the security plugins in identifying and categorizing threats.
- Examine the reports to verify the accuracy of identified vulnerabilities and threats against the known scenarios introduced during testing.
- Look for false positives (incorrectly identified threats) and false negatives (missed threats) and evaluate their impact on the overall accuracy of threat identification.

Prioritization of Threats:

- Understand how well the security plugins prioritize identified threats based on severity and potential impact.

- Check if the reports categorize threats according to severity levels (e.g., critical, high, medium, low).
- Assess the relevance of the prioritization to the organization's risk tolerance and business impact.
- Evaluate if the plugins provide actionable insights on which vulnerabilities or threats should be addressed first based on their severity and potential impact.

Remediation Recommendations:

- Determine the effectiveness of the plugins in providing clear and actionable remediation recommendations.
- Evaluate the clarity and completeness of remediation guidance provided in the reports.
- Check if the plugins offer step-by-step instructions or links to relevant resources for addressing identified vulnerabilities and threats.
- Assess the feasibility and practicality of the recommended remediation steps.

Historical Trend Analysis:

- Understand the security posture over time by analyzing historical data and trends.
- If available, review historical reports and assess how the security posture has changed over time.
- Look for patterns in the frequency and severity of identified threats.
- Evaluate the plugins' ability to provide insights into emerging trends and potential areas of improvement.

Customization and Filtering Options:

- Assess the flexibility of the reporting tools, allowing users to customize and filter information.
- Check if the reports offer customization options, such as filtering by specific criteria (e.g., date range, severity).
- Evaluate the ease of use and flexibility in tailoring reports to meet the organization's specific requirements.

Integration with Other Tools:

- Determine the plugins' ability to integrate with other security tools and platforms.
- Assess if the reports can be integrated with other security information and event management (SIEM) systems or dashboards.
- Check for compatibility with third-party tools and the ease of sharing report data with relevant stakeholders.

Executive Summary and Dashboards:

- Evaluate the clarity and effectiveness of executive summaries and dashboards.
- Review executive summaries or dashboard views that provide high-level insights for executive stakeholders.
- Assess the clarity of key performance indicators, metrics, and overall security status communicated through these summary views.

Best Practices Research:

Leveraging Nessus plugins effectively is crucial for enhancing threat detection strategies. Here are industry best practices and guidelines for using Nessus plugins effectively:

Regular Plugin Updates:

Best Practice: Ensure that Nessus plugins are regularly updated to include the latest vulnerability checks and threat intelligence.

Rationale: Regular updates keep the plugin database current, allowing Nessus to detect and assess the latest vulnerabilities and threats.

Customization of Scans:

Best Practice: Tailor Nessus scans to align with the organization's specific environment, risk profile, and compliance requirements.

Rationale: Customized scans enhance the relevance of results, reduce noise, and focus on the most critical vulnerabilities applicable to the organization.

Thorough Scan Coverage:

Best Practice: Use Nessus to perform comprehensive scans covering all assets, networks, and systems within the organization.

Rationale: Full scan coverage ensures that no critical assets are overlooked, providing a holistic view of the organization's security posture.

Fine-Tuning Scan Policies:

Best Practice: Adjust scan policies based on the nature of the target systems (e.g., web applications, databases) to optimize scanning efficiency.

Rationale: Fine-tuning scan policies improves accuracy, reduces false positives, and enhances the overall efficiency of vulnerability assessments.

Prioritization of Findings:

Best Practice: Leverage Nessus to prioritize vulnerabilities based on severity levels and potential impact on the organization.

Rationale: Prioritization enables security teams to focus on addressing the most critical vulnerabilities first, improving risk management.

Integration with Security Workflows:

Best Practice: Integrate Nessus with other security tools and workflows, such as SIEM systems, ticketing systems, and orchestration platforms.

Rationale: Integration streamlines the vulnerability management process, facilitates collaboration, and automates response actions.

Credential-Based Scanning:

Best Practice: Utilize Nessus's credential-based scanning capabilities for authenticated scans.

Rationale: Authenticated scans provide more accurate and detailed information about the target systems, helping identify vulnerabilities that may not be visible in non-authenticated scans.

Customization and Optimization:

Customizing and optimizing Nessus plugins is essential to ensure that the vulnerability scanning tool aligns with specific security requirements and compliance standards. Here's a guide on how to experiment with plugin customization options, configurations, and tuning settings:

Scan Policy Customization:

* Tailor scan policies to align with the organization's security requirements.

* Access the Nessus user interface and navigate to the "Policies" section.

* Create a new policy or modify existing ones to adjust parameters like scan intensity, targets, and credentials.

* Experiment with different policy configurations to find the right balance between scan thoroughness and efficiency.

Plugin Selection and Exclusion:

*Optimize scan performance by selecting or excluding specific plugins based on the organization's needs.

* Use the Nessus user interface to review the list of available plugins.

* Customize scan policies to include or exclude specific plugin families or individual plugins.

* Experiment with different plugin configurations to focus on detecting vulnerabilities relevant to the organization.

Scan Scheduling and Timing:

* Optimize scan schedules and timing to minimize impact on production systems.

* Adjust scan schedules to times when network and system usage is low to reduce the impact on production environments.

* Experiment with different scan timing configurations to find the most suitable schedule for the organization.

Credential-Based Scanning:

* Improve scan accuracy by using authenticated scans with proper credentials.

* Ensure that appropriate credentials are configured for authenticated scans.

* Experiment with different credential options and configurations to maximize coverage and accuracy.

Scan Result Filtering:

* Streamline and prioritize scan results for more efficient remediation.

* Use filtering options in the Nessus user interface to focus on specific severity levels or vulnerability types.

* Experiment with different filters to tailor scan results based on the organization's risk tolerance and priorities.

Integration with Other Tools:

* Integrate Nessus with other security tools and platforms for streamlined workflows.

* Explore integration options with SIEM systems, ticketing systems, or orchestration platforms.

* Configure integrations to automate response actions and facilitate collaboration between security tools.

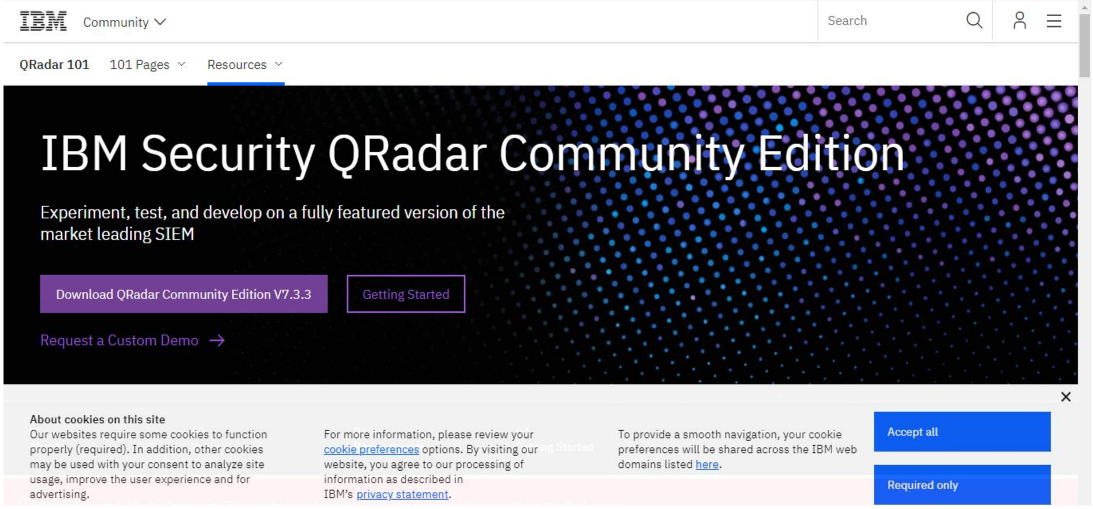
STAGE 3 : QRADAR INSTALLATION SOC DASHBOARD

IBM QRadar offers a wide range of features that help organizations effectively manage their security operations and detect potential threats. Here are some key features of IBM QRadar

- Log Management
- -Event Correlation and Analytics
- -Network Security Monitoring
- -Threat Intelligence Integration
- -Incident Investigation and Response
- -Compliance and Reporting
- -Threat Hunting
- -Integration Ecosystem
- -Advanced Analytics and User Behavior Analytics (UBA)
- -Automation and Orchestration

STEPS TO INSTALL:

1. Installation and Setup: Start by installing QRadar in your environment. Follow the installation guide provided by IBM to deploy the necessary components, such as the QRadar Console, Event Processors, and Data Nodes. Configure network connectivity and ensure that data sources are properly integrated with QRadar.



IBM Security QRadar Community Edition

Experiment, test, and develop on a fully featured version of the market leading SIEM

About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising.

For more information, please review your cookie preferences options. By visiting our website, you agree to our processing of information as described in IBM's privacy statement.

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed here.

2,.Data Source Configuration: Identify the data sources you want to monitor in QRadar. These can include network devices, servers, applications, logs, and more. Configure the appropriate data source protocols and settings to collect and ingest the log data into QRadar.

3.Network Configuration:

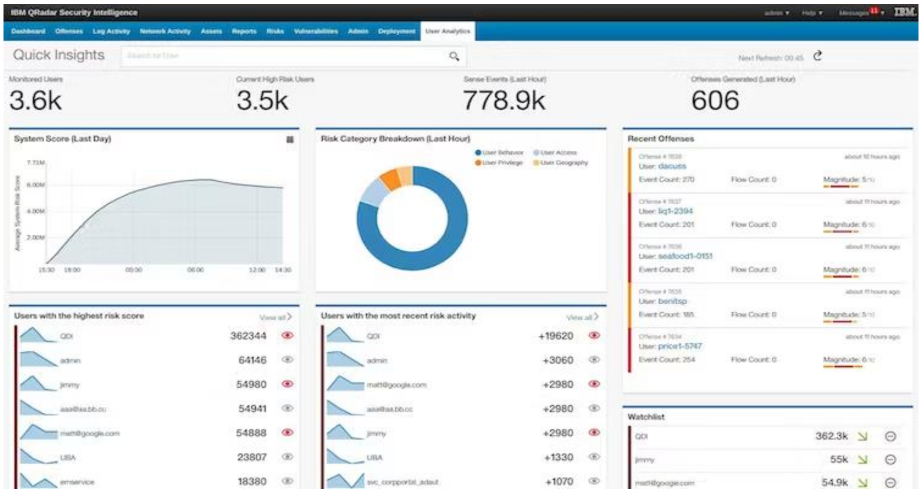
- Integrate QRadar with your network infrastructure, including configuring port mirroring or span ports on network switches to capture network traffic.
- Configure event sources to send logs to QRadar, such as syslog forwarding, log file collection, or integration with security devices and applications.

4.Initial Setup and Licensing:

- Complete the initial setup process, including system updates, license activation, and acceptance of the license agreement.
- Verify the connectivity between components, test log ingestion, and ensure events are being processed correctly.

5.Post-Installation Tasks:

- Configure backups and disaster recovery measures for your QRadar deployment.
- Implement best practices for system hardening, including securing administrative access, configuring firewalls, and implementing security policies.



Monitored Users 3.6k

Current High Risk Users 3.5k

Sense Events (Last Hour) 778.9k

Offenses Generated (Last Hour) 606

Users with the highest risk score

QDI	362344
admin	64146
jimmy	54980
aaa@aa.bb.cc	54941
matt@google.com	54888
UBA	23807
emservice	18380

Users with the most recent risk activity

QDI	+19620
admin	+3060
matt@google.com	+2980
aaa@aa.bb.cc	+2980
jimmy	+2980
UBA	+1330
svc_corpportal_adaut	+1070

Recent Offenses

Offense # 7638 about 10 hours ago
User: dacuss
Event Count: 270 Flow Count: 0 Magnitude: 5/10

Offense # 7637 about 11 hours ago
User: liq1-2394
Event Count: 201 Flow Count: 0 Magnitude: 6/10

Offense # 7636 about 11 hours ago
User: seafood1-0151
Event Count: 201 Flow Count: 0 Magnitude: 6/10

Offense # 7635 about 11 hours ago
User: benitsp
Event Count: 185 Flow Count: 0 Magnitude: 5/10

Offense # 7634 about 11 hours ago
User: price1-5747
Event Count: 254 Flow Count: 0 Magnitude: 6/10

Watchlist

QDI	362.3k
jimmy	55k
matt@google.com	54.9k

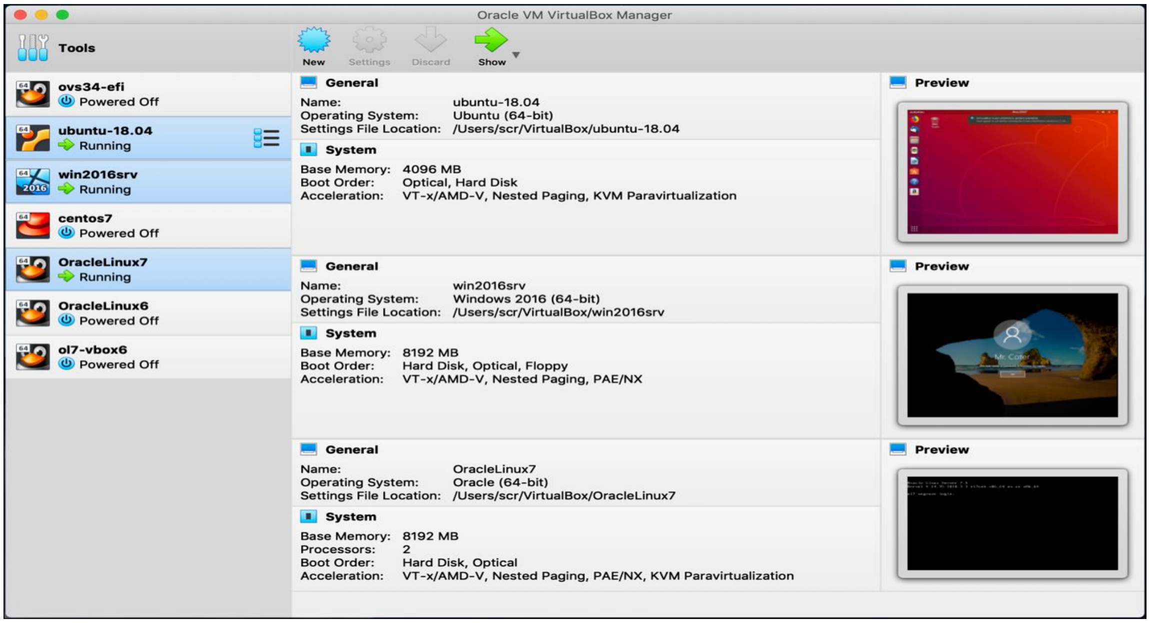
INSTALLATION OF VIRTUALBOX AS OVA FILE (open virtualization appliance) :

- To install IBM QRadar using an OVA (Open Virtualization Appliance) file, you can follow these steps:

- Download the OVA file: Obtain the IBM QRadar OVA file from the official IBM website or the IBM Passport Advantage website. Make sure you have the necessary license keys for your installation.

- Virtualization Software: Install virtualization software that supports OVA files, such as VMware vSphere, Oracle VirtualBox, or Microsoft Hyper-V. Choose the virtualization platform that best fits your environment and requirements.

- Import the OVA file: Open your virtualization software and import the IBM QRadar OVA file. This process may vary slightly depending on the virtualization platform you are using. Typically, you can go to the "File" or "Import" menu and select the OVA file from your local storage.



ovs34-efi
Powered Off
ubuntu-18.04
Running
win2016srv
Running
centos7
Powered Off
OracleLinux7
Running
OracleLinux6
Powered Off
ol7-vbox6
Powered Off

General
Name: ubuntu-18.04
Operating System: Ubuntu (64-bit)
Settings File Location: /Users/scr/VirtualBox/ubuntu-18.04

System
Base Memory: 4096 MB
Boot Order: Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

General
Name: win2016srv
Operating System: Windows 2016 (64-bit)
Settings File Location: /Users/scr/VirtualBox/win2016srv

System
Base Memory: 8192 MB
Boot Order: Hard Disk, Optical, Floppy
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX

General
Name: OracleLinux7
Operating System: Oracle (64-bit)
Settings File Location: /Users/scr/VirtualBox/OracleLinux7

System
Base Memory: 8192 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Adding Agents to Qradar :

1. Identify Agent Types: Determine the types of agents you want to connect to QRadar based on your monitoring requirements. Agents can include endpoint agents, network agents, or log source agents, depending on the data sources you want to monitor.

2. Install Agents: Install the appropriate agents on the devices or systems you wish to monitor. The installation process may vary depending on the agent type and the specific software being used. Follow the instructions provided by the agent vendor to install and configure the agents correctly.

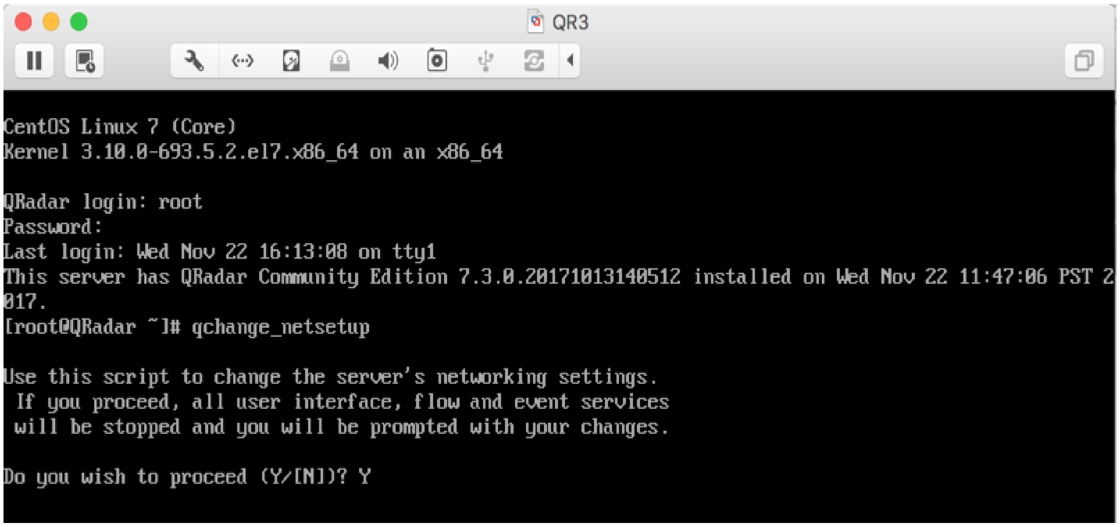
3. Configure Agent Settings: Once the agents are installed, configure their settings to establish a connection with IBM QRadar. This typically involves specifying the IP address or hostname of the QRadar console or Event Processor, along with any required authentication credentials.

Start the VM:

Log in to the console with these credentials, as shown below.

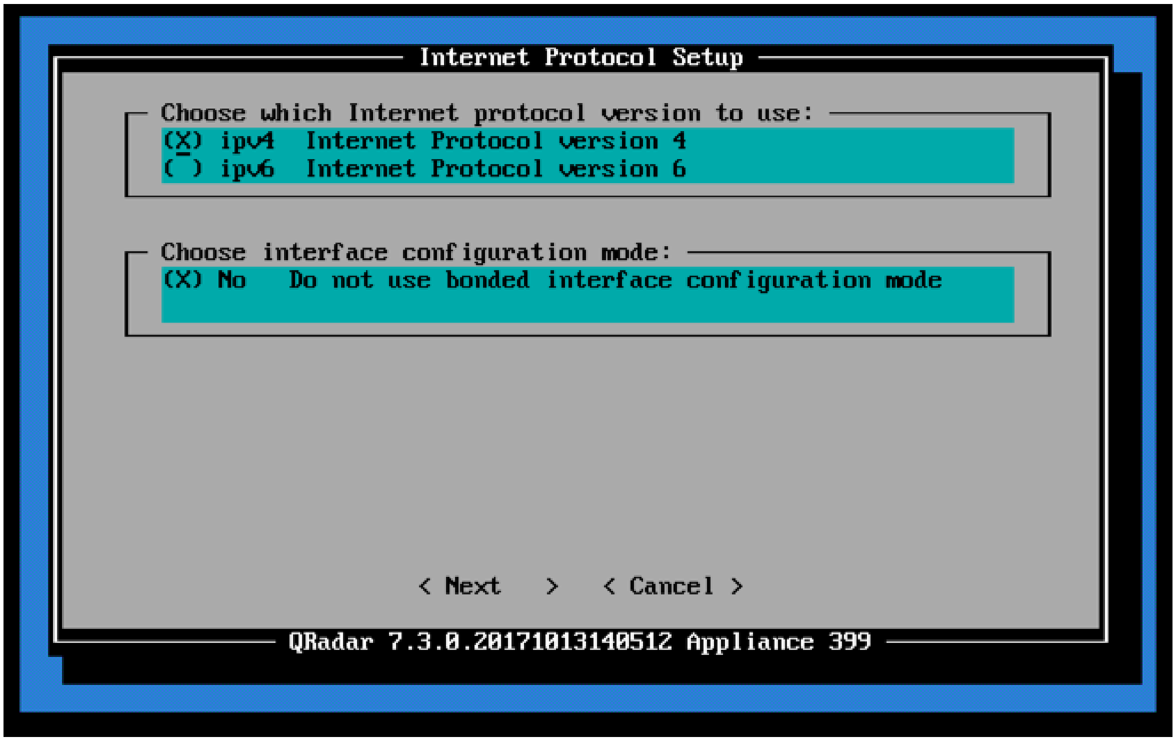
- Username: root

- Password: P@ssw0rd



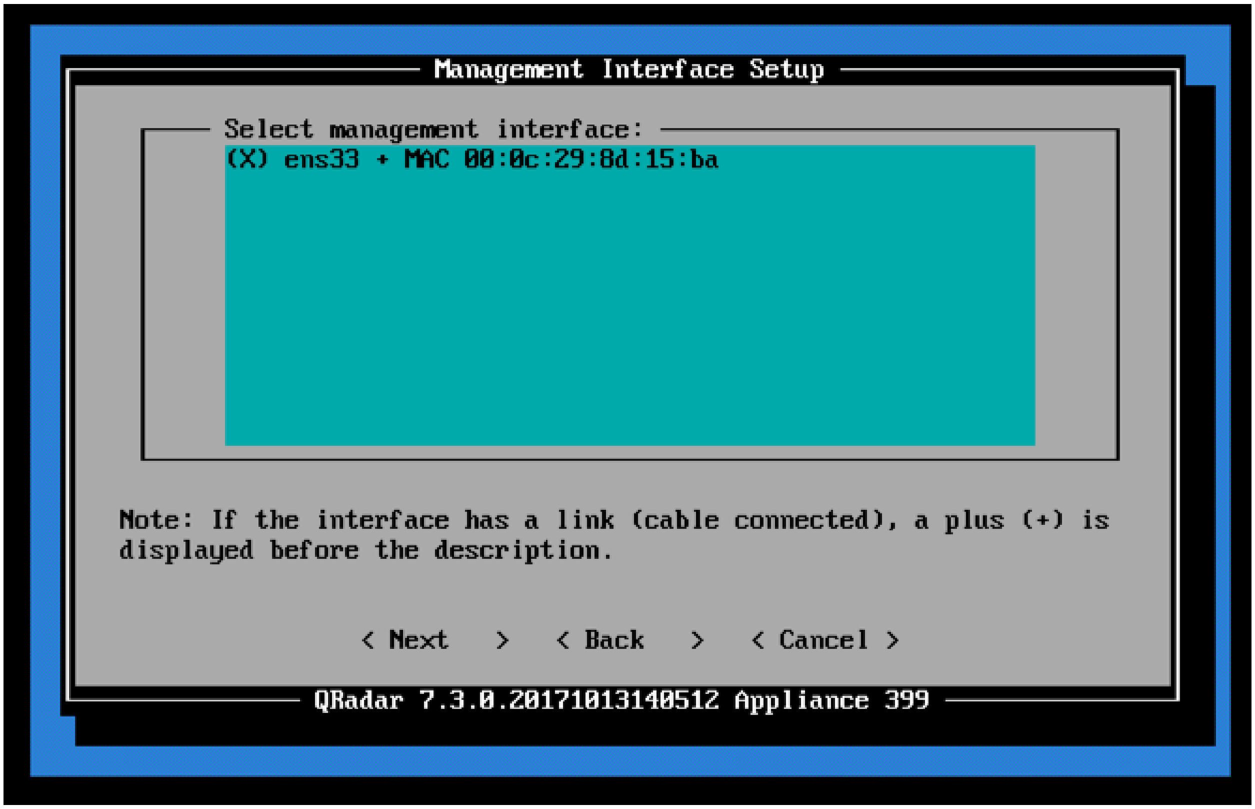
```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.5.2.el7.x86_64 on an x86_64

QRadar login: root
Password:
Last login: Wed Nov 22 16:13:08 on tty1
This server has QRadar Community Edition 7.3.0.20171013140512 installed on Wed Nov 22 11:47:06 PST 2
017.
[root@QRadar ~]# qchange_netsetup

Use this script to change the server's networking settings.
 If you proceed, all user interface, flow and event services
 will be stopped and you will be prompted with your changes.

Do you wish to proceed (Y/[N])? Y
```

- A series of crudely graphical screens appear. Use Tab to move through the options and Enter to select them.
- In the first screen, accept the default options of "ipv4" and "No", as shown below.
- Press Tab until Next is highlighted and then press Enter.



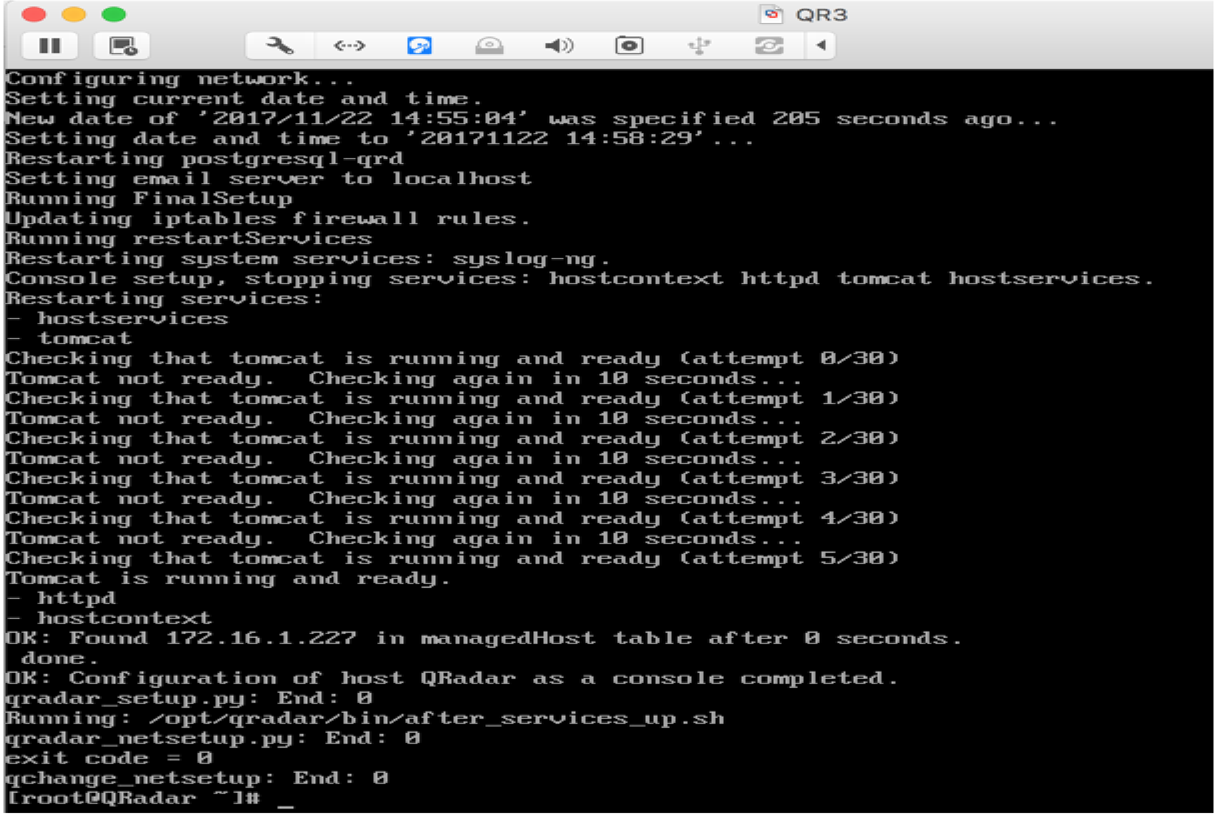
```
Internet Protocol Setup

  Choose which Internet protocol version to use:
  (X) ipv4   Internet Protocol version 4
  ( ) ipv6   Internet Protocol version 6

  Choose interface configuration mode:
  (X) No    Do not use bonded interface configuration mode

                  < Next    >  < Cancel >

QRadar 7.3.0.20171013140512 Appliance 399
```

- At the "Management Interface Setup" screen, accept default options of "ens33", as shown below.
- Press Tab until Next is highlighted and then press Enter.
- At the "Network Information Setup" screen, it should fill in with good default values. Make sure one of the DNS servers is 8.8.8.8 as shown below.
- Make a note of the server's IP address! You will need it later.
- Press Tab until Finish is highlighted and then press Enter.



```
Management Interface Setup

Select management interface:
(X) ens33 + MAC 00:0c:29:8d:15:ba

Note: If the interface has a link (cable connected), a plus (+) is
displayed before the description.

QRadar 7.3.0.20171013140512 Appliance 399
```

- Wait while the machine configures networking and restarts services, as shown below.
- Tomcat is Java-based and slow to start.
- Logging In to QRadar
- On your host system, in a Web browser, go to this URL, replacing the IP address with the IP address of your QRadar VM.
- https://172.16.1.226/console/
- Approve the self-signed certificate.



```
Configuring network...
Setting current date and time.
New date of '2017/11/22 14:55:04' was specified 205 seconds ago...
Setting date and time to '20171122 14:58:29'...
Restarting postgresql-qrd
Setting email server to localhost
Running FinalSetup
Updating iptables firewall rules.
Running restartServices
Restarting system services: syslog-ng.
Console setup, stopping services: hostcontext httpd tomcat hostservices.
Restarting services:
- hostservices
- tomcat
Checking that tomcat is running and ready (attempt 0/30)
Tomcat not ready.  Checking again in 10 seconds...
Checking that tomcat is running and ready (attempt 1/30)
Tomcat not ready.  Checking again in 10 seconds...
Checking that tomcat is running and ready (attempt 2/30)
Tomcat not ready.  Checking again in 10 seconds...
Checking that tomcat is running and ready (attempt 3/30)
Tomcat not ready.  Checking again in 10 seconds...
Checking that tomcat is running and ready (attempt 4/30)
Tomcat not ready.  Checking again in 10 seconds...
Checking that tomcat is running and ready (attempt 5/30)
Tomcat is running and ready.
- httpd
- hostcontext
OK: Found 172.16.1.227 in managedHost table after 0 seconds.
 done.
OK: Configuration of host QRadar as a console completed.
qradar_setup.py: End: 0
Running: /opt/qradar/bin/after_services_up.sh
qradar_netsetup.py: End: 0
exit code = 0
qchange_netsetup: End: 0
[root@QRadar ~]# _
```

Viewing Log Sources

- In the QRadar administration page, at the top center, click the Admin tab.

- Scroll down to the "Data Sources" section and click "Log Sources", as shown below.

- An "Add a log source" window appears. In the "Log Source Type" list box, scroll down to see "Microsoft Windows Security Event Log", as shown below.

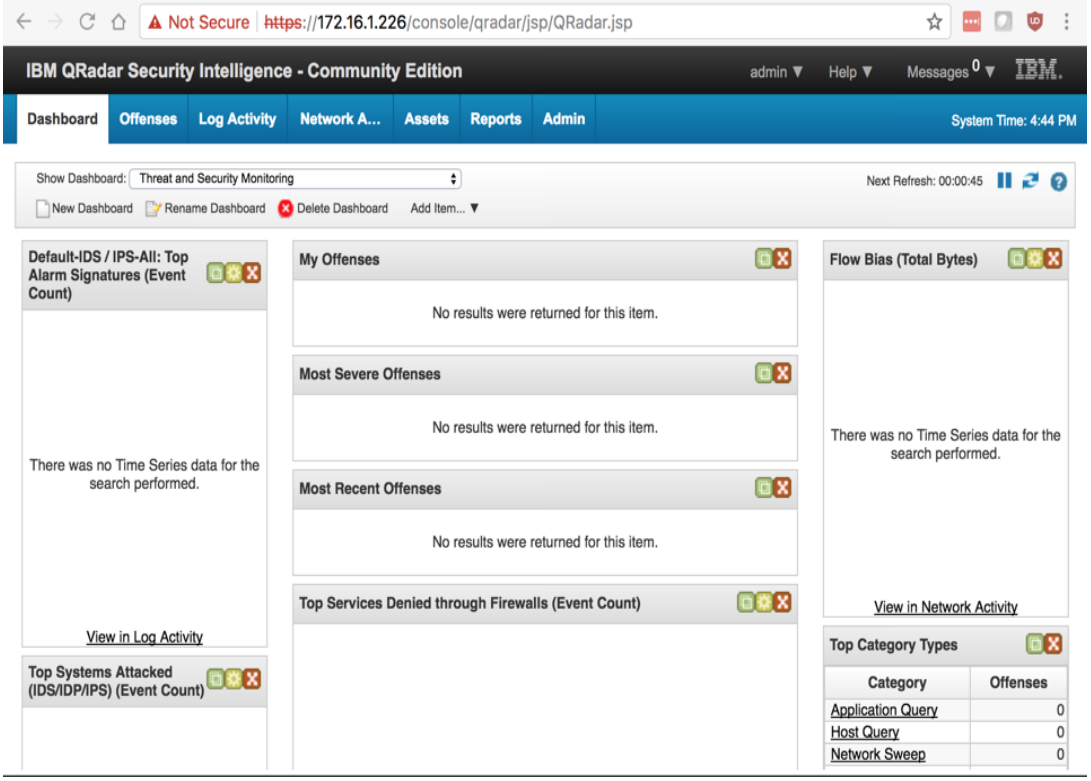
- You don't need to select it at this time; just to verify that it's there. It's not included in the default QRadar Community Edition installation, but I added it to the VM you downloaded already.

- Making an IBM Account

- In a Web browser, go to

- https://www.ibm.com/account/us-en/signup/register.html

- Create an IBM ID. You will need it to download software below.



There was no Time Series data for the search performed.

No results were returned for this item.

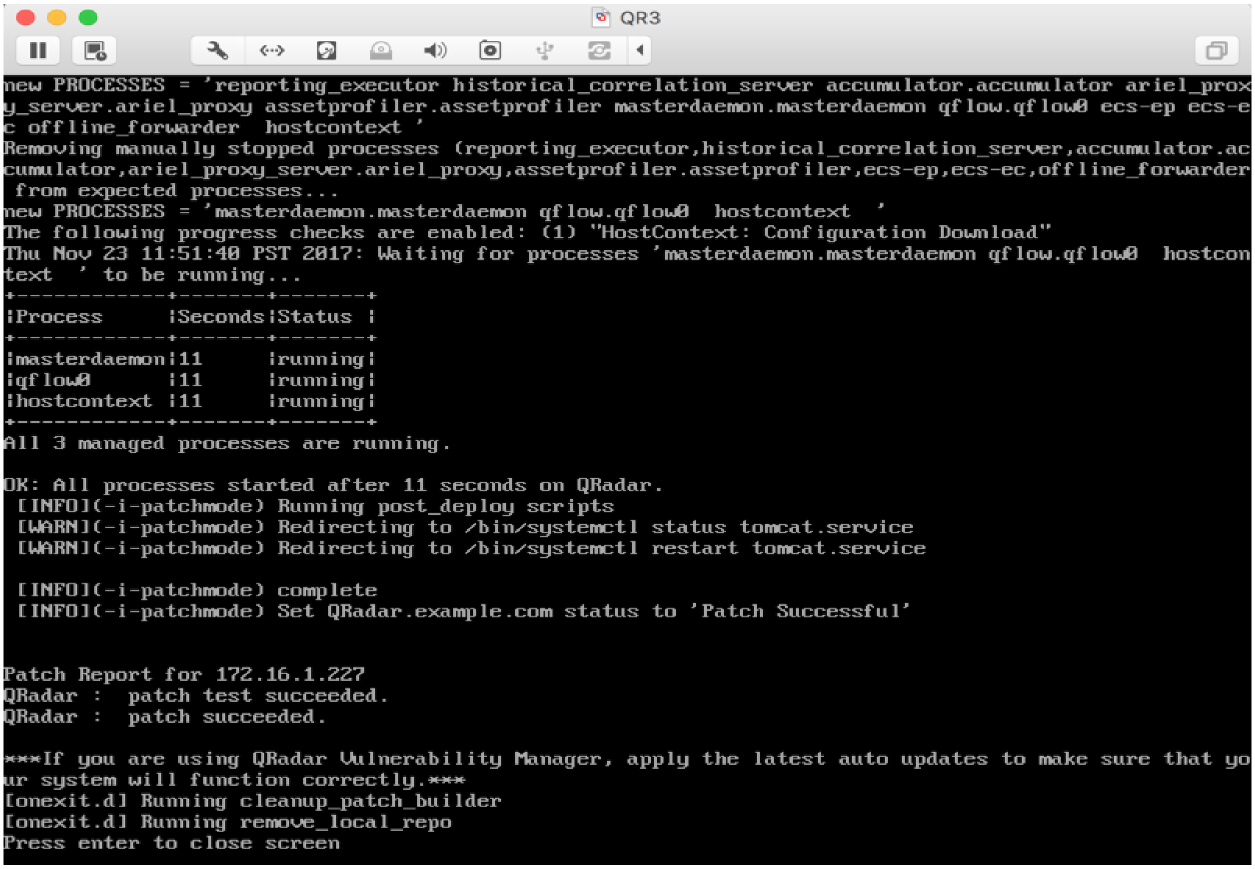
No results were returned for this item.

No results were returned for this item.

There was no Time Series data for the search performed.

Category	Offenses
Application Query	0
Host Query	0
Network Sweep	0

- Installing Software on the QRadar VM
- In the right pane of FileZilla, click the top yellow folder icon for /
- In the folder list, click /tmp
- In the left pane of FileZilla, navigate to your Downloads folder
- In your QRadar VM console, execute these commands, as shown below.
- mkdir -p /media/updates
- cd /tmp
- mount -o loop -t squashfs 730_QRadar_wincollectupdate-7.3.0.106.sfs /media/updates
- /media/updates/installer
- A message asks "Do you wish to continue?". Enter Y.



```
new PROCESSES = 'reporting_executor historical_correlation_server accumulator.accumulator ariel_prox
y_server.ariel_proxy assetprofiler.assetprofiler masterdaemon.masterdaemon qflow.qflow0 ecs-ep ecs-e
c offline_forwarder  hostcontext '
Removing manually stopped processes (reporting_executor,historical_correlation_server,accumulator.ac
cumulator,ariel_proxy_server.ariel_proxy,assetprofiler.assetprofiler,ecs-ep,ecs-ec,offline_forwarder
 from expected processes...
new PROCESSES = 'masterdaemon.masterdaemon qflow.qflow0  hostcontext  '
The following progress checks are enabled: (1) "HostContext: Configuration Download"
Thu Nov 23 11:51:40 PST 2017: Waiting for processes 'masterdaemon.masterdaemon qflow.qflow0  hostcon
text  ' to be running...
+-------------+-------+-------+
|Process      |Seconds|Status |
+-------------+-------+-------+
|masterdaemon|11      |running|
|qflow0       |11     |running|
|hostcontext |11      |running|
+-------------+-------+-------+
All 3 managed processes are running.

OK: All processes started after 11 seconds on QRadar.
 [INFO](-i-patchmode) Running post_deploy scripts
 [WARN](-i-patchmode) Redirecting to /bin/systemctl status tomcat.service
 [WARN](-i-patchmode) Redirecting to /bin/systemctl restart tomcat.service

 [INFO](-i-patchmode) complete
 [INFO](-i-patchmode) Set QRadar.example.com status to 'Patch Successful'


Patch Report for 172.16.1.227
QRadar :  patch test succeeded.
QRadar :  patch succeeded.

***If you are using QRadar Vulnerability Manager, apply the latest auto updates to make sure that yo
ur system will function correctly.***
[onexit.d] Running cleanup_patch_builder
[onexit.d] Running remove_local_repo
Press enter to close screen
```

- In your Web browser, log in to the QRadar GUI again with the credentials admin and P@ssw0rd

- Click the Admin tab.

- A message says "There are no changes to deploy". This is contrary to the IBM patch Release Notes, which say that a manual deploy and release is required after the patch. However, the console showed that this patch automatically performed those steps already.

- This is typical for enterprise-class software patches--you can't always rely on the documents being accurate.

- Deleting the Patch File

- In FileZilla, in the right pane, left-click the 730_QRadar_wincollectupdate-7.3.0.106.sfs, then right-click it and click Delete. Click Yes to delete it.

- Installing Wincollect on the Windows System
- Copy the appropriate version of Wincollect from your host machine's Downloads folder to your Windows machine.

- For 32-bit Windows: wincollect-7.2.7-20.x86.exe
- For 64-bit Windows: wincollect-7.2.7-20.x64.exe

- Start the installer. Accept the default selections until you see the "Setup Type" box.

- Click "Stand Alone, as shown below, and then click Next.

- In the next box, accept the default Machine poll interval and click Next.

- In the "Heartbeat Parameters" box, accept the default options and click Next.

- In the "Installation Parameters Summary" box, click Next.

- Click Install.

- Click Finish.

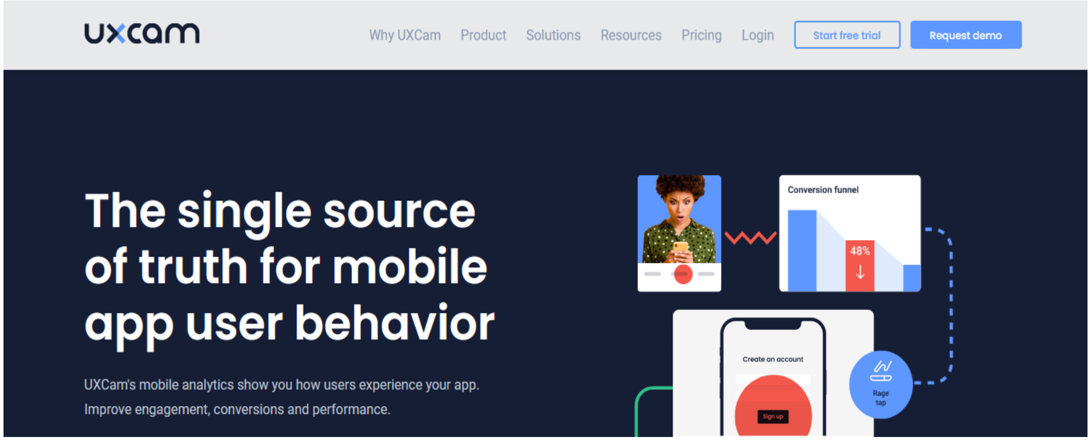
SOC DASHBOARD DEVELOPMENT:

What is soc?

- This SOC dashboard is a data-centric application that allows you to interact with and analyze a dataset, with each row representing a unique object.

- You can develop SOC dashboard with many tools available.

- One of the tool here using is UI/UXCAM.

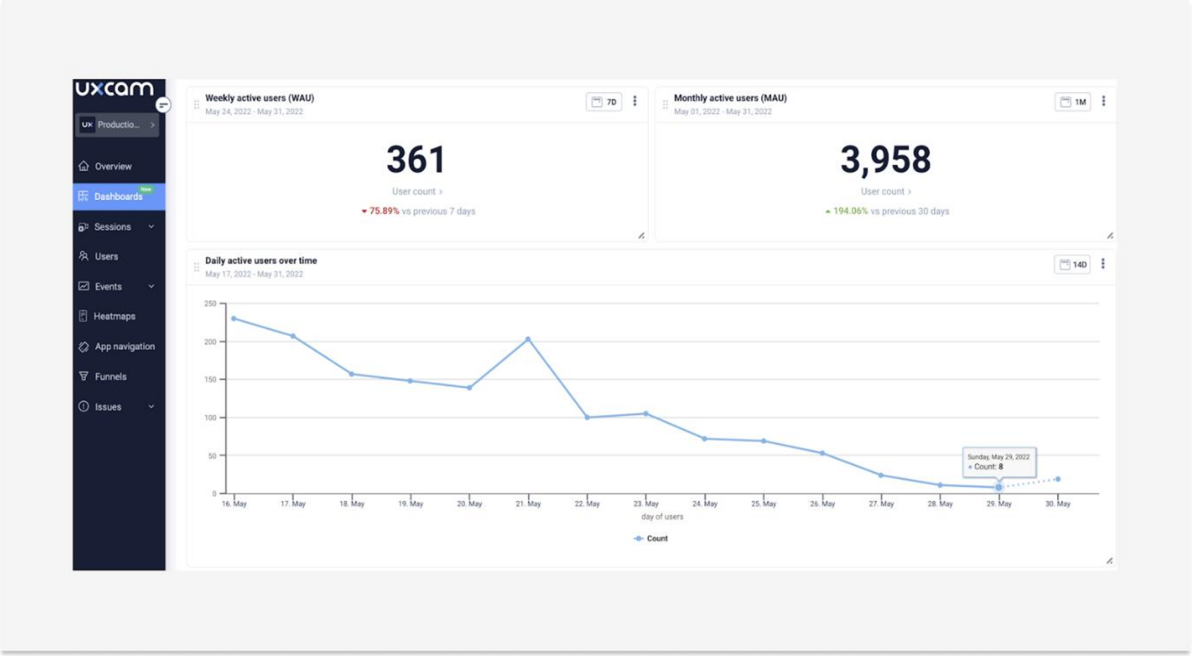


The single source of truth for mobile app user behavior

UXCam's mobile analytics show you how users experience your app. Improve engagement, conversions and performance.

View Of KPIs:

- **Key performance indicators** (KPIs) are an effective way to measure the success of any program (including cybersecurity) and aid in decision-making.



Weekly active users (WAU)
May 24, 2022 - May 31, 2022

361
User count ›
▾ 75.89% vs previous 7 days

Monthly active users (MAU)
May 01, 2022 - May 31, 2022

3,958
User count ›
▴ 194.06% vs previous 30 days

Daily active users over time
May 17, 2022 - May 31, 2022

Sunday, May 29, 2022
● Count: 8

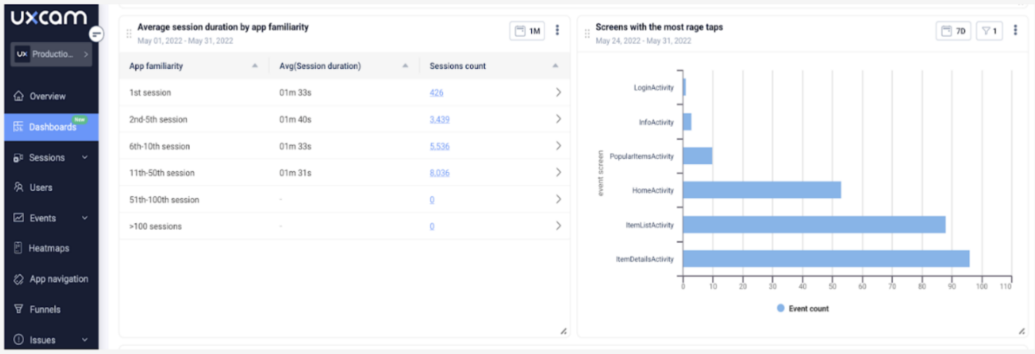
- For product teams, it's really important that KPIs tell the complete story of product usage and performance. Not only from a tech standpoint but also from the value that it gives to the customers.

- KPIs like Number of sessions per user, Session duration, Retention Rate, Daily active users (DAU), Monthly active users (MAU) etc. gives the engagement level of the product with the user. This is the front end of the product.

- Examples of new users by acquisition source, returning users after first visit by acquisition source, app version adoption.

Here's an example of some KPIs you can build on your dashboard.

- Weekly active users
- Monthly active users
- Daily active users over time
- Users by country
- Users by gender
- New users by acquisition source
- Users returning after first visit by acquisition source
- App version adoption
- Top events by occurrence
- Total visited screens
- Top device models among your users
- Average session duration by ap familiarity
- Screens with the most rage taps
- Conversion based on type of membership (loyalty vs regular)
- Average purchase value per age group

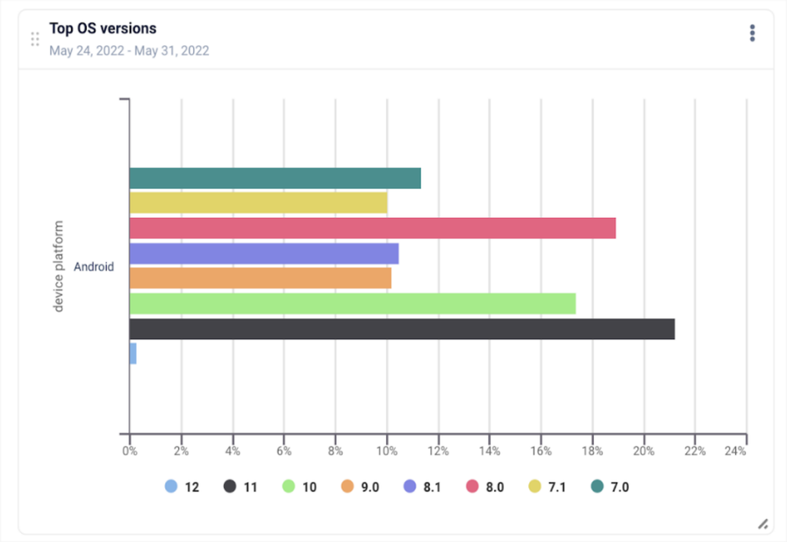


Average session duration by app familiarity
May 01, 2022 - May 31, 2022

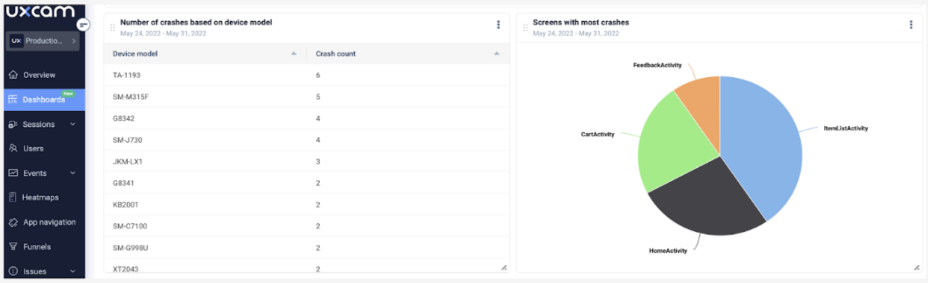
App familiarity	Avg(Session duration)	Sessions count
1st session	01m 33s	426
2nd-5th session	01m 40s	3,439
6th-10th session	01m 33s	5,536
11th-50th session	01m 31s	8,036
51th-100th session	-	0
>100 sessions	-	0

Screens with the most rage taps
May 24, 2022 - May 31, 2022

- Setting the maintenance of these are your KPIs and also lets you observe how your app behaves in real scenarios, as opposed to controlled testing settings



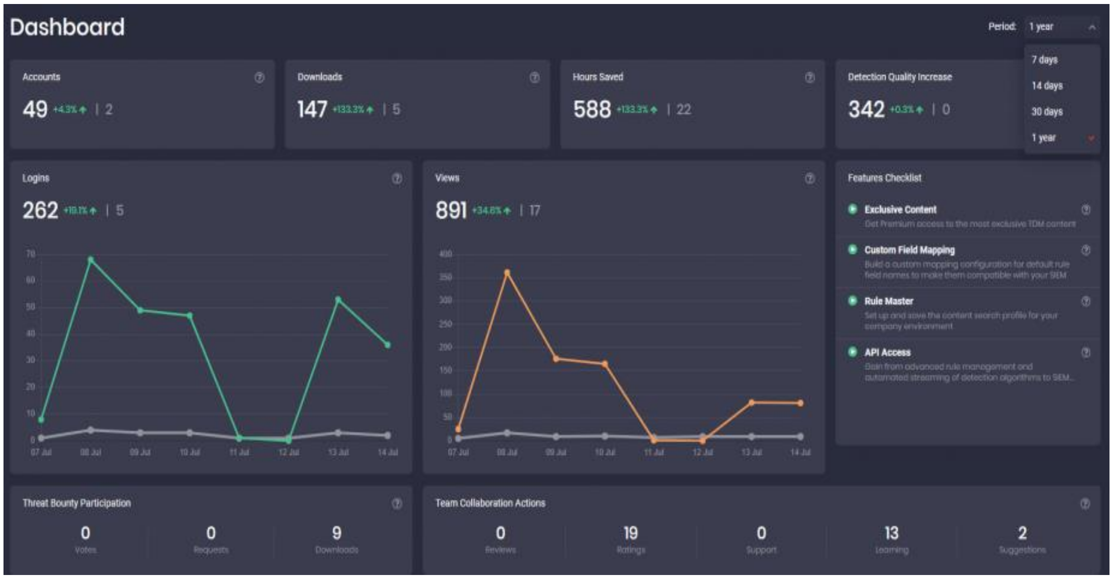
- In general, engineering is a pretty broad category so we're just going to generalize here with engineers who work on maintaining a mobile app and ensuring its performance. Engineering managers use these metrics to measure the progress to keep their teams on schedule.



Number of crashes based on device model
May 24, 2022 - May 31, 2022

Device model	Crash count
TA-1193	6
SM-M315F	5
G8342	4
SM-J730	4
JKM-LX1	3
G8341	2
KB2001	2
SM-C7100	2
SM-G998U	2
XT2043	2

- The SOC Prime TDM platform has already represented the Leaderboards page covering the general SOC Prime TDM statistics on top authors, content release dynamics, MITRE ATT&CK® coverage, leading platforms by rule count, and other data in numbers.
- By default, all company statistics are displayed for the annual period, but can also be filtered by a less lengthy time frame — from a monthly period to a range of 7 days



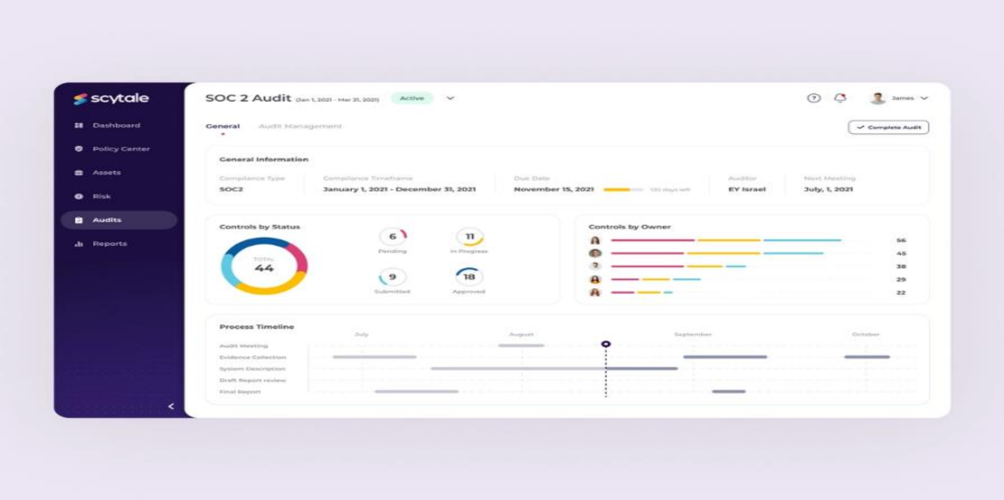
Exclusive Content
Get Premium access to the most exclusive TDM content

Custom Field Mapping
Build a custom mapping configuration for default rule field names to make them compatible with your SIEM

Rule Master
Set up and save the content search profile for your company environment

API Access
Gain from advanced rule management and automated streaming of detection algorithms to SIEM...

- Design your dashboard. How do you want to visualize your data? What kind of charts and graphs will be most effective for you?
- You will need to consider the needs of your SOC analysts and make sure that the dashboard is easy to use and understand.



SOC 2 Audit (Jan 1, 2021 - Mar 31, 2021) Active

General Information

Compliance Type	Compliance Timeframe	Due Date	Auditor	Next Meeting
SOC2	January 1, 2021 - December 31, 2021	November 15, 2021	EY Israel	July, 1, 2021

Controls by Status

TOTAL 44

6 Pending

11 In Progress

9 Submitted

18 Approved

Controls by Owner

56

45

38

29

22

Process Timeline

Audit Meeting

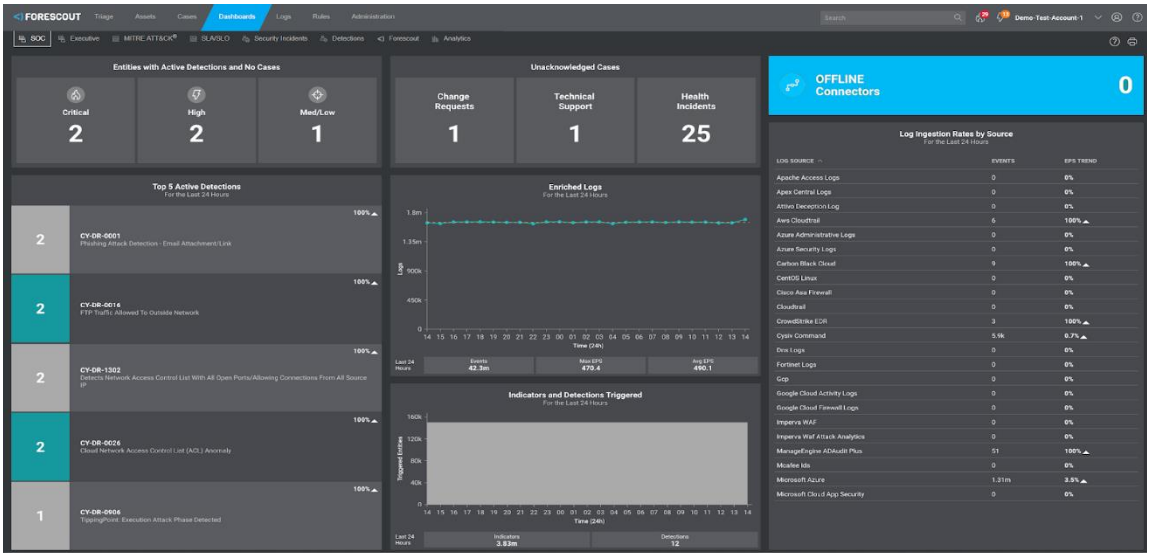
Evidence Collection

System Description

Draft Report review

Final Report

- Configure your dashboard. Once you have designed your dashboard, you will need to configure it to track your KPIs. This will involve setting up alerts, thresholds, and visualizations.



Entities with Active Detections and No Cases

Critical	High	Med/Low
2	2	1

Unacknowledged Cases

Change Requests	Technical Support	Health Incidents
1	1	25

OFFLINE Connectors 0

Top 5 Active Detections
For the Last 24 Hours

2 CY-DR-0001 Phishing Attack Detection - Email Attachment/Link 100% ▲

2 CY-DR-0016 FTP Traffic Allowed To Outside Network 100% ▲

2 CY-DR-1302 Detects Network Access Control List With All Open Ports/Allowing Connections From All Source IP 100% ▲

2 CY-DR-0026 Cloud Network Access Control List (ACL) Anomaly 100% ▲

1 CY-DR-0906 TippingPoint: Execution Attack Phase Detected 100% ▲

Enriched Logs
For the Last 24 Hours

Last 24 Hours	Events	Max EPS	Avg EPS
	42.3m	470.4	490.1

Indicators and Detections Triggered
For the Last 24 Hours

Last 24 Hours	Indicators	Detections
	3.83m	12

Log Ingestion Rates by Source
For the Last 24 Hours

LOG SOURCE	EVENTS	EPS TREND
Apache Access Logs	0	0%
Apex Central Logs	0	0%
Attivo Deception Log	0	0%
Aws Cloudtrail	6	100% ▲
Azure Administrative Logs	0	0%
Azure Security Logs	0	0%
Carbon Black Cloud	9	100% ▲
CentOS Linux	0	0%
Cisco Asa Firewall	0	0%
Cloudtrail	0	0%
CrowdStrike EDR	3	100% ▲
Cysiv Command	5.9k	0.7% ▲
Dns Logs	0	0%
Fortinet Logs	0	0%
Gcp	0	0%
Google Cloud Activity Logs	0	0%
Google Cloud Firewall Logs	0	0%
Imperva WAF	0	0%
Imperva Waf Attack Analytics	0	0%
ManageEngine ADAudit Plus	51	100% ▲
Mcafee Ids	0	0%
Microsoft Azure	1.31m	3.5% ▲
Microsoft Cloud App Security	0	0%

- **Finally,** Test and refine your dashboard. Once your dashboard is configured, you will need to test it to make sure that it is working properly. You should also refine the dashboard based on feedback from your SOC analysts.
- Last but not least, raise awareness and educate everyone involved, company internal or external, about the risks — crucial for any cybersecurity strategy to be effective. Just consider that 95% of data breaches are caused by human error.

Conclusion:

A comprehensive approach to mobile app and cybersecurity monitoring involves tracking not only user engagement metrics but also technical performance indicators. The SOC Prime TDM platform offers a robust solution for threat detection, and its dashboard provides valuable insights into company-wide activities. To enhance cybersecurity, organizations should not only focus on technological aspects but also implement risk and crisis management plans, constant environmental scanning, and awareness and education initiatives to mitigate the human factor in data breaches. The integration of these strategies contributes to a holistic and proactive cybersecurity posture for organizations.

THANK YOU