SISA

SISA TOP 5

2022 - 2023

Forensic Driven Learnings

Table of
Contents

Foreword **03**
Executive Summary **05**
Introduction **06**
Trends Observed in Our Forensic Investigations **07**
Ingress Trends **07**
Phishing Attack and Deployment of the Malware 07
Web Application Exploit 08
Unknown Exploit 09
Compromise of VPN Credentials and Access via VPN 09
Ingress from Third Party Network 09
Compromised Cloud Credentials / Access keys 09
Compromised SaaS Application Credentials 09
Lateral Movement Trends **10**
OS Credential Dumping Technique 10
Exploit of Unsecured Credentials 11
Malware which Exploits the Credentials Stored in Password Stores 11
Use of Defense Evasion Mechanisms 11
Use of Discovery Techniques 12
Action on Objective Trends **13**
Synchronized Ransomware Attack 13
Social Engineering Attack On the End Customer 13
Balance Modification Attack 13
Cause vs. Contribution Factors **14**
SISA Top 5 Learnings **15**
Secure Vulnerable Loopholes 15
Strengthen Endpoint Response 17
Deploy Intelligent Monitoring 18
Set up Diligent Access Management 19
Execute Proper Incident Response and Forensics 20
About SISA Forensic Learning Session **21**
References **21**

Foreword

World over, data breaches are soaring despite an ever-increasing investment in cybersecurity tools and technologies. A host of factors ranging from exponential growth in the volume of data, rising adoption of APIs, distributed IT landscape, acceleration of digital transformation, and increasing lucrativeness of cybercrime, are fueling this surge. As intruders weaponize AI/ML tools to exploit vulnerabilities across IT infrastructures, it is imperative for organizations to outsmart even the most sophisticated intruder.

The SISA Top 5 Forensic Driven Learnings report with its in-depth view of prevalent intruder tactics and techniques, provides learnings based on real-world experience of its forensic practitioners. This blend of learnings from observed attack patterns with practitioner led insights to improve resilience, is a valuable read for any organization looking to enhance its cybersecurity posture.

Lt General (Dr) Rajesh Pant
National Cybersecurity Coordinator,
Prime Minister's Office, Government of India

The SISA Top 5 Forensic-driven Learnings 2022-23 report will be a valuable read for many CISOs and their teams, especially as it is based on real world experience from SISA in carrying out their forensic investigations, compliance audits and incident response cases. Highly recommend all CISOs study and adopt the best practices highlighted in this report to help build resilience to ransomware and breaches and improve the overall security posture of their enterprise.

Brian O'Higgins
Cybersecurity Technology Evangelist,
Canada

Compliments to SISA team in publishing their 3rd edition of Top 5 Forensic Driven Learnings 2022-23. The report is insightful for CISOs and their teams, and has a practitioner-led approach based on the team's forensic investigations, compliance audits and incidents response conducted over close to two years. The report reinforces that phishing and web application vulnerability exploits continue to be a big cause for breaches. Given the widespread use of credential harvesting tools, compromised cloud credentials and of SaaS applications, the report highlights the need for Zero Trust and adopting best practices of password vaults and MFA. I also endorse the recommended best practice of Forensic Readiness Audits.

Rama Vedashree
CEO, Data Security Council of India

Executive **Summary**

As the cyber threat landscape continues to evolve dynamically and the attack surface constantly expands, enterprises worldwide are falling victim to rising data breaches. The fact that data breaches are increasing both in frequency and complexity further adds to the cybersecurity challenges of CISOs and CIOs. With **15+ years of industry presence** in cybersecurity and as one of the top 4 global PCI forensic investigators, SISA brings vast domain knowledge and experience from conducting **1,000+ client engagements every year.** The SISA Top 5 Forensic Driven Learnings report brings out SISA's learnings from forensic investigations, compliance audits, security operations, and incident response activities performed between **April 1, 2020, and December 31, 2021.**

This year's report offers an in-depth view of the most prevalent intruder tactics and techniques broken down by each stage of the breach life cycle while also encapsulating top **trends observed over the past 1.5 years**. Importantly, it presents SISA's learnings from the real-world experience gained by our forensic practitioners from observing the pattern of attacks.

Key Findings from the Report Include:

- The frequently used vector to gain initial access is phishing attacks and malware deployment – **observed in nearly 43% of cases.**
- Intruders are increasingly targeting applications hosted in the **User Acceptance Testing (UAT) environment** and/or **non-critical applications** like the Human Resources Management System (HRMS), travel portals, etc., for deploying web application exploits.
- The use of credential harvester tools like Mimikatz and its various variants is a popular technique that intruders use to perform lateral movement.
- Lack of patching/application security is a key factor causing **27% of breaches** and **46%** of the time serving as a contributing factor. This is followed by inadequate antivirus (AV) and access control resulting in **11% of the breaches** and **contributing to 41%** of them.
- The **dwell time** of intruders on **average is 180 days**, which underscores the need for enterprises to employ preliminary forensics to contain the breach's impact.

The findings and insights from the report can offer valuable inputs towards creating a robust, secure and compliant enterprise ecosystem. **Here are the top reasons why every CISO should read this report:**

To redefine your **cybersecurity posture** and make it a priority to reduce your attack surface

To get a deeper understanding of the **HOW and WHY of data breaches**

To create a set of well-defined measures to **improve cyber resilience**

The report offers an in-depth view of the **most common exploits and intruder actions,** features detailed commentary on trends observed across the **attack lifecycle**, and highlights top factors driving **global data breaches.**

Introduction

The ever-increasing interconnected and perimeter-less networks, the accelerated migration to the cloud, and the distributed remote working model induced by the Covid-19 pandemic, have added more complexity to the rapidly evolving cyber threat landscape. Also, the rapid digital transformation undertaken by organizations accompanied by the proliferation of data in the cloud has increased the area of the cyber-attack surface, opening up the organization to new vulnerabilities. The statistics related to the rapid rise of cyberattacks are staggering. The total number of data breaches until **Q3 2021 already surpassed the total number in 2020 by 17%, with 1,291 breaches in 2021 compared to 1,108 breaches in 2020[1].** Additionally, the average total cost of a data breach has increased nearly **10% to $4.24 million[2] over the last year.**

These breaches are soaring despite an ever-increasing investment in cybersecurity tools and technologies. While enterprise spending on cybersecurity is expected to rise across the board, a majority (78%) of senior IT and security leaders believe that their organizations lack sufficient protection against cyberattacks[3].

So, what is causing the chasm between these alarming rates of incidents that enterprises face compared to their investments? We believe a host of factors, ranging from exponential growth in the volume of data, rising adoption of **APIs and interfaces** widening the attack surface**, distributed IT landscape,** acceleration of **digital transformation,** and increasing lucrativeness of cybercrime, are fueling the surge in breaches. Besides, advancement in technology is aiding intruders to weaponize **AI/ML tools to exploit vulnerabilities across IT infrastructure** and outsmart even the most sophisticated cyber defenses.

The pandemic-induced shift to remote and hybrid work models has opened the floodgates to phishing and ransomware attacks. **80%** of organizations experienced a successful email-based phishing attack in 2021 – a startling **45% increase over 2020[4].** Cyber attackers have been exploiting the **'bare minimum'** security default settings present in various online collaboration and productivity tools to successfully launch email phishing attacks. This, coupled with the lack of cybersecurity training, non-deployment of antivirus (AV) software on work-issued devices, and employee distraction associated with remote working, has offered added ammunition to cybercriminals. Ransomware attacks, too, have seen a dramatic leap, with the total number of attacks jumping **105% during 2021 compared to 2020[5].**

Another fallout of the remote/hybrid work model is the rise in **insider threats**. Insider threat incidents have risen **44% over the past two years to 6,803,** with costs per incident up more than a third to **$15.38 million**[6]. Notably, **56%** of incidents reported were due to employee or contractor negligence[6]. In addition, the increasing amount of data stored and rapid transition to the cloud is making detection of insider threats harder, prompting organizations to deploy User Behavior Analytics and Data Loss Prevention tools.

Even as the pandemic itself recedes into something resembling an endemic, some of the newly adopted models and practices are likely to stay for longer – leaving behind a significant amount of sensitive data on company premises. As a result, organizations will need to shore up data control frameworks and strike a proper balance between access, security, and privacy to minimize leaks and exposure. That apart, adopting a **data fabric** architecture can help automate data discovery, governance, and consumption across hybrid and multi-cloud environments – an essential element in building strong cyber defenses.

Trends observed in our **Forensic Investigations**

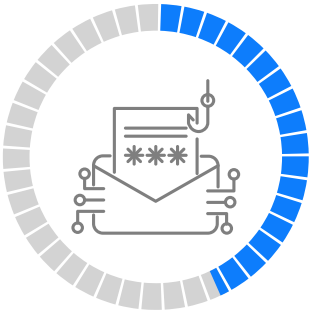
MITRE created the **MITRE ATT&CK framework** to document attackers' tactics and techniques used in a breach. To simplify the attacker/intruder tactics, we have condensed the entire **MITRE ATT&CK** framework tactics into three categories. They are the Ingress Point, Lateral Movement, and Action on Objective.

The Ingress Point deals with how the intruder can compromise the network and gain a foothold into the environment. The Ingress Point covers the first four tactics outlined in the **MITRE ATT&CK** framework. While investigating, we capture details of how the attacker deploys tactics to gain initial access. The Ingress Point also covers the steps used by the intruder to gain a persistent foothold within the network, which covers the techniques mentioned in the **MITRE Persistence tactics.** Unfortunately, it is rare for us to ascertain the tactics used by the intruder for reconnaissance and resource development.

Once the intruder gets a foothold in the network, the intruder is looking to make a Lateral Movement to access other systems of interest, primarily because the initially compromised system may not have sensitive or confidential data. The Lateral Movement can cover various tactics such as **Privilege Escalation, Defence Evasion, Credential Access, Discovery, Collection, Command, and Control - the tactics mentioned** in the MITRE ATT&CK framework. After the intruder gains access to the systems of interest, the intruder executes the last phase, Action on Objective. The Action on Objective covers the exfiltration and impact tactics defined in the MITRE ATT&CK.

As part of every forensic investigation we carry out, we collate the various methods through which the intruders have gained access to the system, performed lateral movements, and met their Action on Objective. Based on these details, we have shortlisted the common methods used by intruders under the following sections.

MITRE created the **MITRE ATT&CK** Framework in **2013** to **document attackers' tactics and techniques used in a breach.**



In almost **43%** of the cases we have investigated, **phishing is the primary method used,** to compromise the environment.

Ingress trends

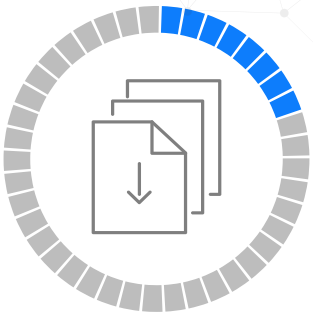
The ingress point or the initial access to system zero of the compromised environment can happen using different methods. We have identified the following frequently used methods during our forensic investigations.

Phishing Attack and Deployment of the Malware

In almost **43%** of the cases we investigated, phishing is the primary method used, to compromise the environment. In the instances where we retrieved the phishing email, **23% had a malicious file attachment,** while the rest contained URLs to sites that hosted malicious content.

One interesting trend that we've observed while analyzing phishing emails is that they originate from **trusted email IDs,** i.e., from colleagues or third parties present in the user's contacts. We found malware-embedded attachments in **23% of the total phishing cases.** In the remaining cases, it was a URL redirect. In **70% of the emails** that we were able to retrieve as part of our forensics, the link was encoded either in the PDF, Docx, txt, PPT, or similar format, and the phishing link did not exist in the email body.

Usually, only the initial malware deployed is downloaded, enabling the intruder to download additional malware. This additional malware allows the intruder to create a persistent connection to the system and network.



We found malware-embedded attachments in **23%** of the total phishing cases.

Web application exploit

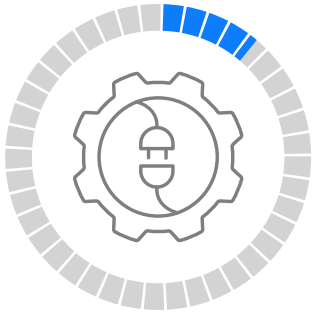
The other major Ingress Point is via web application exploits. The vulnerabilities that the intruder exploits for deploying a web shell include **SQL injection vulnerability,** malicious file upload vulnerability, exploitation of vulnerable libraries, and OS injection vulnerability. As part of our incident response activities, we have observed many web applications exploiting other web app vulnerabilities. These exploits are often used to gain access to the application and may not lead to deploying a web shell or remote access tool to the network.

Another point of interest concerning web application exploits is that applications hosted in the **User Acceptance Testing (UAT)** environment, non-critical applications like the Human **Resources Management System (HRMS),** travel portals, and company intranet sites, are being actively exploited for deploying the web shell. Most of these applications, mainly available or accessible only via the intranet, were exposed to the internet for the employees to access during the pandemic. Further, these applications were not tested regularly to identify vulnerabilities, neither were the applications deployed behind a **Web Application Firewall (WAF).**

The webshell is a kind of remote tool that can be accessed via a browser, through which the intruder can gain complete access to the server and execute any commands. In almost **11%** of the investigations where a webshell was identified, we found that the compromise was through a vulnerability present in the API used by the clients.

Interestingly, in all our investigations over the past **1.5 years**, the initial access into the environment via a web-based application exploit was mainly identified in the UAT environment or the non-critical **virtual local area networks (VLANs)** rather than an application hosted in the production or **critical demilitarized zone (DMZ).**

However, in **January 2022,** we witnessed an uptick in the number of incident responses on the production servers. All these incident response activities were due to the Log4j exploits carried out by the intruder on the application servers. We expect this trend to strengthen and anticipate increased compromises due to the ubiquitous nature of **Log4j in applications** globally.

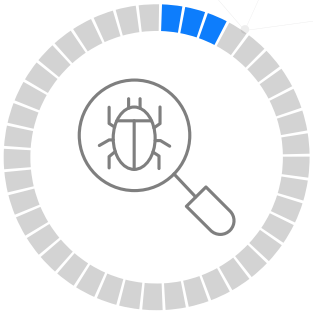


In almost **11%** of the investigations where a web shell was identified, we found that the compromise was through a **vulnerability present in the API used by the clients.**

> We anticipate **increased compromises due** to the ubiquitous nature of **Log4j in applications globally.**

Unknown exploit

In around 8% of our investigations, we identified the initial system (system zero) that was exploited by the intruder but could not identify how the particular server/system was exploited. Many vulnerabilities associated with Apache, Windows exchange server, etc., were identified in the past year.



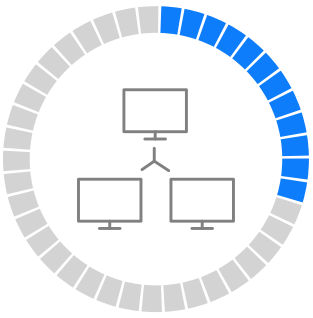
Compromise of VPN credentials and access via VPN

In around 4% of our investigations, we ascertained that the intruder accessed the client environment via a compromised **virtual private network (VPN)** credentials. Unfortunately, the client had not used out-of-band **Multi-Factor Authentication** (MFA) for the VPN access.

In around **4%** of our investigations, we ascertained that the intruder accessed the client environment via compromised Virtual Private Network (VPN) credentials.

Ingress from third-party network

In 30% of the investigations, we have observed the initial compromise occurred via a connected third-party network. The intruder had compromised the third-party network and accessed the client production environment to plant remote back doors via lateral movement. We found that these were compromised via a phishing email or VPN credentials of the third-party networks.



Compromised cloud credentials / Access keys

Due to the pandemic, many of our clients adopted a hybrid model to host their systems in various cloud platforms. SISA's investigations have revealed the following common ingress points for the cloud environment:

1. **Compromise of cloud account credentials** happened via the user laptop whose credentials were compromised and contained a keylogger or another type of malware. Another reason cloud user accounts were compromised was because the clients had **not enabled MFA** to log in to the cloud console.
2. Another trend that we observed was that cloud keys stored in the user's laptop were compromised in several cases. Using the **cloud private keys,** the intruders were able to access the cloud accounts of the clients.

In **30%** of the **investigations** we carried out over the past **1.5 years,** the initial compromise occurred **via a connected third-party network.**

Compromised SaaS application credentials

Many clients use **SaaS applications for their day-to-day business** activities. Applications like **CRM, Bank on the Cloud, etc.,** are being used to service the end customer. Intruders are compromising the client employee systems to gain access to credentials of various SaaS applications. These credentials are then used to download or gather the data stored in the applications.

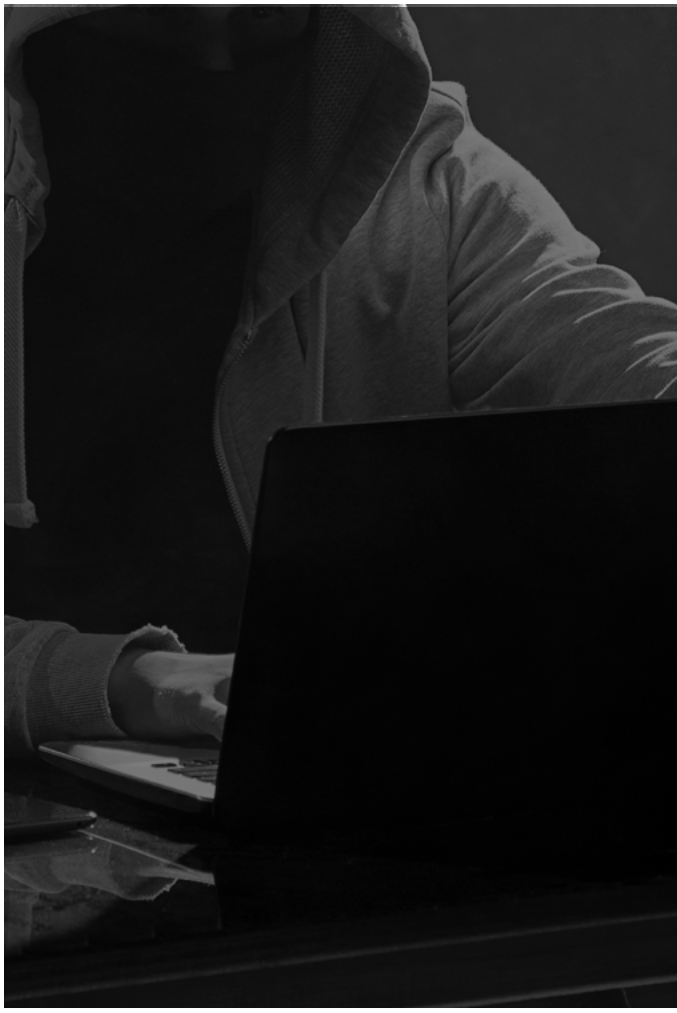
Missing security controls that led to initial ingress

As per our forensics investigations, not having the right security in place to address the below-mentioned issues, and is a key reason for the initial ingress:

- **Timely patching** of systems
- **AV** not present in the **targeted system**
- The **inability** of the AV to quarantine or delete the file
- Exposing web interfaces and APIs without any WAF
- Lack of **monitoring and incident response** activity on the work-from-home (WFH) systems
- **Vulnerable** web applications

Lateral movement trends

Once the intruders gain access to the network, they look to escalate the privilege, gain credential access, try defense evasion techniques, and do a lateral movement to discover the systems of interest. In all our investigations, we have **not identified the intruder conducting a brute force attack for credential access.** Instead, the following processes were observed to have been used by the intruder to access the credentials.



OS credential dumping technique

Use of credential harvester tool like **Mimikatz** is widely used to get credential details. Although Mimikatz is an old malware, we continue to identify various variants of this malware used by the intruder for credential harvesting. As per the antivirus logs, the AV was able to identify the variants of the malware as suspicious files, but unfortunately, the AV was unable to either delete or quarantine the files.

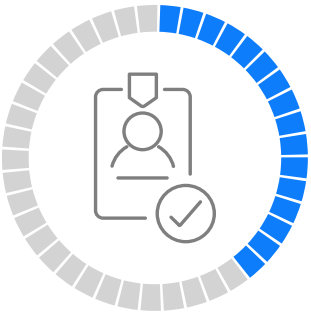
Another credential harvesting technique observed is where the intruder dumps the entire **Local Security Authority Server Service (LSASS)** process and retrieves the credentials.

Exploit of unsecured credentials

In almost **40% of our forensic investigation cases,** we have identified that the client administrator teams kept either a text, scripts or document file containing the credentials to various user accounts such as the common user account, service account, DBA, etc. We have identified the files containing the credentials on the systems, which was confirmed as also accessed by the intruder. Through the logs review and discussion with the client team, SISA confirmed that the unauthorized access observed was made using the credentials present in these files.

Another vulnerability we observed during the investigation is the **storage of the database connection string containing** the DB credentials in the web configuration file of the web server and application server.

As a general practice by the client's administrator team, we usually see that the client administrator team creates individual user accounts; however, the **generic/shared/group accounts** are also present in the system. In many instances, we have identified that the generic/shared/group accounts were used for regular **business-as-usual (BAU)** activities. Using such accounts for BAU activities lacks accountability and hence is a soft target for the intruder. As a result, the intruder generally targets these types of accounts or service accounts to remain out of sight.



In almost **40%** of our forensic investigation cases, we have identified that the **client administrator teams kept either a notepad** or **an excel file containing the credentials** to various user accounts like the common user **account, service account, DBA, etc.**

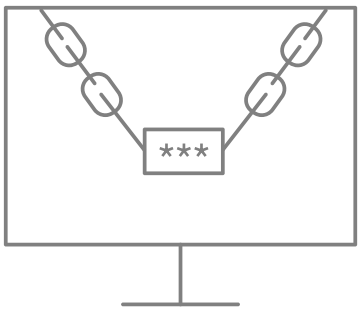
Malware which exploits the credentials stored in password stores

During the investigations and malware reverse engineering, we have observed that the malware, which captures the data via the keylogger (input capture technique) and captures the credentials via the passwords, is stored in the Security Memory and Windows Credential Manager.

Use of defense evasion mechanisms

Our observations indicate the use of the same applications that the administrator uses for **day-to-day activities**; for example, **psexec application, Mosh, autossh, sysdig, Netcat, RSAT, AD LDS set of tools, Dfsutil, Dfscmd,** etc. Intruders use these commonly used applications by the administrators to evade defense mechanisms. Most of these applications will be white-listed in the EDR solutions or usually signed by the OS providers. Hence, the intruder uses these applications to perform a lateral movement to go undetected by AV or EDR solutions.

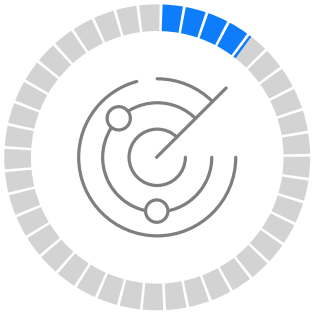
In the case of a Windows environment, we have mainly observed the use of **PowerShell and psexec** applications by the intruder to perform lateral movements or for file-sharing within the environment.



Use of discovery techniques

In most cases, we have observed that the intruders have used the basic netstat and ping request to identify the devices within the network. In **less than 10% of the cases**, we have observed the presence of a network scanning tool for mapping the network. Any network scanning generates traffic noise. This might be one of the reasons we are not seeing any significant scanning activity carried out by the intruder for mapping the network.

The other commonly used utilities by the intruder for mapping the network are **'AdFind'** and **'Net.'** Net utility is a Windows operating system component and can be used for gathering system and network information and lateral movement. The executables that we have observed for net utility are **'net1.exe'** and **'net.exe.'** AdFind utility is a command-line query tool used to gather information from the active directory.



In less than **10%** of our cases, we have observed the presence of a **network scanning tool** for mapping the network.

Lapses that led to lateral movements

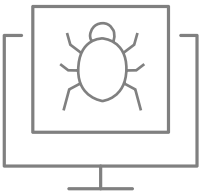
Not properly segmenting the **VLAN** thereby enabling the intruder to move from a **non-critical environment to a critical one.**

Not properly implementing **MFA;** hence, the intruder can move within the servers without entering the MFA for authenticating themselves.

Continued usage of **common user credentials and insecure practices** such as storing the credentials in a file.

Action on objective trends

Once the intruders access the critical environment, they have the endgame or the action on objective implemented. The various action on objectives that SISA has observed over the last 1.5 years are cited below.



In a **synchronized ransomware attack,** the backup copies of the images are also ingested with the malware, and when the **backup images** are bought online, the same are encrypted.

Synchronized ransomware attack

It is not the attack of encrypting one or two critical servers; instead, it is a synchronized attack where the entire data center and disaster recovery (DR) site are taken down with **ransomware attack.** The backup copies of the images are also ingested with the malware, and when the backup images are bought online, the same are encrypted.

Social engineering attack on the end customer

In this scenario, the clients' end customer gets a call stating the details of a transaction that was made in the last one hour. For example, if a consumer withdraws $100 through an ATM transaction, within an hour, he/she receives a call informing them of $1,000 transaction in an attempt to mislead the consumer. As the caller provides all the customer-related details, the end customer believes that the caller is from that financial institution. Once trust is established, the end customer is scammed with various actions on objectives such as sharing the OTP, installing a malicious application, etc. In this scenario, the intruder is within the network, and the intruder exfiltrates a copy of the transaction/customer details for scamming the end customer.

A similar example of an action on objective observed is where the intruder can compromise the credentials to **SaaS applications containing the end customer details, for example, CRM application.** Since the complete customer details are available in these SaaS applications, the intruder can use this data to scam the end customer. This type of action on objective is prevalent in both financial and non-financial institutions.

A common action on objective observed is where the intruder compromises the **credentials to SaaS applications** containing the end customer details, such as CRM, and then using this data to scam the end customer.

Balance modification attack

In this type of action on objective, the intruder opens an account with a financial institution and gets a credit, debit, or prepaid card. Once they have the card, they access the card management applications of this financial institution and change the balances of these cards. As they have a card, they can perform transactions such as withdrawing cash from the **ATM, e-commerce transactions, etc.**, as a genuine customer would do. The financial institutions can determine these fraudulent transactions only during the **end-of-day settlement.** These balance notification attacks are mainly observed on prepaid cards, forex cards, and gift cards.

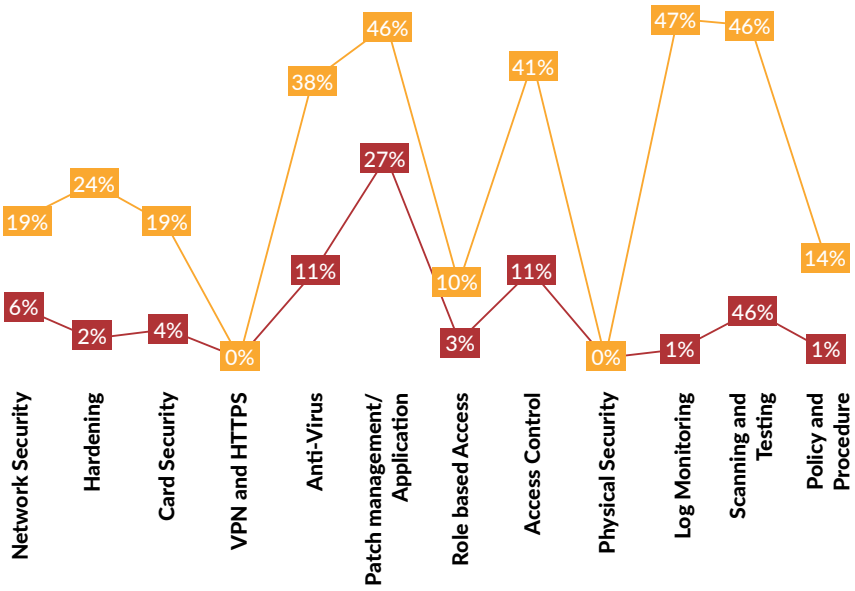
The other common action on objective attacks observed is intruders making the client data available on the **dark web** and **resorting to extortion** of ransom based on the exfiltrated data.

Cause vs. **Contribution factors**

By analyzing the findings from our forensic investigations, we have identified and classified the reasons for breaches as Causes and Contributors.

- A Cause of a breach is the failure of a best security practice that provided the attacker the initial ingress point.
- A Contributor to breach is a set of best security practices that have not been met that likely contributed to the exposure, breadth of attack, and/or ease by which the attacker(s) could move laterally within the environment. By itself, a contributing factor is not the primary cause of the breach, but when combined with other unmet requirements/ sub-requirements, it facilitated and/or contributed to the impact of the breach.

Cause vs. Contribution analysis

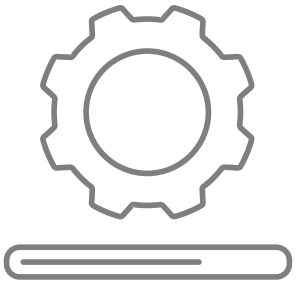


In the above graph, the blue line indicates the cause of the breach, while the orange line refers to the contributor to the breach. As part of the investigation, there can be multiple causes and contributions to a breach. As seen in the graph, a failure to implement best practices in patch management/application security results is the **highest cause (27%)** and **contribution (46%) to a breach.** The second largest cause is the lack of implementing best practices in **antivirus and access control**, leading to the initial ingress in **11% of breaches.** Further, the lack of best practices in log monitoring, scanning, and testing activities contributes to the intruder's lateral movement within the network in 46-47% of cases observed.

SISA **Top 5 Learnings**

How did we arrive at SISA Top 5?

SISA Top 5 learnings presented in this report are our learnings based on our forensic investigations and incident response activities performed between **April 1, 2020, to December 31, 2021.** As a leading forensic investigator, SISA has successfully investigated several cybersecurity breaches to understand the root cause and contain them to minimize the impact on organizations. The findings and insights are based on our domain knowledge, and the real-world experience of our forensic practitioners gathered from observing the pattern of attacks.



While **fixing all patches at once is nearly** impossible, it is critical to identify which security concerns and **software updates** are most relevant to an **organization's environment.**

Secure vulnerable loopholes

To prevent attacks from known vulnerabilities, patching continues to be one of the most critical measures that organizations must adhere to. Unfortunately, companies fall behind on patching for many reasons that range from infrastructure complexity to a shortage of staff to keep up with the ever-increasing rate of releases. Research data **indicates 18,325** common vulnerabilities and exposures in 2020, **while 2021 has seen 14,525 in the first nine months alone[7].** Vulnerabilities can be present in operating systems, applications, web applications hosted within the environment, libraries, and platforms that the organization uses. For example, Log4j vulnerability is an apt example of how a library file used by most applications across the globe can lead to vulnerability in all those applications.

While fixing all patches at once is nearly impossible, it is critical to identify which security concerns and software updates are most relevant to an organization's environment. SISA has observed that patching a non-critical environment is a lower priority to most enterprises. Intruders exploit this vulnerability and use it as an ingress point to make lateral movement into a critical environment. The recent episode of Log4j zero-day vulnerability found in a commonly used logging tool that allowed hackers to launch **Remote Code Execution (RCE)** attacks against affected systems further underscores the importance of patching. The use of automated patch monitoring and management tools is a critical lever that organizations can use to maintain a structured patch management process in today's complex and heterogeneous environments.

The vulnerabilities aren't just the vendor platform ones but those present in all the web interface applications, including the API calls. SISA has observed that most hackers **target vulnerable applications such as UAT systems and non-critical applications with** a **web interface** and then make lateral movements by deploying backdoors in servers to access sensitive IT data/assets. Some of the common vulnerabilities exploited are SQL injection, malicious file upload, OS command injection vulnerability, and security misconfiguration.

Another noticeable trend is that most clients are unaware of **Personally Identifiable Information (PII)** or sensitive data stored in the application logs and databases.

Recommended best practices

Create an accurate list of IT assets and inventory covering the entire ecosystem and not just limited to the production environment. Include the **third-party applications**, **libraries, and platforms** used/deployed in your environment.

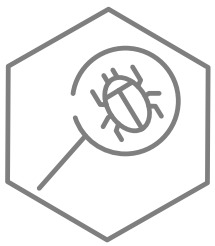
Have a management program for identifying vulnerabilities not just in OS but in all applications (like Adobe, MS Word, Excel, etc.) deployed within the network, web applications, mobile applications, APIs, libraries, and platforms. A fortnightly or monthly **vulnerability assessment scan** is ideal.

The vulnerability management program must ensure that all vulnerabilities with a **CVSS score of 6.5 and higher are mitigated immediately** or it must control to stop the exploitation of the vulnerability that is present. As most of the vulnerabilities with a CVSS score of less than 6.5 can't be exploited remotely, these vulnerabilities can follow the organization's current patch management process.

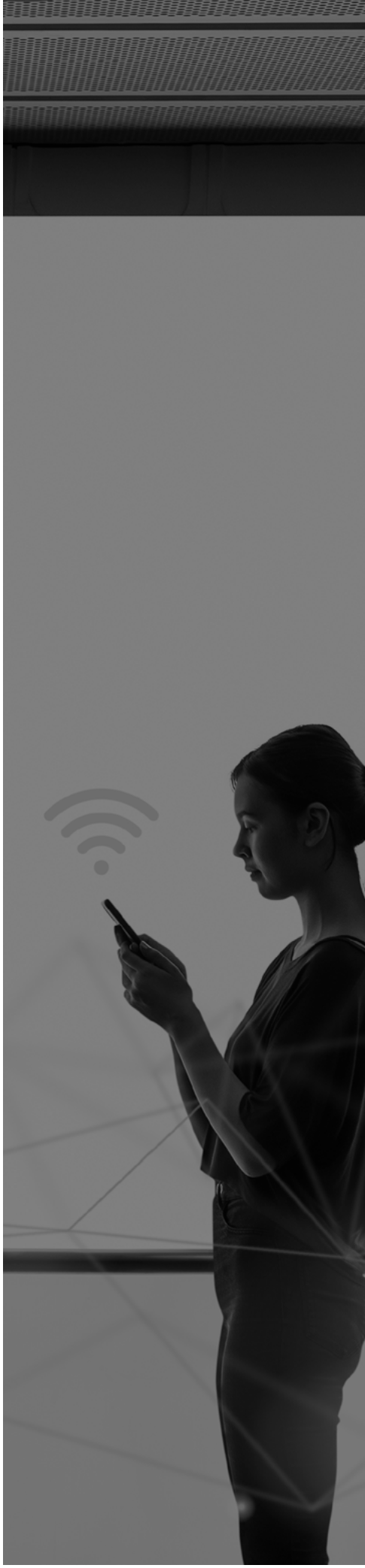
In the case of web applications, API, and mobile application, conducting the monthly test isn't possible. Hence, ensure all traffic from these applications is routed through a Web Application Firewall (WAF). The WAF should be configured for dropping critical and high severity malicious traffic.

Run **Data Discovery and Classification tool** across the organization to identify the locations where PII data are stored so that controls can be drafted for protecting the same.

Ensure that the vulnerability management program covers all system components and locations, especially UAT and remote/WFH systems.



The **vulnerability management program** must ensure that all vulnerabilities with a **CVSS score** of **6.5** and higher are mitigated immediately or it must control to stop the **exploitation** of the **vulnerability** that is present.



Strengthen endpoint response

Currently, the use of custom malware and genuine tools by intruders as a defense evasion technique for lateral movement is becoming widespread. **Most of the antivirus** and **EDR solutions may detect these malwares,** but unfortunately, they may not delete or quarantine the same. The solutions might flag them as suspicious, at best. Hence, the organization needs to invest in a robust endpoint response solution, which will enable them to take action against any malicious malware which might not be removed or quarantined by the endpoint detection solution.

As the intruders **target remote/WFH systems,** the ability to respond to suspicious incidents in the remote system plays a crucial role in protecting the end-users and enterprises. Also, organizations need to have a team for monitoring and conducting an incident response for various antivirus/EDR use cases, such as disabling the endpoint detection solutions, re-configuring them, etc.

Recommended best practices

- Even if you have an antivirus solution, deploy an **endpoint response solution** to enable the IT/Infosec/IR team to respond to a suspicious event in the endpoint systems.
- Implement **DNS security solutions** in the endpoint systems for restricting command and control communication by malwares which would evade the endpoint detection solutions.
- Ensure that all the endpoints are monitored, use cases for endpoints are configured, and playbook including incident response are covered in case of suspicious activities at the endpoint devices.
- Ensure that the **team is trained** and able to respond to contain any malicious activities at the endpoint devices.

The use of **custom malware** and genuine tools by intruders as a **defense evasion** technique for lateral movement is becoming very prevalent.

Deploy intelligent monitoring

Most of the breached entities had a central **logging/log monitoring solution** deployed in the environment. They either had a separate monitoring team, or their IT team was monitoring the logs periodically. But unfortunately, they weren't able to detect the breach.

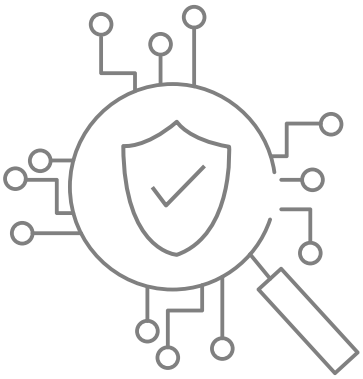
Intelligent threat monitoring involves continuous monitoring of an organization's networks and endpoints for evidence of malicious internal or external threats. Every action on the system generates a log, and effective monitoring of logs is critical to enable the early detection of threats. Integrating threat intelligence offers enterprises an edge through proactive threat blocking, landscape modeling, threat simulation, and real-time reporting. SISA has observed that, on an average, an intruder resides in the company network for about 180 days, which explains why organizations need to have robust threat monitoring systems. Further, our investigations have found that **DNS activity logs** are usually not present while outbound **HTTP traffic, proxy server logs, web server access logs,** and **WAF logs are not usually integrated into SIEM,** leading to potentially expanding the attack surface. Organizations can consider deploying an ML-based monitoring solution that goes beyond traditional rules-based and signature-based tools for detecting anomalies that might be suspicious.

> **SISA** has observed that, on average, an **intruder resides in the company network** for about **180 days,** which explains why organizations need to have **robust threat monitoring systems**

Recommended best practices

Complete coverage – It's essential that the monitoring activity should cover the organization's entire technology infrastructure and shouldn't be limited to a few critical systems. It should cover the non-critical environment such as the **UAT, testing setup, cloud environment (if any), user segment, SAAS applications,** etc. Limiting the monitoring to just a few critical systems is one of the biggest reasons the entities could not detect the breach.

Irrespective of the solutions used for monitoring, having a comprehensive set of use cases for identifying suspicious events are important. Organizations should consider incorporating the **Sigma rules** at minimum as part of the monitoring activity.



Threat Intel or Indicators of Compromise (IOCs) are one of the easiest methods for identifying suspicious events or a potential breach, or an advanced persistent threat (APT). Hence, organizations should ensure that at least the **open-source threat intel feeds** are integrated into the monitoring activity.

As intruders are increasingly using various defense evasion techniques, the organization should consider using **ML-based anomaly detection** techniques and tools for identifying anomalies in the user behaviors, network traffic, etc.

The organization should also have a **Threat Hunting Activity,** both manual and ML-based, for identifying threats that would have evaded all the security controls deployed.

Set up diligent access management

Access management plays a critical role in securing identity and profile data. With compromised passwords cited as the most common cause of data breaches, securing digital identities needs to be a combination of strengthening access control measures and authentication mechanisms. SISA has observed that the absence of a strong password and account lockout policy, **shared user IDs** to administer servers, and **non-implementation of MFA** for accessing sensitive data have been major contributors to data breaches. Adopting a **Zero Trust** security approach built on the principles of "trusting no one" can help organizations prevent identity theft, data breaches, and illegal access to sensitive information by controlling user access to critical information. Another imperative is to continuously monitor an employee's networking activity and behavior to identify and detect abnormalities that might point to unauthorized access. Context-based, step-up authentication can verify employee identities irrespective of location and device, which can help organizations spot suspicious sign-ins and act upon them swiftly.

Recommended best practices

- **Implement role-based access control** to define and enforce how users are identified in a system by using the principle of least privilege.
- Ensure proper **configuration of MFA**. The MFA should ensure that it's an **out-of-band authentication** and that it is applicable for accessing all applications and system components.
- Regularly conduct **Cloud Security Assessment reviews** to ensure no misconfiguration in the cloud.
- Secure passwords by using password vaults and **strong password credentials,** and educate the administrators on the dangers of recording the credentials.
- Perform periodic user and role reviews for all SaaS applications, conduct access audits, and **review access privileges** to meet the changing needs.

> Adopting a Zero Trust security approach built on the principles of **"trusting no one"** can help organizations prevent identity theft, **data breaches, and illegal access** to sensitive information by **controlling user access.**

Execute proper incident response and forensics

Having robust and integrated incident response and forensics is vital to **identify, remediate and investigate security incidents** early on to minimize recovery time and costs. While **incident response** focuses on the containment of a breach, compromise, or attack, **forensics** deals with an in-depth examination of the data to understand the tactics, technique, and procedures (TTP) and potentially prevent a recurrence. Given that the **dwell time of intruders is 180 days on average,** preliminary forensics becomes critical to understand the root cause, pattern of attacks, and extent of impact and thereby lower the possibility of lateral movement.

Recommended best practices

- Periodically test and document incident response plan and integrate with **Business Continuity Plan (BCP).**
- Conduct a periodic **forensic review of the logs** to confirm that no potential breach has gone unnoticed.
- Conduct **Forensic Readiness Audit** to assess preparedness to detect, manage and investigate a security incident.
- Prepare and document detailed **incident response playbook** for responding to suspicious events.
- Have an Incident Response team who can contain malicious incidents.

About SISA **Forensic Learning Sessions**

SISA's dedicated **Forensic Learning Sessions (FLS)** share crucial learnings with senior leadership for our customers. Our FLS includes our observations of attack surfaces, key weaknesses exploited by attackers, critical security controls to be set up to mitigate/reduce cyber risk, and counter measures to be put in place in the event of a breach. The case studies that we use are based on actual events. This session is delivered as a consultative session, with our core PFIs (Payment Forensics Investigators) answering your questions and advising you on the necessary security precautions. **Contact us** if you are interested in SISA's FLS.

References

1. Fortune, "The number of data breaches in 2021 has already surpassed last year's total", October 7, 2021
2. IBM, Cost of a Data Breach Report 2021
3. Help Net Security, "Most IT security leaders lack confidence in their company's security posture," March 1, 2021
4. Proofpoint, 2022 State of the Phish Report explores increasingly active threat landscape, importance of people-centric security, Feb 22, 2022
5. SonicWall, ransome ware attacks surged in 2X in 2021, Feb 17, 2022
6. 2022 Ponemon Cost of Insider Threats Global Report
7. Info Security, "How to Improve Patch Management," September 28, 2021

About SISA Information Security

SISA is a forensics-driven cybersecurity company, with offices across the globe and is trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective security services, and solutions.

SISA is one of the Top 4 Global PCI Forensic Investigators

1,000+
Active engagements

2,000+
Global customers served

40+
Countries

Our Offerings

Compliance

PCI Compliance
- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI Software Security Framework
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ

Risk and Compliance
- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Swift
- Cloud Security
- Risk Assessment
- Quarterly Security Audit

Security Testing

Application Security
- Application PenetrationTesting
- CREST/CERT-in Approved Security Testing
- API Testing
- Secure Code Review

Network Security
- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- ASV Scan

IoT Security Testing

Managed Security Services

Phishing Simulation

MDR

Managed Detection and Response Solution - SISA ProACT

Incident Response and Forensics
- Incident Response/ Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation

Advanced Threat Hunting

Data Protection

Data Discovery and Classification Tool-SISA Radar
- Card Data Discovery
- PII (Privacy) Data Discovery
- Data Classification

Data Discovery as a Service

Training

Payment Data Security Implementation Programs
- CPISI
- CPISI Advanced
- CPISI-D

Security Incident Detection and Response Programs
- CIDR

Forensic Learning Sessions for Senior Management

To learn more about SISA's offerings visit us at www.sisainfosec.com or contact your SISA sales representative at contact@sisainfosec.com

SISA
Forensics-driven Cybersecurity