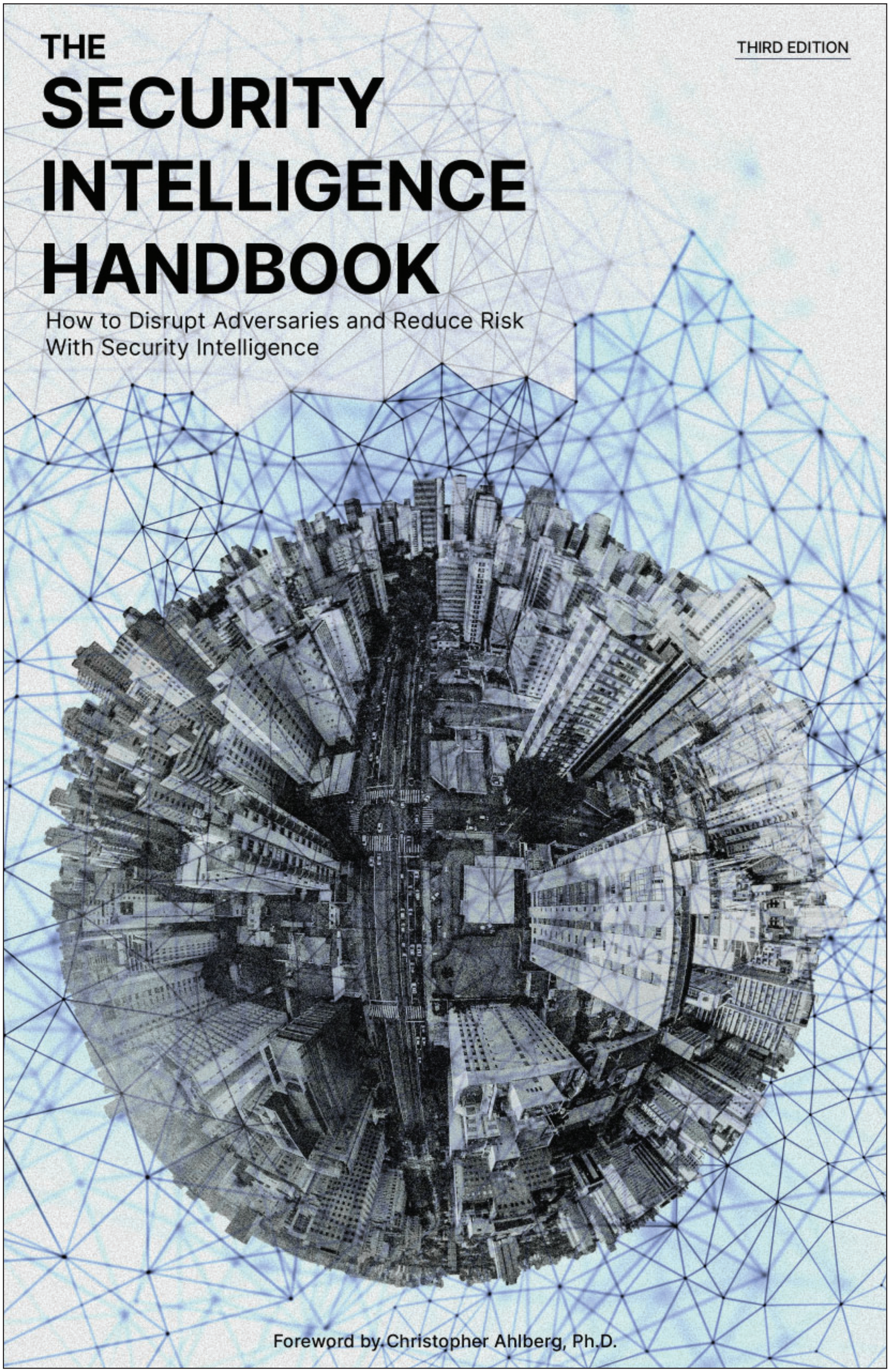
FIGURE SUPPLEMENT


THE
SECURITY
INTELLIGENCE
HANDBOOK
How to Disrupt Adversaries and Reduce Risk
With Security Intelligence
THIRD EDITION
Foreword by Christopher Ahlberg, Ph.D.

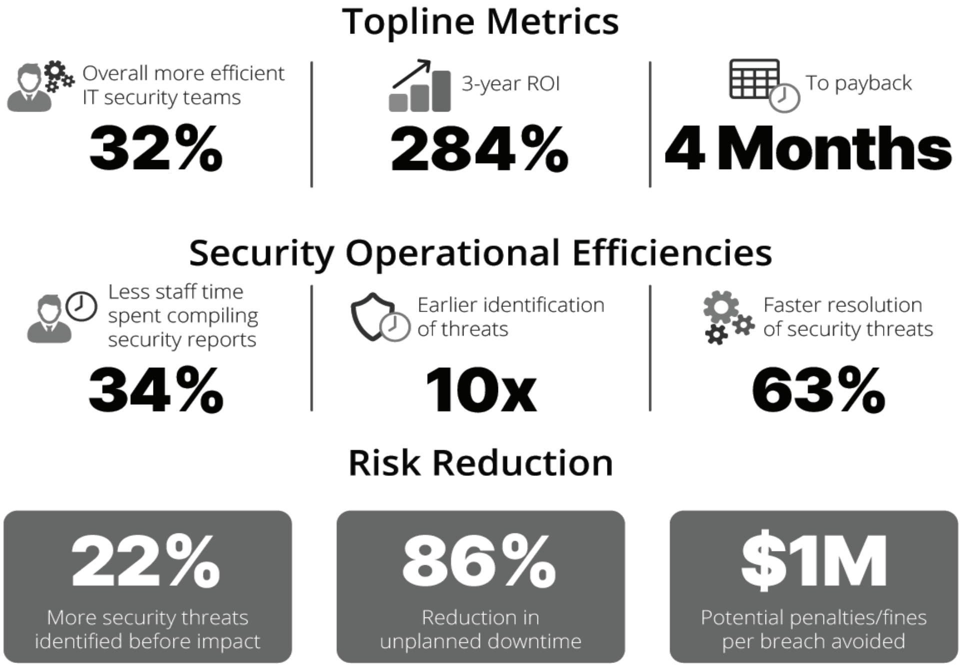


Figure 1-1: A security intelligence program can produce dramatic improvements in security and efficiency. Source of data: IDC

Data consists of discrete facts and statistics gathered as the basis for further analysis.

Information is comprised of multiple data points that are combined to answer specific questions.

Intelligence is the output of an analysis of data and information that uncovers patterns and provides vital context to inform decision-making.

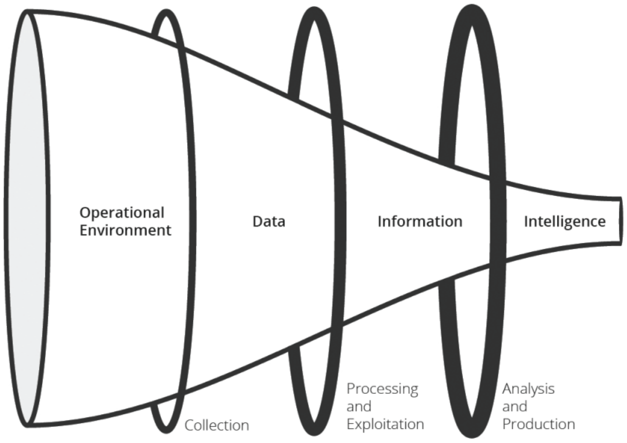


Figure 1-2: The relationship between data, information, and intelligence.

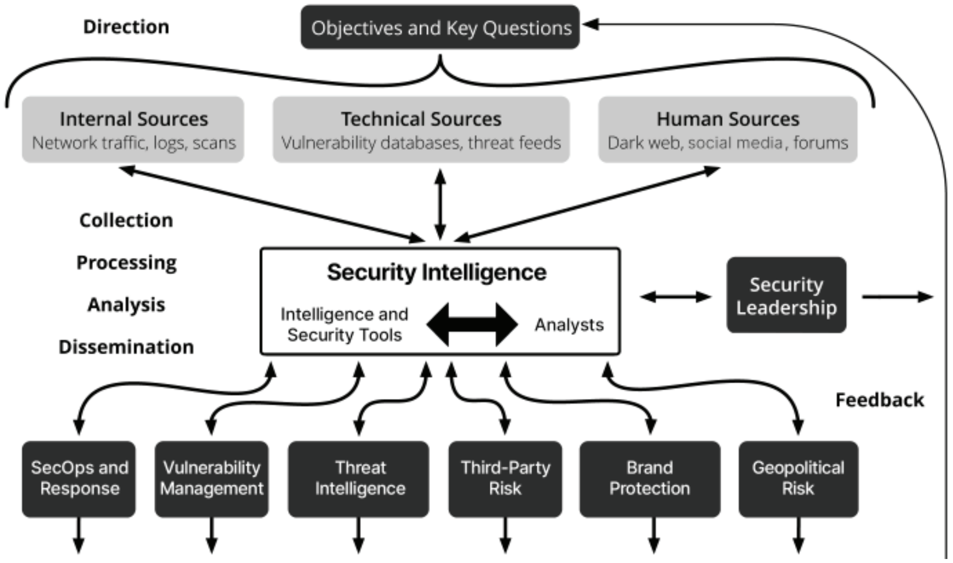
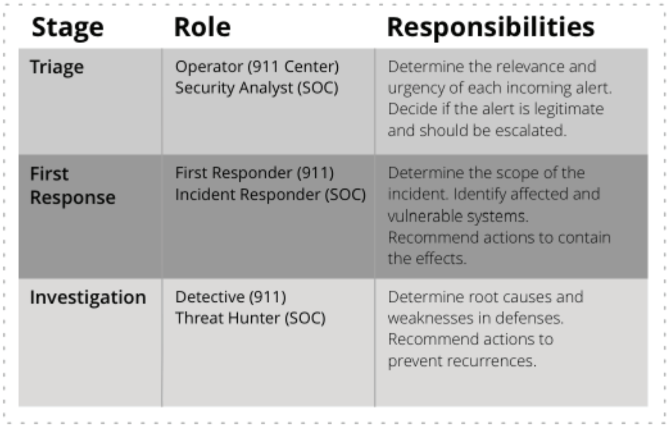


Figure 3-1: Security intelligence and the six phases of the intelligence cycle.



Stage	Role	Responsibilities
Triage	Operator (911 Center) Security Analyst (SOC)	Determine the relevance and urgency of each incoming alert. Decide if the alert is legitimate and should be escalated.
First Response	First Responder (911) Incident Responder (SOC)	Determine the scope of the incident. Identify affected and vulnerable systems. Recommend actions to contain the effects.
Investigation	Detective (911) Threat Hunter (SOC)	Determine root causes and weaknesses in defenses. Recommend actions to prevent recurrences.

Figure 4-1: The roles and responsibilities of emergency services teams and SecOps teams are similar.

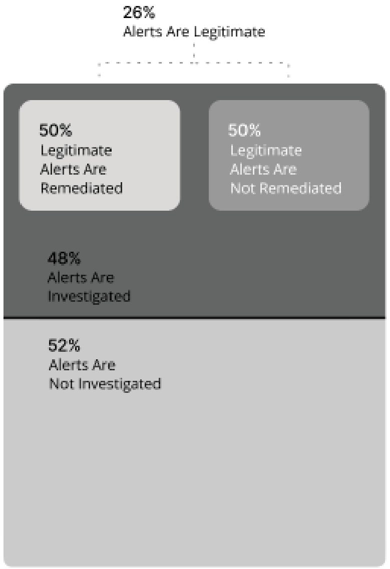
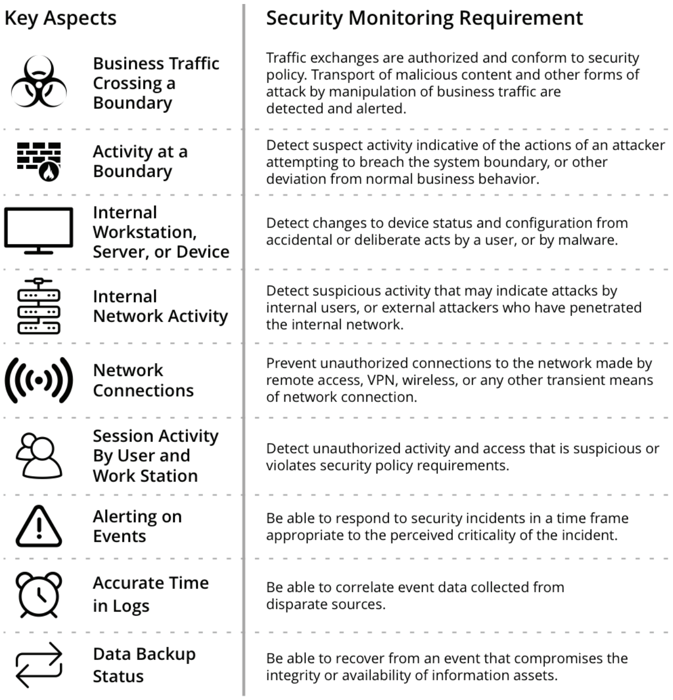
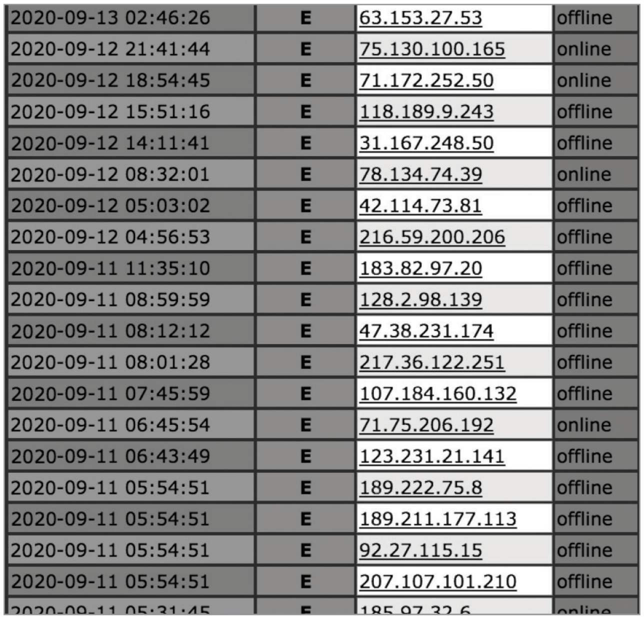


Figure 4-2: Many threat alerts are not investigated or remediated. (Source: Cisco)



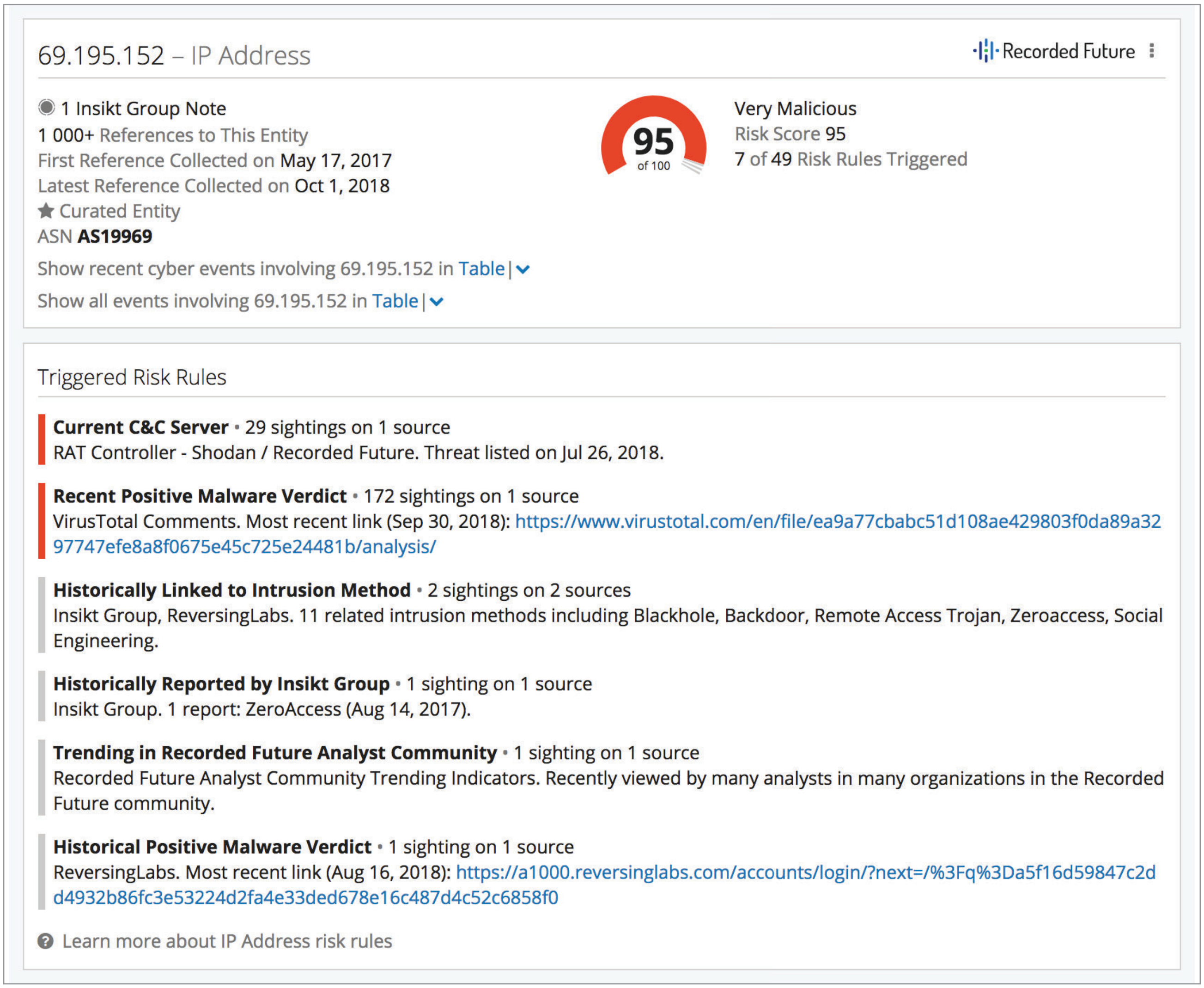
Key Aspects	Security Monitoring Requirement
Business Traffic Crossing a Boundary	Traffic exchanges are authorized and conform to security policy. Transport of malicious content and other forms of attack by manipulation of business traffic are detected and alerted.
Activity at a Boundary	Detect suspect activity indicative of the actions of an attacker attempting to breach the system boundary, or other deviation from normal business behavior.
Internal Workstation, Server, or Device	Detect changes to device status and configuration from accidental or deliberate acts by a user, or by malware.
Internal Network Activity	Detect suspicious activity that may indicate attacks by internal users, or external attackers who have penetrated the internal network.
Network Connections	Prevent unauthorized connections to the network made by remote access, VPN, wireless, or any other transient means of network connection.
Session Activity By User and Work Station	Detect unauthorized activity and access that is suspicious or violates security policy requirements.
Alerting on Events	Be able to respond to security incidents in a time frame appropriate to the perceived criticality of the incident.
Accurate Time in Logs	Be able to correlate event data collected from disparate sources.
Data Backup Status	Be able to recover from an event that compromises the integrity or availability of information assets.

Figure 4-3: Key aspects of security monitoring and internal sources of context. (Source: UK NCSC)



2020-09-13 02:46:26	E	63.153.27.53	offline
2020-09-12 21:41:44	E	75.130.100.165	online
2020-09-12 18:54:45	E	71.172.252.50	online
2020-09-12 15:51:16	E	118.189.9.243	offline
2020-09-12 14:11:41	E	31.167.248.50	offline
2020-09-12 08:32:01	E	78.134.74.39	online
2020-09-12 05:03:02	E	42.114.73.81	offline
2020-09-12 04:56:53	E	216.59.200.206	offline
2020-09-11 11:35:10	E	183.82.97.20	offline
2020-09-11 08:59:59	E	128.2.98.139	offline
2020-09-11 08:12:12	E	47.38.231.174	offline
2020-09-11 08:01:28	E	217.36.122.251	offline
2020-09-11 07:45:59	E	107.184.160.132	offline
2020-09-11 06:45:54	E	71.75.206.192	online
2020-09-11 06:43:49	E	123.231.21.141	offline
2020-09-11 05:54:51	E	189.222.75.8	offline
2020-09-11 05:54:51	E	189.211.177.113	offline
2020-09-11 05:54:51	E	92.27.115.15	offline
2020-09-11 05:54:51	E	207.107.101.210	offline
2020-09-11 05:31:45	E	185.97.32.6	online

Figure 4-4: It is very difficult to find relevant information in a raw threat feed and correlate it with other data related to an alert.



69.195.152 – IP Address

Recorded Future

1 Insikt Group Note
1 000+ References to This Entity
First Reference Collected on May 17, 2017
Latest Reference Collected on Oct 1, 2018
★ Curated Entity
ASN **AS19969**

Show recent cyber events involving 69.195.152 in Table |
Show all events involving 69.195.152 in Table |

95 of 100

Very Malicious
Risk Score 95
7 of 49 Risk Rules Triggered

Triggered Risk Rules

Current C&C Server • 29 sightings on 1 source
RAT Controller - Shodan / Recorded Future. Threat listed on Jul 26, 2018.

Recent Positive Malware Verdict • 172 sightings on 1 source
VirusTotal Comments. Most recent link (Sep 30, 2018): https://www.virustotal.com/en/file/ea9a77cbabc51d108ae429803f0da89a3297747efe8a8f0675e45c725e24481b/analysis/

Historically Linked to Intrusion Method • 2 sightings on 2 sources
Insikt Group, ReversingLabs. 11 related intrusion methods including Blackhole, Backdoor, Remote Access Trojan, Zeroaccess, Social Engineering.

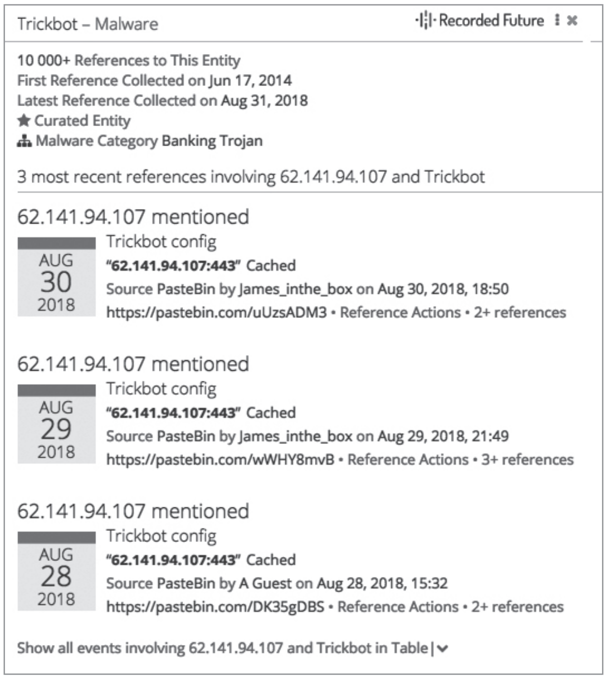
Historically Reported by Insikt Group • 1 sighting on 1 source
Insikt Group. 1 report: ZeroAccess (Aug 14, 2017).

Trending in Recorded Future Analyst Community • 1 sighting on 1 source
Recorded Future Analyst Community Trending Indicators. Recently viewed by many analysts in many organizations in the Recorded Future community.

Historical Positive Malware Verdict • 1 sighting on 1 source
ReversingLabs. Most recent link (Aug 16, 2018): https://a1000.reversinglabs.com/accounts/login/?next=/%3Fq%3Da5f16d59847c2dd4932b86fc3e53224d2fa4e33ded678e16c487d4c52c6858f0

Learn more about IP Address risk rules

Figure 4-5: A SecOps intelligence solution automatically enriches alerts with context such as previous sightings, associations with attack types and threat actors, and risk scores. (Source: Recorded Future)



Trickbot – Malware

Recorded Future

10 000+ References to This Entity
First Reference Collected on Jun 17, 2014
Latest Reference Collected on Aug 31, 2018
★ Curated Entity
Malware Category Banking Trojan

3 most recent references involving 62.141.94.107 and Trickbot

62.141.94.107 mentioned

AUG 30 2018

Trickbot config
"62.141.94.107:443" Cached
Source PasteBin by James_inthe_box on Aug 30, 2018, 18:50
https://pastebin.com/uUzsADM3 • Reference Actions • 2+ references

62.141.94.107 mentioned

AUG 29 2018

Trickbot config
"62.141.94.107:443" Cached
Source PasteBin by James_inthe_box on Aug 29, 2018, 21:49
https://pastebin.com/wWHY8mvB • Reference Actions • 3+ references

62.141.94.107 mentioned

AUG 28 2018

Trickbot config
"62.141.94.107:443" Cached
Source PasteBin by A Guest on Aug 28, 2018, 15:32
https://pastebin.com/DK35gDBS • Reference Actions • 2+ references

Show all events involving 62.141.94.107 and Trickbot in Table |

Figure 5-1: Security intelligence connecting an IP address with the Trickbot malware. (Source: Recorded Future)

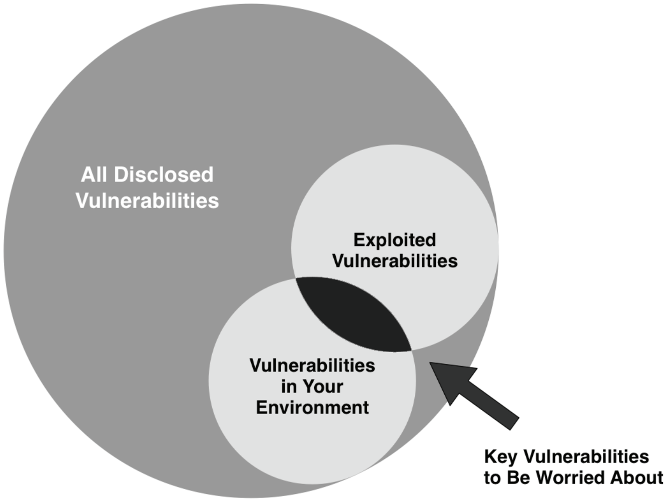
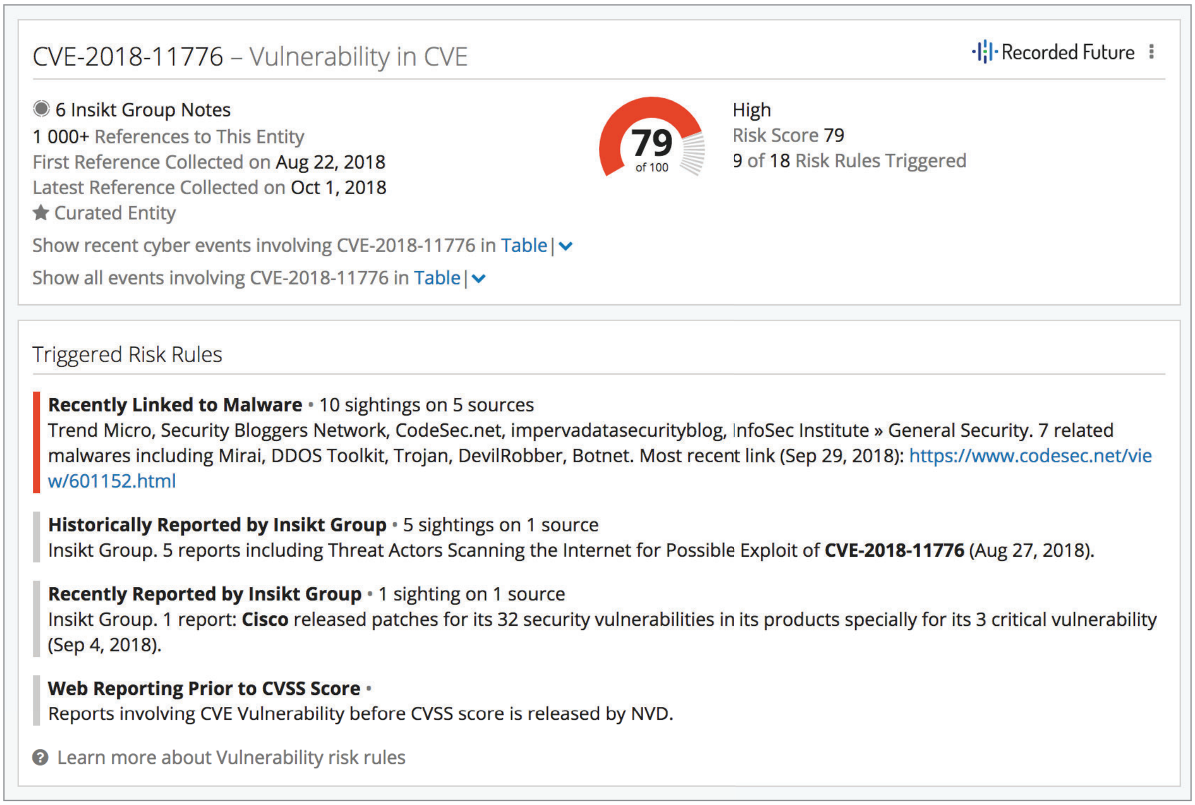

All Disclosed Vulnerabilities
Exploited Vulnerabilities
Vulnerabilities in Your Environment
Key Vulnerabilities to Be Worried About

Figure 6-1: The greatest actual risks are vulnerabilities that are present in your organization's environment and are currently being exploited. (Source: Gartner)



CVE-2018-11776 – Vulnerability in CVE

Recorded Future

6 Insikt Group Notes
1 000+ References to This Entity
First Reference Collected on Aug 22, 2018
Latest Reference Collected on Oct 1, 2018
★ Curated Entity

79 of 100

High
Risk Score 79
9 of 18 Risk Rules Triggered

Show recent cyber events involving CVE-2018-11776 in Table |
Show all events involving CVE-2018-11776 in Table |

Triggered Risk Rules

Recently Linked to Malware • 10 sightings on 5 sources
Trend Micro, Security Bloggers Network, CodeSec.net, impervadatasecurityblog, InfoSec Institute » General Security. 7 related malwares including Mirai, DDOS Toolkit, Trojan, DevilRobber, Botnet. Most recent link (Sep 29, 2018): https://www.codesec.net/view/601152.html

Historically Reported by Insikt Group • 5 sightings on 1 source
Insikt Group. 5 reports including Threat Actors Scanning the Internet for Possible Exploit of **CVE-2018-11776** (Aug 27, 2018).

Recently Reported by Insikt Group • 1 sighting on 1 source
Insikt Group. 1 report: **Cisco** released patches for its 32 security vulnerabilities in its products specially for its 3 critical vulnerability (Sep 4, 2018).

Web Reporting Prior to CVSS Score •
Reports involving CVE Vulnerability before CVSS score is released by NVD.

Learn more about Vulnerability risk rules

Figure 6-2: Security intelligence related to a vulnerability. (Source: Recorded Future)

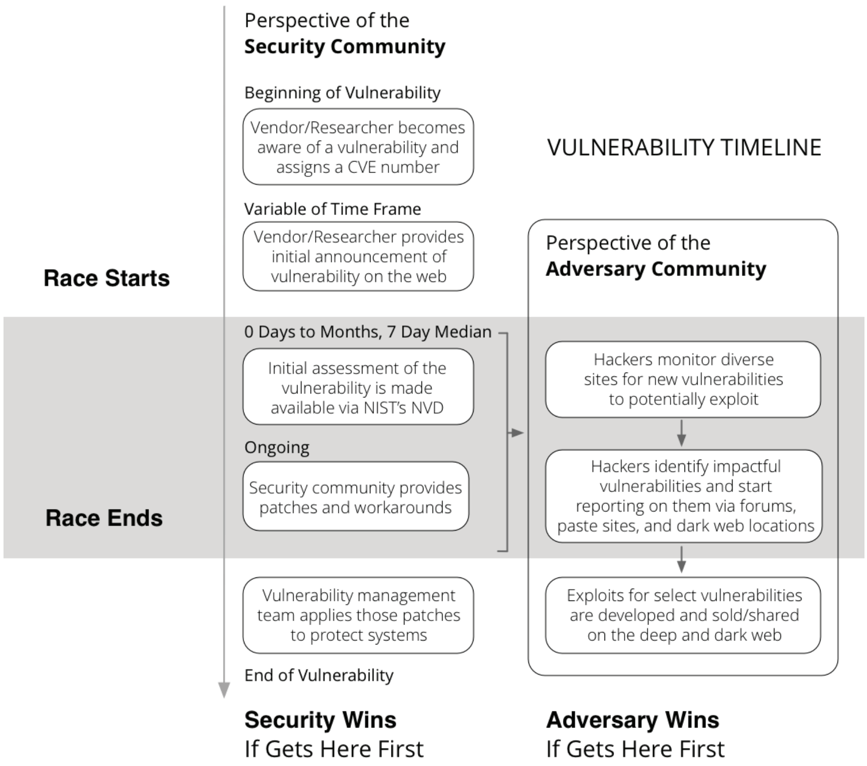

Perspective of the
Security Community
Beginning of Vulnerability
Vendor/Researcher becomes aware of a vulnerability and assigns a CVE number
VULNERABILITY TIMELINE
Variable of Time Frame
Vendor/Researcher provides initial announcement of vulnerability on the web
Perspective of the
Adversary Community
Race Starts
0 Days to Months, 7 Day Median
Initial assessment of the vulnerability is made available via NIST's NVD
Hackers monitor diverse sites for new vulnerabilities to potentially exploit
Ongoing
Security community provides patches and workarounds
Hackers identify impactful vulnerabilities and start reporting on them via forums, paste sites, and dark web locations
Race Ends
Vulnerability management team applies those patches to protect systems
Exploits for select vulnerabilities are developed and sold/shared on the deep and dark web
End of Vulnerability
Security Wins
If Gets Here First
Adversary Wins
If Gets Here First

Figure 6-3: The race between security professionals and adversaries.

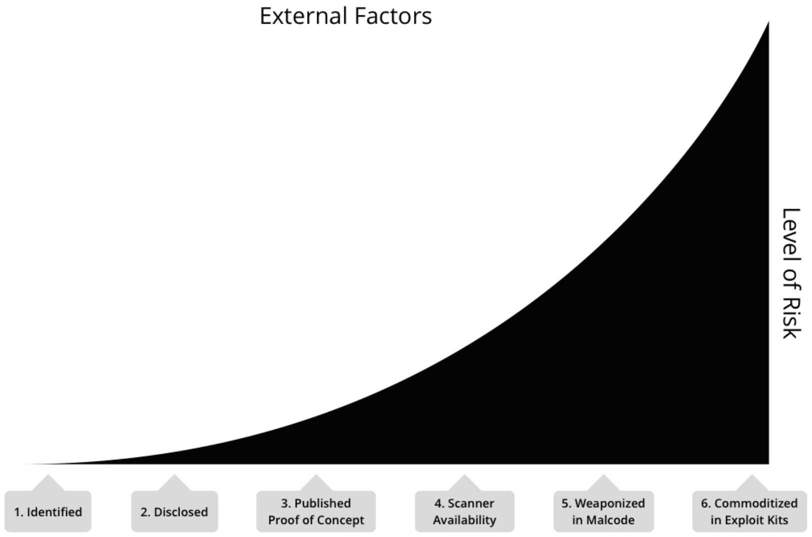
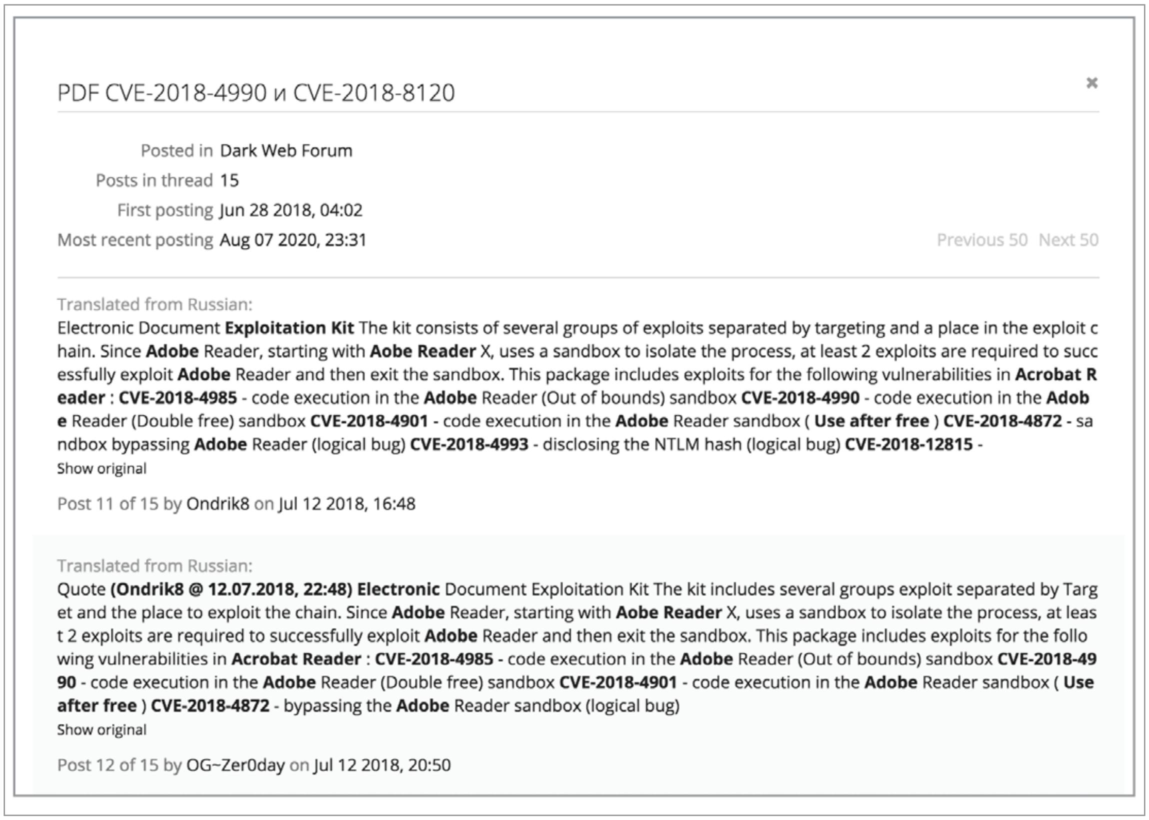


Figure 6-4: Real risk rises dramatically when vulnerabilities become weaponized and commoditized.



Posted in Dark Web Forum
Posts in thread 15
First posting Jun 28 2018, 04:02
Most recent posting Aug 07 2020, 23:31

Translated from Russian:
Electronic Document **Exploitation Kit** The kit consists of several groups of exploits separated by targeting and a place in the exploit chain. Since **Adobe** Reader, starting with **Aobe Reader** X, uses a sandbox to isolate the process, at least 2 exploits are required to successfully exploit **Adobe** Reader and then exit the sandbox. This package includes exploits for the following vulnerabilities in **Acrobat Reader** : **CVE-2018-4985** - code execution in the **Adobe** Reader (Out of bounds) sandbox **CVE-2018-4990** - code execution in the **Adobe** Reader (Double free) sandbox **CVE-2018-4901** - code execution in the **Adobe** Reader sandbox (**Use after free**) **CVE-2018-4872** - sandbox bypassing **Adobe** Reader (logical bug) **CVE-2018-4993** - disclosing the NTLM hash (logical bug) **CVE-2018-12815** -
Show original

Post 11 of 15 by Ondrik8 on Jul 12 2018, 16:48

Translated from Russian:
Quote **(Ondrik8 @ 12.07.2018, 22:48) Electronic** Document Exploitation Kit The kit includes several groups exploit separated by Target and the place to exploit the chain. Since **Adobe** Reader, starting with **Aobe Reader** X, uses a sandbox to isolate the process, at least 2 exploits are required to successfully exploit **Adobe** Reader and then exit the sandbox. This package includes exploits for the following vulnerabilities in **Acrobat Reader** : **CVE-2018-4985** - code execution in the **Adobe** Reader (Out of bounds) sandbox **CVE-2018-4990** - code execution in the **Adobe** Reader (Double free) sandbox **CVE-2018-4901** - code execution in the **Adobe** Reader sandbox (**Use after free**) **CVE-2018-4872** - bypassing the **Adobe** Reader sandbox (logical bug)
Show original

Post 12 of 15 by OG~Zer0day on Jul 12 2018, 20:50

Figure 6-5: An exchange of information between threat actors on a dark web forum translated from Russian. (Source: Recorded Future)

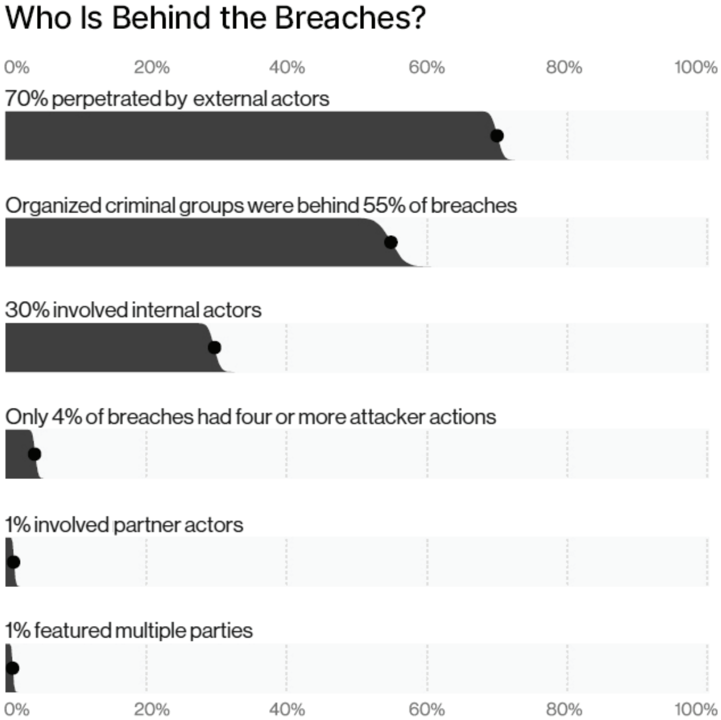


Figure 7-1: Top external actor varieties in data breaches. (Source: Verizon Data Breach Investigation Report 2020)

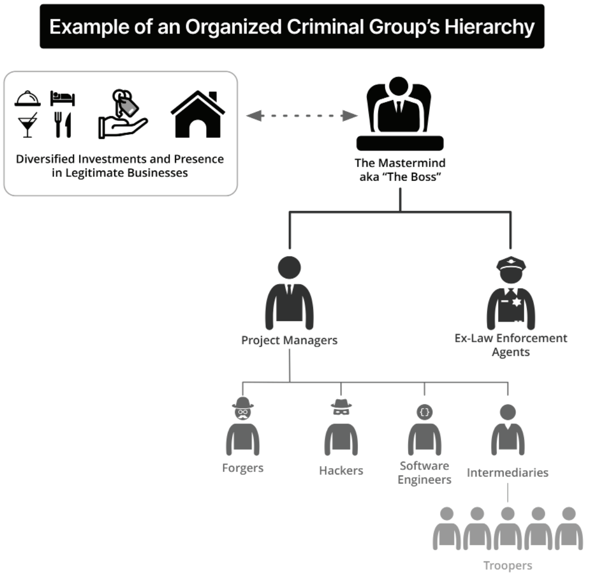

Example of an Organized Criminal Group's Hierarchy
Diversified Investments and Presence in Legitimate Businesses
The Mastermind aka "The Boss"
Project Managers
Ex-Law Enforcement Agents
Forgers
Hackers
Software Engineers
Intermediaries
Troopers

Figure 7-2: A typical organizational chart for a cybercrime syndicate. (Source: Recorded Future)

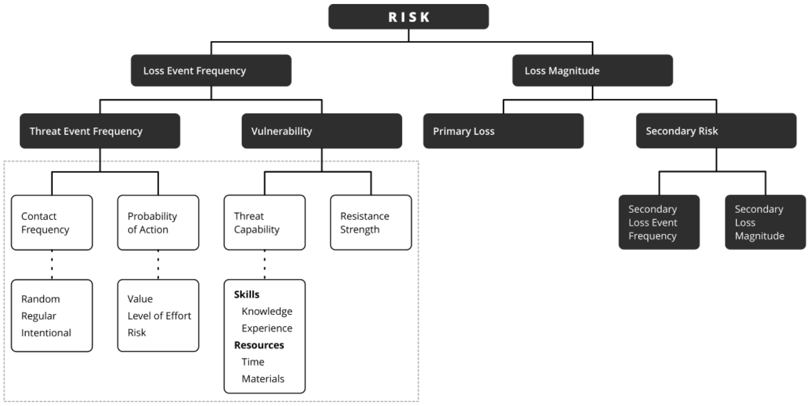
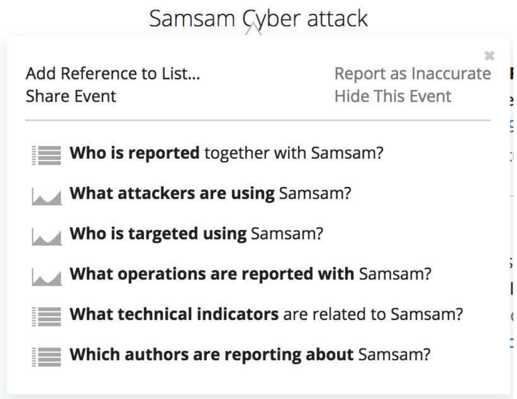


Figure 8-1: The FAIR Framework, with elements informed by intelligence highlighted. (Source: The FAIR Institute)



Samsam Cyber attack

Add Reference to List...
Share Event

Report as Inaccurate
Hide This Event

Who is reported together with Samsam?

What attackers are using Samsam?

Who is targeted using Samsam?

What operations are reported with Samsam?

What technical indicators are related to Samsam?

Which authors are reporting about Samsam?

Figure 8-2: Questions about a malware sample that a security intelligence solution answers. (Source: Recorded Future)

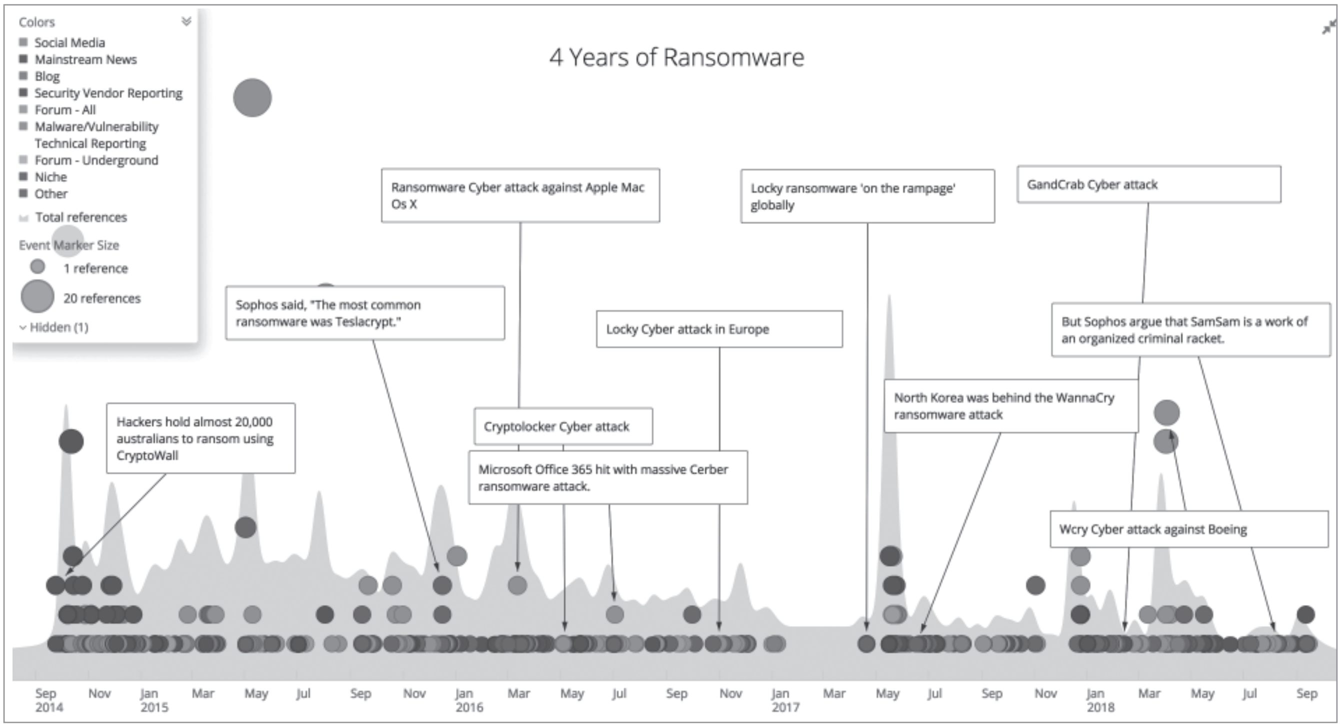
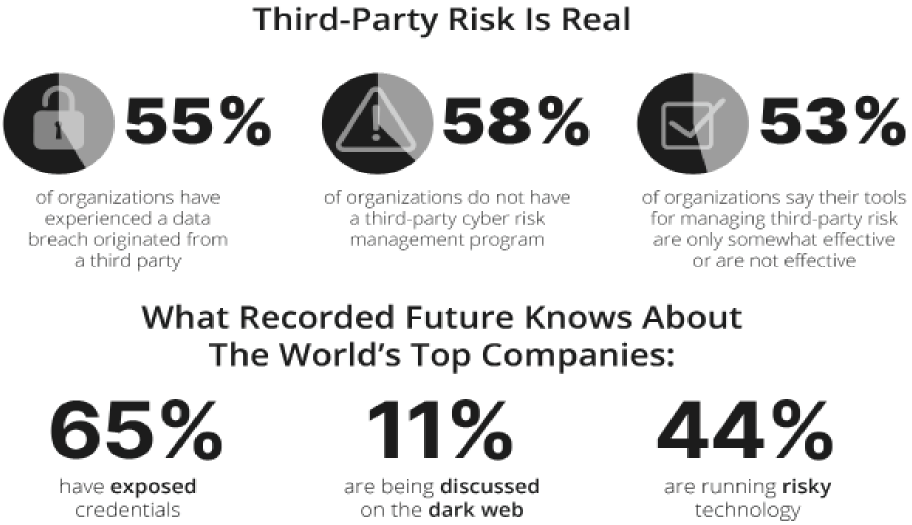


Figure 8-3: Timeline depicting the proliferation of new ransomware families. (Source: Recorded Future)



Third-Party Risk Is Real

55% of organizations have experienced a data breach originated from a third party

58% of organizations do not have a third-party cyber risk management program

53% of organizations say their tools for managing third-party risk are only somewhat effective or are not effective

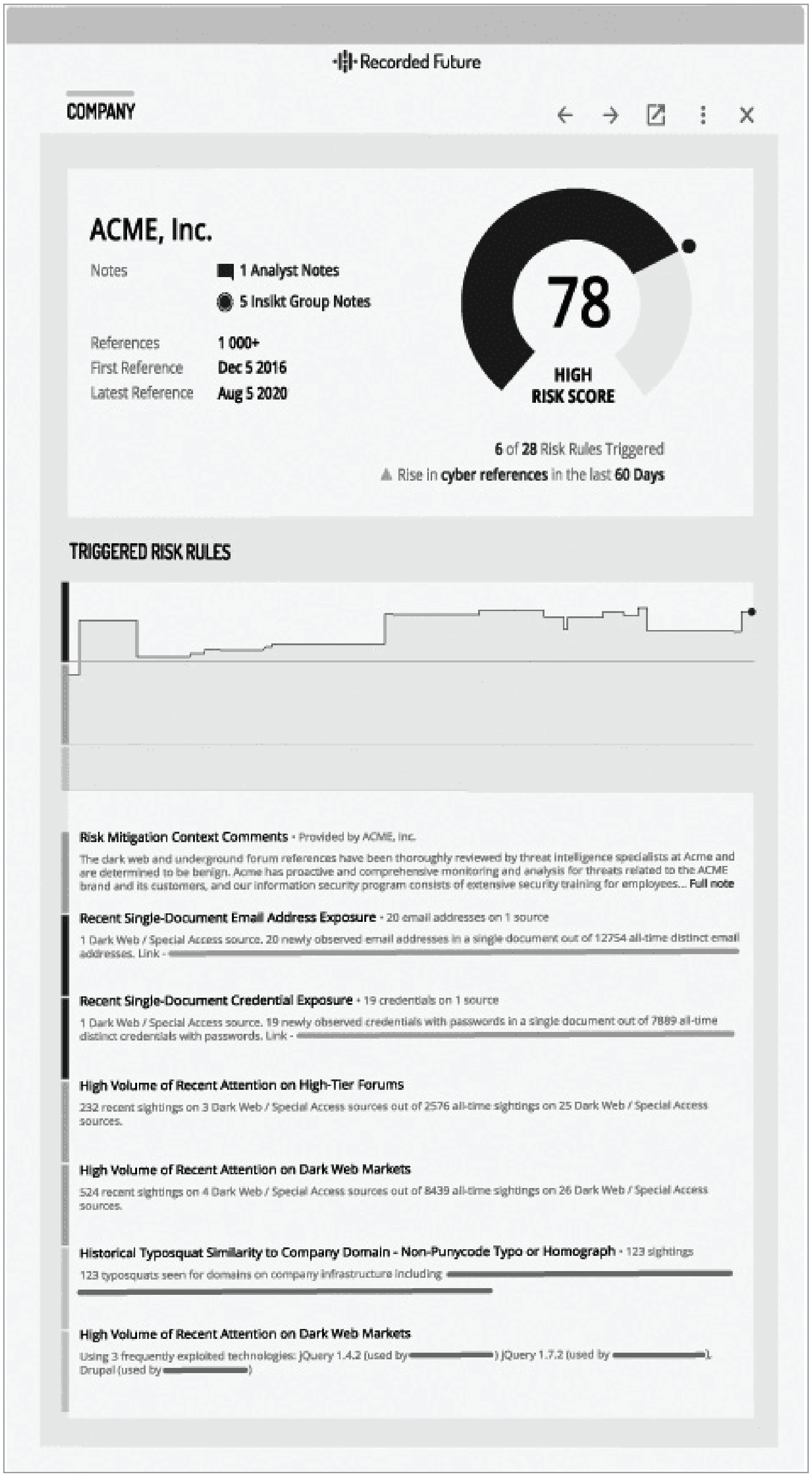
What Recorded Future Knows About The World's Top Companies:

65% have **exposed** credentials

11% are being **discussed** on the **dark web**

44% are running **risky** technology

Figure 9-1: Most organizations are exposed to significant risks through their relationships with third parties.
(Sources: Ponemon Institute and Recorded Future)



ACME, Inc.

Notes: 1 Analyst Notes; 5 Insikt Group Notes

References: 1 000+

First Reference: Dec 5 2016

Latest Reference: Aug 5 2020

78 HIGH RISK SCORE

6 of 28 Risk Rules Triggered

▲ Rise in cyber references in the last 60 Days

Risk Mitigation Context Comments • Provided by ACME, Inc.

The dark web and underground forum references have been thoroughly reviewed by threat intelligence specialists at Acme and are determined to be benign. Acme has proactive and comprehensive monitoring and analysis for threats related to the ACME brand and its customers, and our information security program consists of extensive security training for employees... **Full note**

Recent Single-Document Email Address Exposure • 20 email addresses on 1 source

1 Dark Web / Special Access source. 20 newly observed email addresses in a single document out of 12754 all-time distinct email addresses. Link - [redacted]

Recent Single-Document Credential Exposure • 19 credentials on 1 source

1 Dark Web / Special Access source. 19 newly observed credentials with passwords in a single document out of 7889 all-time distinct credentials with passwords. Link - [redacted]

High Volume of Recent Attention on High-Tier Forums

232 recent sightings on 3 Dark Web / Special Access sources out of 2576 all-time sightings on 25 Dark Web / Special Access sources.

High Volume of Recent Attention on Dark Web Markets

524 recent sightings on 4 Dark Web / Special Access sources out of 8439 all-time sightings on 26 Dark Web / Special Access sources.

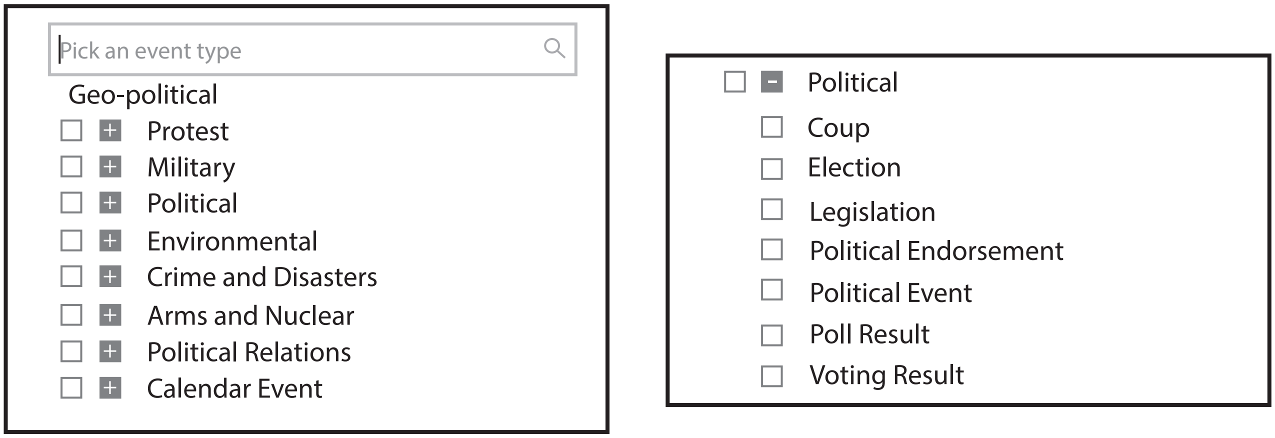
Historical Typosquat Similarity to Company Domain - Non-Punycode Typo or Homograph • 123 sightings

123 typosquats seen for domains on company infrastructure including [redacted]

High Volume of Recent Attention on Dark Web Markets

Using 3 frequently exploited technologies: jQuery 1.4.2 (used by [redacted]) jQuery 1.7.2 (used by [redacted]), Drupal (used by [redacted])

Figure 9-2: Third-party intelligence provides context for identifying shortcomings in the defenses of supply-chain partners.



Pick an event type

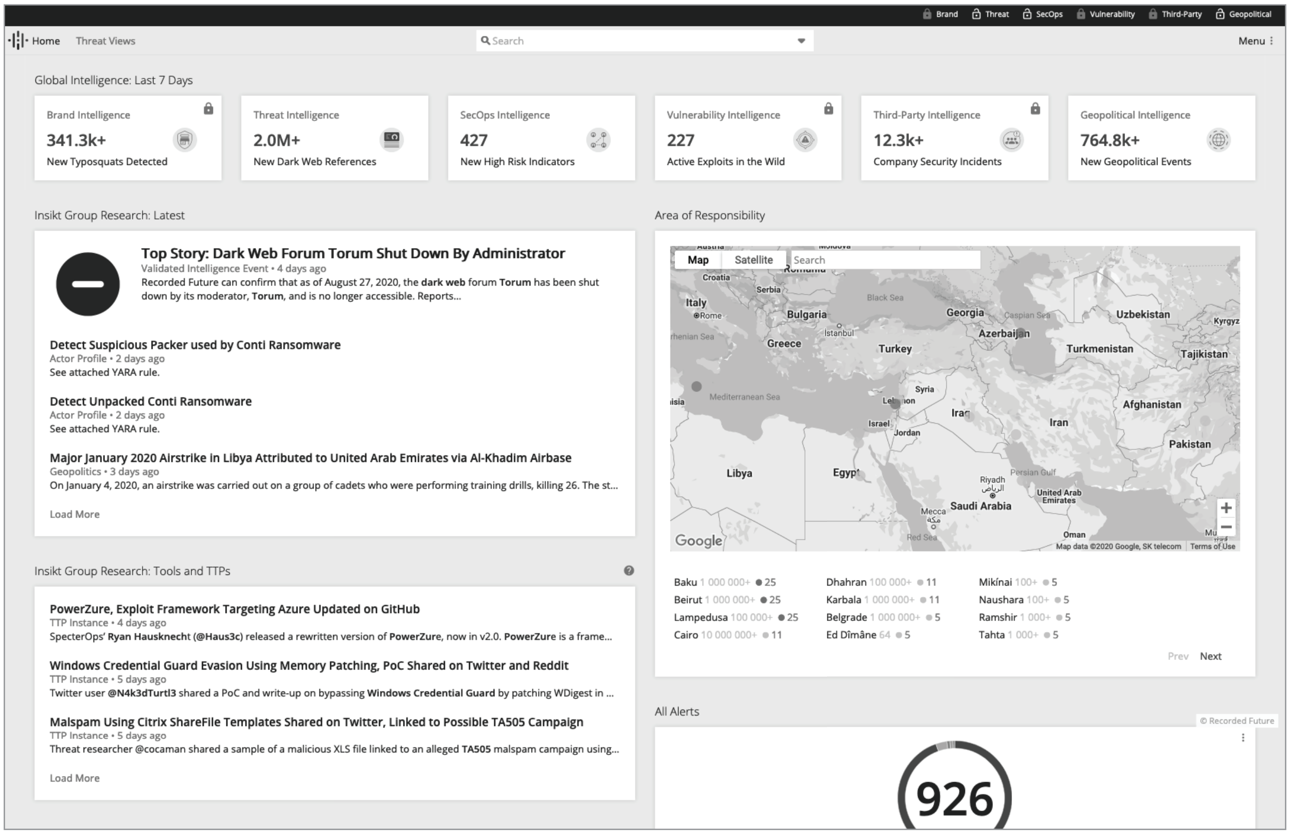
Geo-political

- □ ⊞ Protest
- □ ⊞ Military
- □ ⊞ Political
- □ ⊞ Environmental
- □ ⊞ Crime and Disasters
- □ ⊞ Arms and Nuclear
- □ ⊞ Political Relations
- □ ⊞ Calendar Event

□ ⊟ Political

- □ Coup
- □ Election
- □ Legislation
- □ Political Endorsement
- □ Political Event
- □ Poll Result
- □ Voting Result

Figure 11-1: Examples of geopolitical event categories and the specific items within one category. (Source: Recorded Future)



Global Intelligence: Last 7 Days

Brand Intelligence	341.3k+	New Typosquats Detected
Threat Intelligence	2.0M+	New Dark Web References
SecOps Intelligence	427	New High Risk Indicators
Vulnerability Intelligence	227	Active Exploits in the Wild
Third-Party Intelligence	12.3k+	Company Security Incidents
Geopolitical Intelligence	764.8k+	New Geopolitical Events

Insikt Group Research: Latest

Top Story: Dark Web Forum Torum Shut Down By Administrator
Validated Intelligence Event • 4 days ago
Recorded Future can confirm that as of August 27, 2020, the **dark web** forum **Torum** has been shut down by its moderator, **Torum**, and is no longer accessible. Reports...

Detect Suspicious Packer used by Conti Ransomware
Actor Profile • 2 days ago
See attached YARA rule.

Detect Unpacked Conti Ransomware
Actor Profile • 2 days ago
See attached YARA rule.

Major January 2020 Airstrike in Libya Attributed to United Arab Emirates via Al-Khadim Airbase
Geopolitics • 3 days ago
On January 4, 2020, an airstrike was carried out on a group of cadets who were performing training drills, killing 26. The st...

Load More

Insikt Group Research: Tools and TTPs

PowerZure, Exploit Framework Targeting Azure Updated on GitHub
TTP Instance • 4 days ago
SpecterOps' **Ryan Hausknecht (@Haus3c)** released a rewritten version of **PowerZure**, now in v2.0. **PowerZure** is a frame...

Windows Credential Guard Evasion Using Memory Patching, PoC Shared on Twitter and Reddit
TTP Instance • 5 days ago
Twitter user **@N4k3dTurtl3** shared a PoC and write-up on bypassing **Windows Credential Guard** by patching WDigest in ...

Malspam Using Citrix ShareFile Templates Shared on Twitter, Linked to Possible TA505 Campaign
TTP Instance • 5 days ago
Threat researcher @cocaman shared a sample of a malicious XLS file linked to an alleged **TA505** malspam campaign using...

Load More

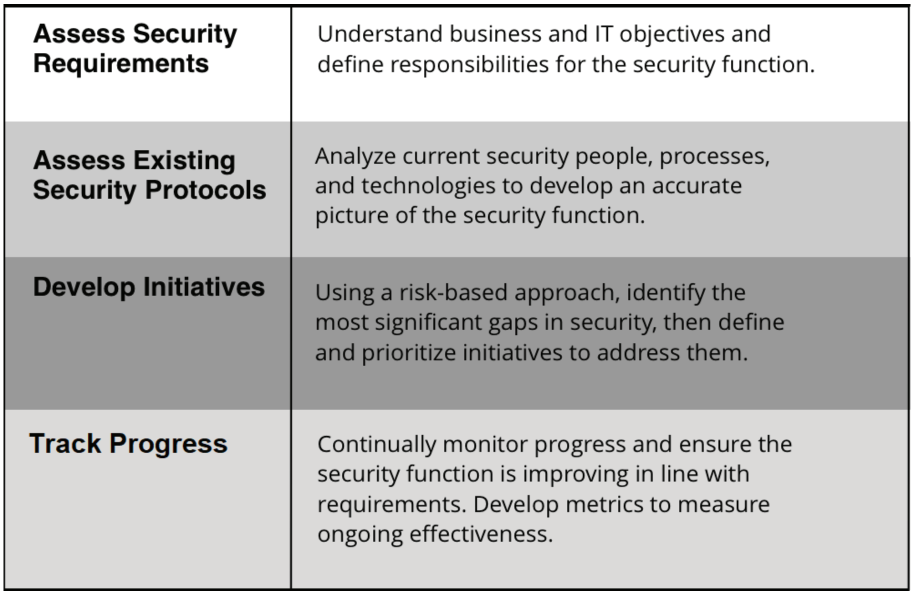
Area of Responsibility

Baku	1 000 000+	● 25	Dhahran	100 000+	● 11	Mikínai	100+	● 5
Beirut	1 000 000+	● 25	Karbala	1 000 000+	● 11	Naushara	100+	● 5
Lampedusa	100 000+	● 25	Belgrade	1 000 000+	● 5	Ramshir	1 000+	● 5
Cairo	10 000 000+	● 11	Ed Dîmâne	64	● 5	Tahta	1 000+	● 5

All Alerts

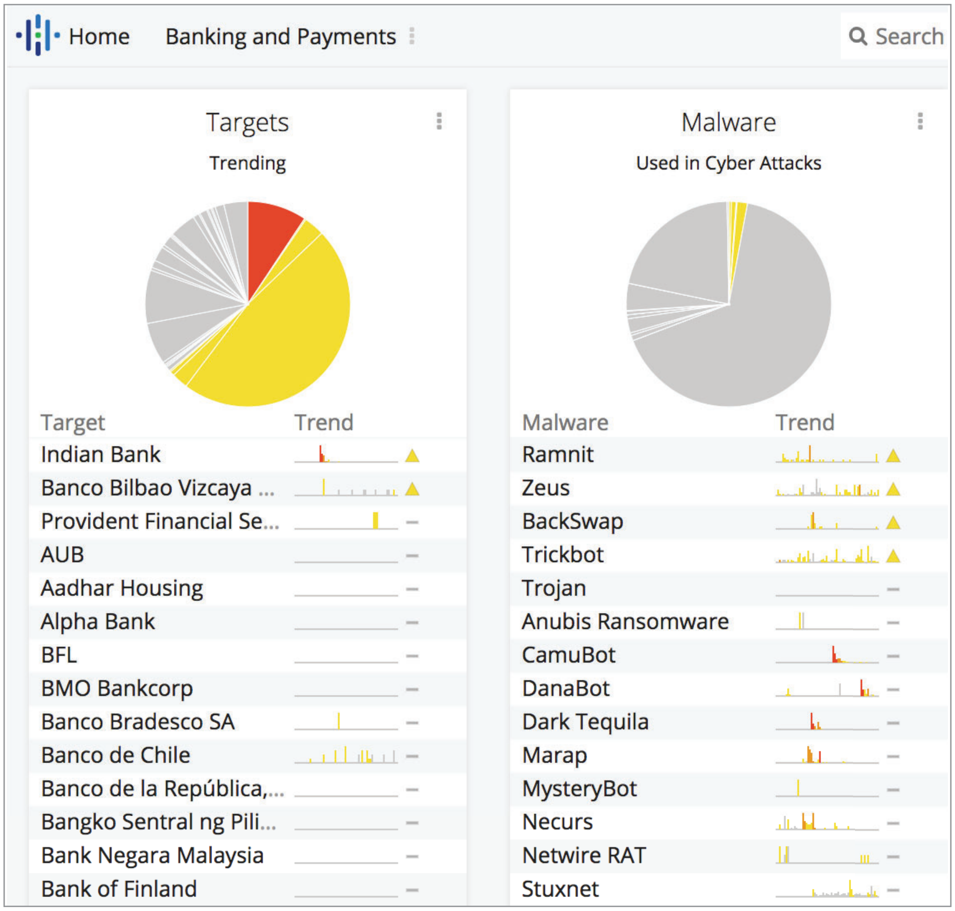
926

Figure 11-2: Example of a dashboard that highlights high-risk areas. (Source: Recorded Future)



Assess Security Requirements	Understand business and IT objectives and define responsibilities for the security function.
Assess Existing Security Protocols	Analyze current security people, processes, and technologies to develop an accurate picture of the security function.
Develop Initiatives	Using a risk-based approach, identify the most significant gaps in security, then define and prioritize initiatives to address them.
Track Progress	Continually monitor progress and ensure the security function is improving in line with requirements. Develop metrics to measure ongoing effectiveness.

Figure 12-1: A standard approach to assessing risk and developing a security strategy.



Targets

Trending

Target	Trend
Indian Bank	▲
Banco Bilbao Vizcaya ...	▲
Provident Financial Se...	–
AUB	–
Aadhar Housing	–
Alpha Bank	–
BFL	–
BMO Bankcorp	–
Banco Bradesco SA	–
Banco de Chile	–
Banco de la República,...	–
Bangko Sentral ng Pili...	–
Bank Negara Malaysia	–
Bank of Finland	–

Malware

Used in Cyber Attacks

Malware	Trend
Ramnit	▲
Zeus	▲
BackSwap	▲
Trickbot	▲
Trojan	–
Anubis Ransomware	–
CamuBot	–
DanaBot	–
Dark Tequila	–
Marap	–
MysteryBot	–
Necurs	–
Netwire RAT	–
Stuxnet	–

Figure 12-2: A security intelligence dashboard pinpoints threats most relevant to a specific industry or technology. (Source: Recorded Future)

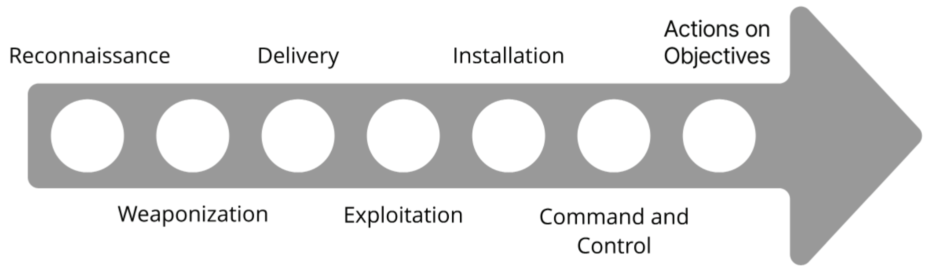


Figure 13-1: Diagram of Lockheed Martin's Cyber Kill Chain framework.

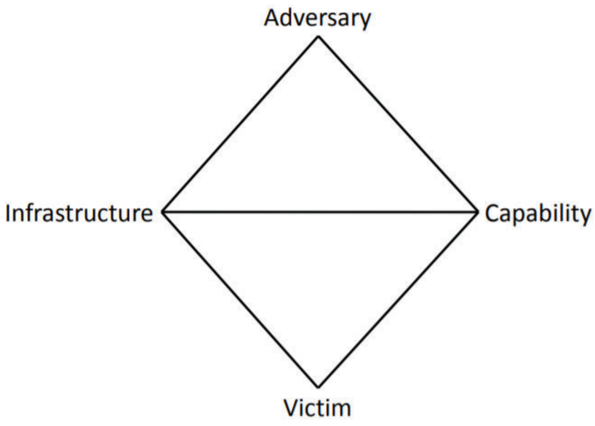
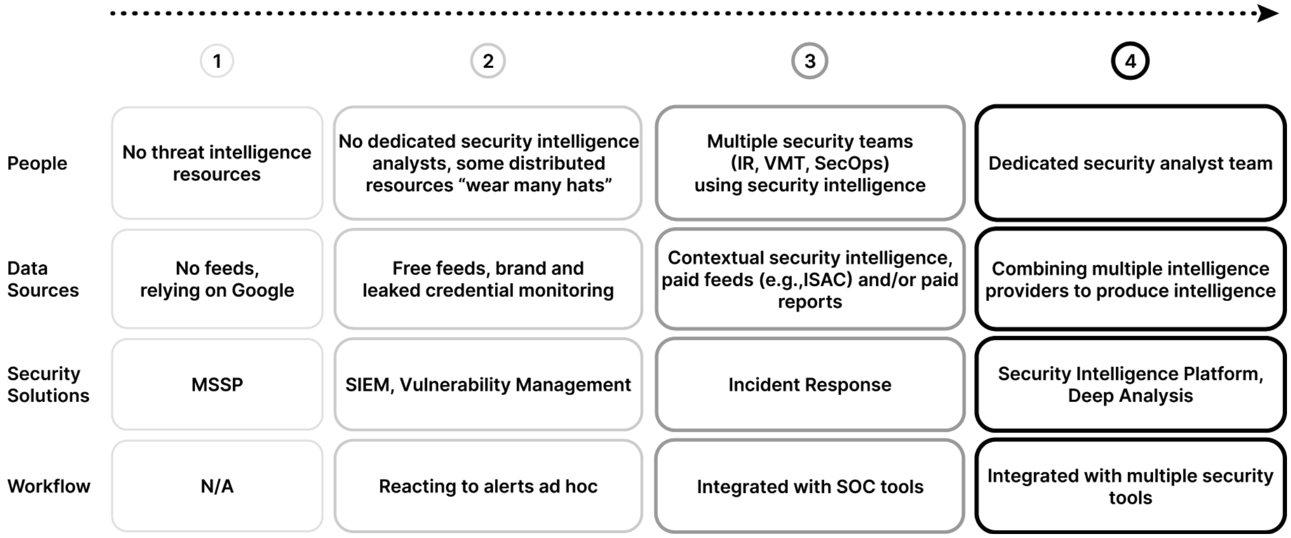


Figure 13-2: A simple Diamond Model design.



	1	2	3	4
People	No threat intelligence resources	No dedicated security intelligence analysts, some distributed resources "wear many hats"	Multiple security teams (IR, VMT, SecOps) using security intelligence	Dedicated security analyst team
Data Sources	No feeds, relying on Google	Free feeds, brand and leaked credential monitoring	Contextual security intelligence, paid feeds (e.g.,ISAC) and/or paid reports	Combining multiple intelligence providers to produce intelligence
Security Solutions	MSSP	SIEM, Vulnerability Management	Incident Response	Security Intelligence Platform, Deep Analysis
Workflow	N/A	Reacting to alerts ad hoc	Integrated with SOC tools	Integrated with multiple security tools

Figure 14-1: Four stages of security intelligence program maturity — from no internal resources to a fully staffed and highly automated program.

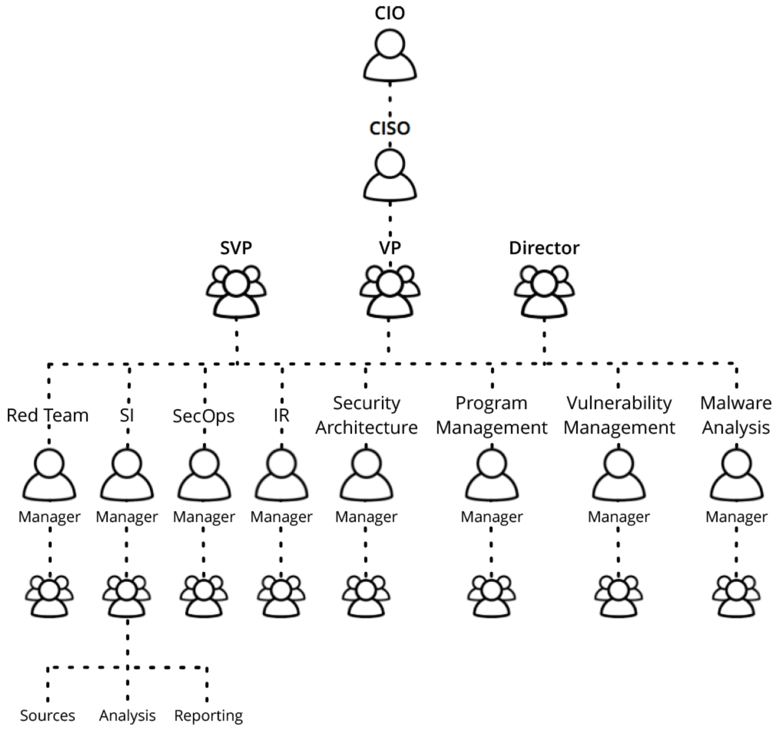


Figure 15-1: Security intelligence as an independent group in the security organizational structure.

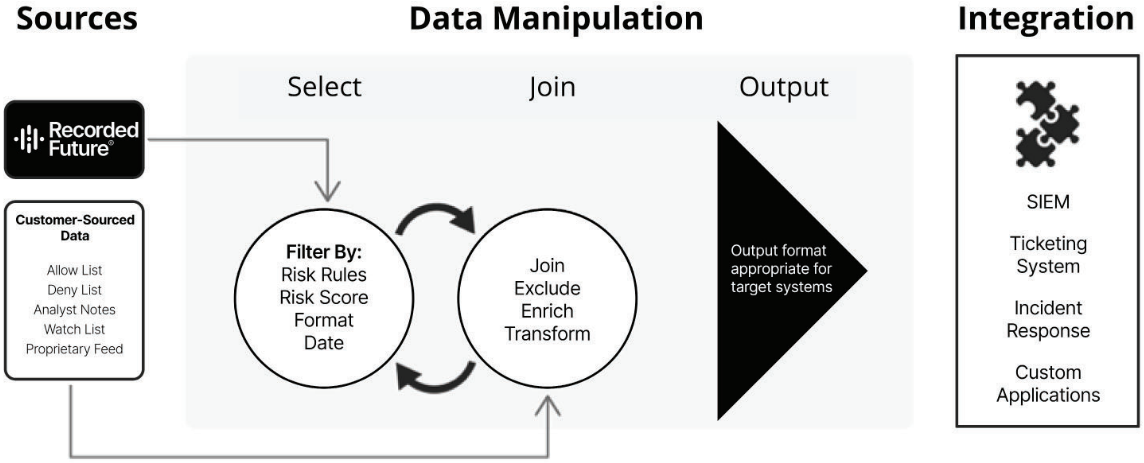


Figure 15-2: A security intelligence platform centralizes, combines, and enriches data, and then formats it for multiple target systems. (Source: Recorded Future)