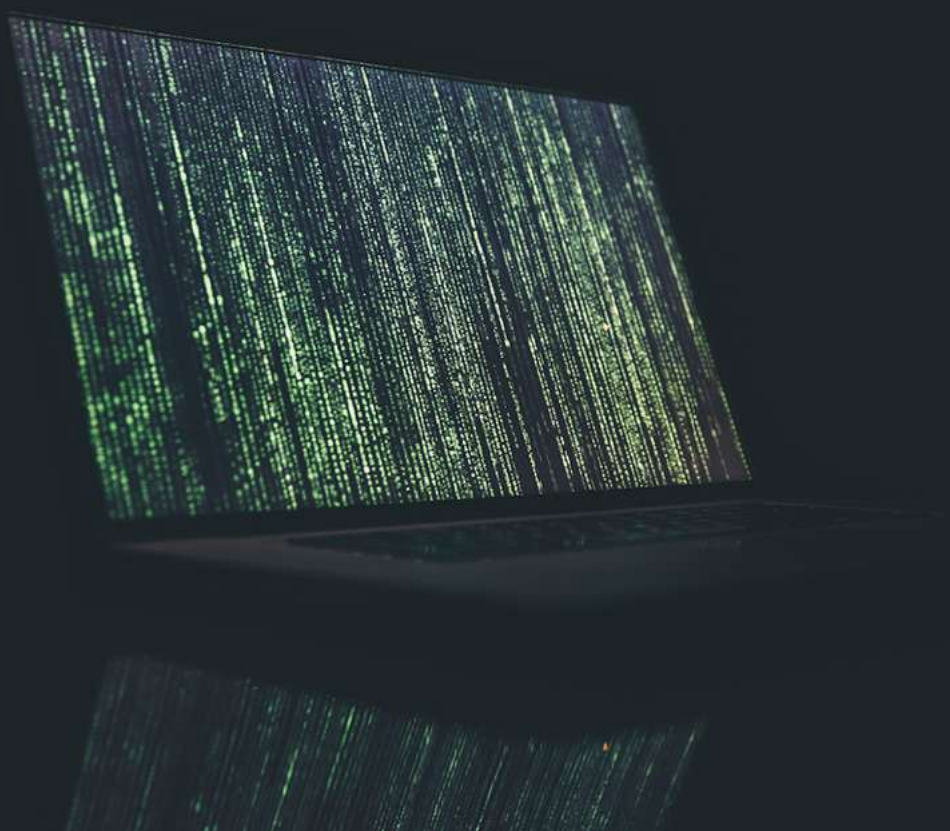
eCrime.ch

White Paper

Enhancing Threat Detection and Incident Response Capabilities with eCrime.ch



Introduction

As technology advances, so does its abuse.

The rapidly growing threat of cybercrimes poses significant risks to organizations worldwide. Per Cybersecurity Ventures, the global loss to cybercrime is predicted to reach $8 trillion by the end of 2023. If cybercrime were a nation, it would be the third-largest economy after U.S. and China.

That's not all. Cybercrime costs are set to reach a staggering $10.5 trillion per year by 2025. That would be more than any other economic transfer in history and exponentially greater than the average annual damage incurred from natural disasters. The average cost of data breaches is set to reach an astounding $5 million by 2023.

Most of these attacks are due to a lack of actionable data extracted from past threats. The need for relevant data to thwart a cyber threat cannot be overestimated. Most organizations must deal with massive raw data and noise that often leads to false positives.

Moreover, cybercriminals continuously find new ways to exploit vulnerabilities and gain unauthorized access to sensitive data and systems. One increasingly prevalent method they use is gaining access through your supply chains, third-party vendors, and outsourced firms.

Third parties pose a significant challenge in preventing cyber-attacks. Vulnerabilities in their networks allow cybercriminals to steal your data stored with partners or to get into your network, resulting in your organization losing substantial financial resources, damaged reputation, and legal issues.

Add to that the evolving threat landscape and the increasing sophistication of cyberattacks, organizations need highly organized data to be fed to TIPs to defend against cyber threats proactively.

This white paper explores the importance of relevant information, tools, and platforms you can use to prevent and mitigate cyber-attacks on your organization. It also reviews the critical role of eCrime.ch Threat and Risk Intelligence Services in helping you enhance threat detection and incident response capabilities.

By analyzing attacks in real time and offering comprehensive threat intelligence and expert insights, eCrime.ch provides actionable guidance to fortify your defenses against the continually evolving landscape of cyber threats.

Industries and Sectors Most Targeted by Cybercriminals

While most cybercriminals attack medium to large organizations, it is not the rule. If you are connected to the internet, you are at risk of a cyber-attack.

Coveware's analysis of ransomware attacks in the first quarter of 2023 revealed that cybercriminals attacked the following two company sizes the most:

- **101 to 1000 employee count (34%), and**
- **11 to 100 employee count (25.2%)**

If you have a smaller firm, you'd feel you can relax. But sorry to burst your bubble. Smaller businesses with an employee count as low as 1 to 10 were also targeted (6.3%). It proves that whatever the size of your organization, you can be in the crosshairs of the threat actors.

According to eCrime.ch, a trusted threat intelligence service specializing in ransomware data leak sites (DLS), over 2,600 posts related to victims were made by ransomware actors in 2022. These posts were found on the dark web.

As per the data, the top sectors attacked were:

- **Financial Organizations**
- **Healthcare**
- **Government**
- **IT Services/IT Consulting**
- **Legal Firms**
- **Automotive Companies**
- **Construction**
- **Education**
- **Insurance Sector**
- **Real Estate**

As evident from the list, multiple sectors are on the list of cybercriminals. But the finance sector, in particular, has become their primary target. According to Sophos Report 2023, the percentage of financial services organizations affected by ransomware rose from 34% in 2020 to 66% in 2022.

If you are a CIO/CTO or CISO in a firm that provides services to financial institutions, your top priority must be to protect your organization's valuable digital assets. If you don't address security issues promptly, a data breach can have far-reaching consequences for the institution and the broader economy. The per-company cybercrime cost is over $18 million for financial firms, around 40% higher than the average of other sectors.

Jonah Force Hill, senior cyber policy advisor and executive director of the U.S. Secret Service Cyber Investigations Advisory Board, warns, "...while virtually all sectors of the global economy fell victim to cybercrime of one kind or another, no sector was more regularly targeted than the financial sector." He further says that the increasing availability of ready-made malware creates opportunities for inexperienced criminals to leverage these tools to commit cybercrimes against financial organizations. These crimes include ransomware operations, DDoS (distributed denial of service) attacks, and BEC (business email compromise) campaigns, among others.

Financial institutions possess sensitive information and cannot afford any downtime due to production needs, making them lucrative targets for cybercriminals seeking maximum monetization opportunities.

Furthermore, cyber-attacks against the financial sector are no longer limited to data theft or fund embezzlement; they now have the potential to manipulate the entire economy, as emphasized by Christine Lagarde, president of the European Central Bank.
The weaknesses in the system mostly boil down to inadequate employee training, insufficient network monitoring, and a lack of real-time threat intelligence.

Here are a couple more examples of cyber-attacks on financial firms:

Genworth Financial (May-June 2023)

PBI Research Services (PBI) experienced a data breach where three clients reported the theft of data belonging to 4.75 million individuals in the recent MOVEit Transfer data-theft attacks. The attacks, initiated by the Clop ransomware gang on May 27th, 2023, involved exploiting a zero-day vulnerability in MOVEit Transfer to target numerous companies.

The first impacted client of the breach was Genworth Financial. PBI Research Services notified the US-based life insurance firm about the breach on June 16. At least 2.5 million records were exposed in the breach. Genworth Financial confirmed its own systems were unaffected, attributing the attack to shared information with a third-party file-sharing service.

Latitude Financial (March 2023)

Latitude Financial experienced the largest confirmed data breach in March 2023, impacting over 14 million records. The Melbourne-based company, offering loans and credit cards in Australia and New Zealand, disclosed that cyber criminals accessed various data, including nearly 8 million driver's licenses, 53,000 passport numbers, and financial statements. An additional 6 million records from as far back as 2005 were also compromised, with the source of the attack still unknown.

The concerning aspect of this breach is that Latitude Financial initially reported only 300,000 affected individuals, indicating a lack of understanding and a rushed disclosure. Updating the estimate raises further scrutiny and risks damaging customer trust. While data breaches can happen anywhere, a poorly managed response suggests inadequate preparedness and raises doubts about the organization's ability to address the breach effectively.

Beanstalk Farms (April 2022)

Beanstalk Farms, a decentralized finance platform, suffered a cryptocurrency theft resulting in a loss of $180 million on April 17, 2022. The attackers obtained a substantial loan, enabling them to gain sufficient voting rights to execute governance changes, ultimately transferring all of Beanstalk's reserves.

Why is the finance sector the favorite target of the threat actors? There are two primary reasons:

1. Banks and other financial organizations have huge attack surfaces due to digital transactions spread over several domains worldwide, and

2. Attacks in the finance sector have the potential for highly damaging outcomes.

According to Verizon's DBIR, in the finance sector, 8.9% of incidents resulted in data breaches. 44% of those breaches were attributed to internal actors, primarily accidental. Motivations behind these attacks predominantly revolve around financial gain, but espionage, grudges, entertainment, and ideology also play a role.

Supply Chain and Third-Party Cyber Attacks

With an increasing digital interconnectedness among global businesses, your organization is vulnerable to yet another modus operandi cyber criminals use to hack your system, supply chain cyber-attacks.

Most companies worldwide have one or more vendors, giving cybercriminals the power to attack thousands of organizations in just one go.

73% of respondents in a KPMG survey of 2022 said they experienced at least one major disruption caused by a vendor in the past three years.

A supply chain or third-party cyber-attack occurs when cybercriminals exploit vulnerabilities in your organization's extended network of suppliers, vendors, and outsourced partners.

Their goal is to gain unauthorized access to your systems, steal sensitive information, or introduce malicious software.

By compromising a trusted third party, attackers can bypass your network's direct defenses and infiltrate your systems unnoticed.

A few supply chain statistics:

60%

Over 60% of SOC leaders confirmed that they plan to implement supply chain security practices in 2022.

84%

84% of IT professionals foresee software supply chain attacks as the biggest cyber threat in the next three years.

265x

Supply chain attacks on software packages surged from 702 to 185,572 between 2019 and 2022, which is an increase of nearly 265 times.

There are several risks associated with supply chain attacks:

Compromised Trust

When you blindly trust your vendors to have good security measures, you might not realize that cybercriminals can exploit their weaknesses to get to you. It's a risk you need to be aware of.

Expanded Attack Surface

Digitally connecting with your suppliers broadens the attack surface. A single vulnerable entry point in the supply chain exposes multiple organizations, including yours, to potential threats.

Data Breach

Through this entry point, cybercriminals enter and steal or corrupt your customers' data, trade secrets, and intellectual property, resulting in heavy financial loss and a damaged reputation.

You need to be proactive in such cases and take the following actions to safeguard your organization against cyber actors:

- Thoroughly perform due diligence on your vendors' cybersecurity standards and practices before onboarding them.
- Ensure you include clauses in your contracts with third parties for regular security reviews, incident response procedures, and data breach notifications.
- Proactively monitor the security posture of your suppliers to ensure compliance with agreed-upon security standards.
- Acquire products or services that keep you abreast of real-time intelligence regarding emerging threats and vulnerabilities to identify potential risks quickly.
- Keep a comprehensive incident response plan ready.
- Educate your employees about the risks associated with supply chain attacks. Train them to identify suspicious activities and phishing attempts.
- Ensure compliance with industry best practices and regularly review security within your organization to identify potential vulnerabilities.

While cybercriminals operate in several ways, supply chain cyber-attacks are rising. If you regularly deal with third parties as part of your business, their security is as important as the security of your own systems.

Maintaining real-time awareness of threat intelligence and ongoing cyber-attacks is paramount to staying one step ahead of cybercriminals and protecting your organization from potential devastation.

Threat Intelligence Platforms, SIEM, and SOAR

By integrating a Threat Intelligence Platform (TIP) with your SIEM or SOAR system, you can leverage advanced threat intelligence to combat modern-day cyber threats. Real-time, comprehensive, and contextual threat intelligence goes a long way in detecting and responding to cyber threats quickly.

But before we delve deeper into the importance of integrating a TIP with your security system, let us understand what these tools are and how they work:

Threat Intelligence Platform (TIP)

A TIP collects and provides valuable intelligence on emerging threats, threat actors, and vulnerabilities. TIPs collect vast amounts of data from external sources, including global threat feeds, open-source intelligence, and industry-specific reports.

A TIP serves as a centralized workspace for your security team to efficiently consume data from different sources. It allows you to

- Combine intelligence from several sources
- Normalize, enrich, and prioritize information for quicker analysis
- Synthesize all the data to extract actionable intelligence and share it with existing security systems

SIEM

Security Information and Event Management (SIEM) is a tool you can use to collect and analyze log and event data from various sources like security networks, servers, applications, databases, and TIPs. It detects and gives alerts regarding security events, such as abnormal login attempts, and provides insights for investigation.

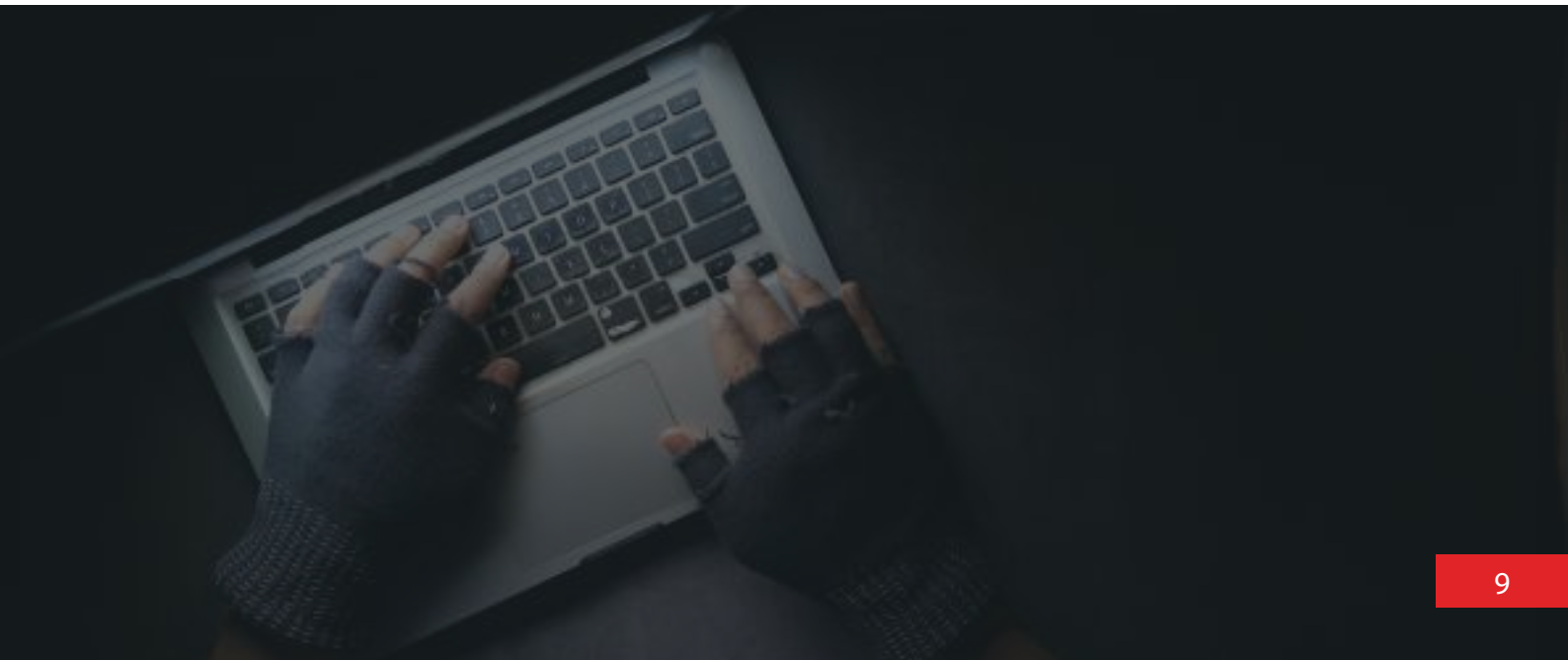
SIEM collects data from different systems and helps your SOC team comply with security regulations. It has three core capabilities: data collection, analytics, and response. SIEM offers visibility in hybrid and multi-cloud environments and helps organizations detect and mitigate threats effectively.

SOAR

Security Orchestration, Automation, and Response (SOAR) is a novel tool designed to streamline and enhance your incident response process. SOAR utilizes AI to prioritize incident alerts and uses an idea called playbooks, predesigned and automated actions that initiate when certain conditions are met.

An instance where SOAR can be a boon for you is malware containment, where it identifies, and quarantines compromised devices without human involvement.

The main components of a SOAR system include orchestration, automation, and response. Orchestration integrates and analyzes data from different security tools, automation eliminates manual tasks, and response involves collecting and prioritizing security events for efficient incident handling.



Supply Chain and Third-Party Cyber Attacks

While SIEMs and TIPs are crucial tools, they come with their own set of limitations:

DATA OVERLOAD

Networks generate a vast amount of log and event data. It is challenging for SIEM and TIP to collect, store, and analyze this amount of data effectively. The sheer scale of data leads to information overload and prevents the timely identification of significant threats.

LACK OF CONTEXT

Your security teams need a good understanding of the threat landscape. The SIEM and TIP often fail to provide insights into the attackers' motives and tactics, preventing you from effectively detecting and responding to threats. This makes it hard to correctly decide which security incidents to focus on and respond to.

FALSE POSITIVES

False positives occur when legitimate events are flagged as potential security incidents. Too many false positives can cause alert fatigue among analysts of your security teams, resulting in wasted time and resources.

MANUAL PROCESSES

Traditional SIEM and TIP solutions often rely on manual processes. If you're using one of them, your team of analysts is spending a considerable time manually analyzing and correlating events, delaying the incident response. Your teams are also prone to the risk of human errors, jeopardizing the efficiency of incident handling.

How eCrime.ch Helps Your Threat Intelligence Platform Work Efficiently

Without sufficient and timely attack data and threat intelligence, all your TIPs, SIEMs, and SOARs offer little value. These tools will only work if they are fed with real-time advanced threat intelligence.

eCrime.ch helps in bridging the gap between your TIP and SIEM. It is the go-to provider for all your needs for comprehensive and real-time threat intelligence.

With eCrime.ch Threat and Risk Intelligence Services in your array of security products, you can have the following benefits:

- eCrime.ch is a highly essential tracker that enables a threat intelligence platform to efficiently perform its various functions, such as
  - Threat Monitoring and Real-Time Alerts
  - Automated Malware Analysis and Actor Profiling
  - Incident Response
  - Operational Intelligence Response
  - Threat Research
- eCrime.ch monitors 90+ actor-maintained ransomware and data leak sites to extract actionable data from past and current threats to prevent future attacks. More sources of threat details, observed attacks and intelligence on new actor groups are added regularly.
- You can perform due diligence on your current and future vendors and third-party suppliers to know if they have ever been attacked in the past. Just search the name or domain of your vendors or the sector they belong to on the eCrime.ch dashboard and Voila! you have the full details of the attack.
- You can even use eCrime.ch to get notified of attacks against your partners/outsourced firms through emails, making you aware in real time regarding third-party risks.
- All collected data is manually reviewed and validated by experienced cybersecurity experts.

- eCrime.ch dashboard provides comprehensive data on cyber-attacks and lets you view data filtered by duration, malware, sector, and country.
- The dashboard also allows you to search any data by keyword and filter and sort the results using different parameters such as threat actors, country, sector, employee count, etc
- Extensive data is made available on the cyber-attacks, including screenshots and sample ransom notes extracted from data leak sites.
- A novel feature, “Intelligence Profiles," allow subscribers to understand how a threat actor or ransomware operates by including abused vulnerabilities, MITRE ATT&CK techniques, and more.
- eCrime.ch also lets you save the data in CSV and JSON formats. You can even generate JSON or CSV files for a custom timeframe.
- eCrime.ch lets you integrate data feed into your existing cyber solutions through its API, enabling you to quickly respond to cyber-attacks on your customers, members, or third parties.
- eCrime.ch dashboard also contains the latest news, updates, and additional resources required to keep you abreast of the world of cybersecurity in real-time.
- eCrime.ch enhances the intelligence and context available for analysis in TIP, SOAR or SIEM

Enhance Your Threat Intelligence with eCrime.ch

If you’re seriously worried about the security of your valuable data and digital networks, join us in the fight against cybercriminals and save yourself from substantial financial losses.

Contact us to get a free 30-day trial to eCrime.ch dashboard.

References

https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

https://edafio.com/blog/cybersecurity-in-2023-average-cost-of-data-breaches-to-reach-5-million/

https://www.coveware.com/blog/2023/4/28/big-game-hunting-is-back-despite-decreasing-ransom-payment-amounts

https://www.sophos.com/en-us/content/state-of-ransomware

https://cybersecurityventures.com/cybersecurity-almanac-2023/

https://www.sciencedirect.com/science/article/pii/S1877050923002752?ref=pdf_download&fr=RR-2&rr=7e2dedd43df7f3ed

https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf

https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/

https://techbeacon.com/security/35-stats-matter-your-security-operations-team

eCrime.ch