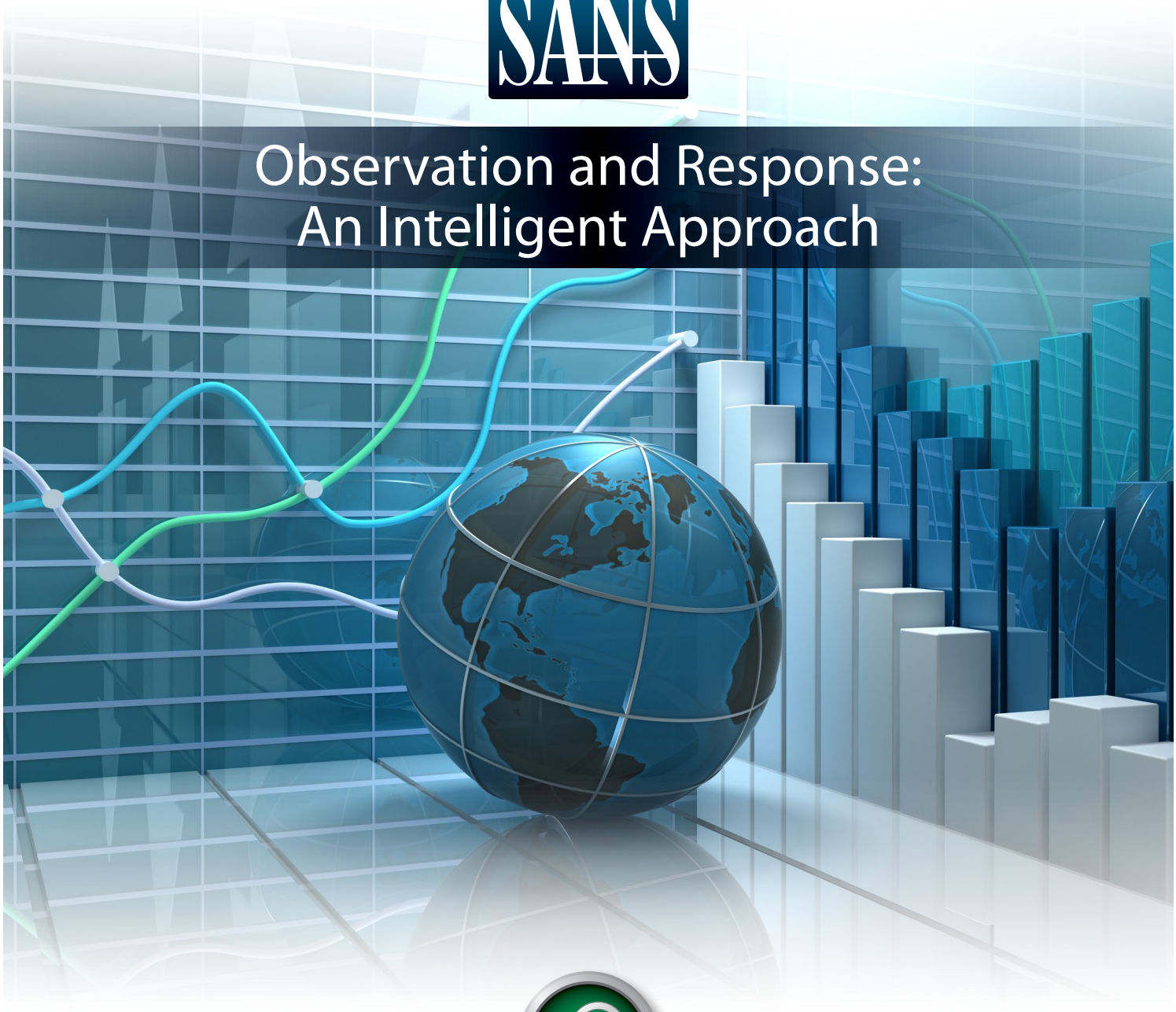
Interested in learning more about security?

SANS Institute InfoSec Reading Room

Observation and Response: An Intelligent Approach

A SANS Analyst Program whitepaper by J. Michael Butler. It discusses how properly focused observation and tracking efforts provide intelligence from inside the enterprise by monitoring for indicators of compromise such as odd point-in-time activities on the network, unusual machine-to-machine communications, outbound transfers, connection requests and many other suspicious activities.



Observation and Response: An Intelligent Approach

A SANS Whitepaper

Written by J. Michael Butler

Advisor: Stephen Northcutt

August 2015

Sponsored by
ThreatStream

Introduction

2015 has been a busy year for attackers. Large health care, insurance, financial, government, retail, hospitality, travel and other big businesses succumbed to lingering, multistage attacks that siphoned sensitive, valuable data out of their enterprise networks.

The victims were well-resourced organizations, in many cases compliant with their regulatory requirements. Nevertheless, the attackers had time to penetrate multiple systems, traverse the networks and even transfer sensitive data out.

This time lapse is what attackers count on. According to the 2015 Verizon Data Breach Investigations Report (DBIR), there is nearly a 75 percent gap between speed to exploit and time to discover. The report said almost 100 percent of attacks were able to compromise systems or fully breach data (send data outside the organization) in less than five days—60 percent were able to compromise their target within minutes. In comparison, less than 25 percent of victim organizations were able to make the discovery in less than five days.[1]

All of these attacks started somewhere, likely at the user endpoint, and took multiple actions that provided indicators of compromise (IOCs). Defenders could have used these IOCs for earlier detection if they were able to observe the IOCs and correlate them with adequate intelligence. Attackers' activities create trails that organizations are likely observing through multiple monitoring technologies, yet administrators often fail to piece together the actions that indicate a compromise is occurring.

Observing, collecting, correlating and tracking these actions and indicators, even though they appear normal to disparate monitoring tools, enables faster response and remediation, particularly when analysts combine the results with information from threat intelligence platforms and other external sources.

[1] Verizon 2015 Data Breach Investigations Report (DBIR), www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf, p. 6, Figure 5.

Observation systems go beyond cause and effect to learn from network traffic, attack targets and the actions and behaviors of the attack—for example, lateral movement, ports and services used or called for and users impersonated. Network defenders can then use this information to update security device rules to block entire classes of behaviors or IOCs. With better observation and tracking of attackers' actions, responders can:

- More quickly get to the root of whether an incident is an in-progress attack or just an abnormality
- Classify targets and attack methods
- Detect and block future iterations
- Develop better security controls for high-value targets

This paper explains why network-based observation and tracking are important to faster response, where observation outside the network is important, and what types of intelligence can augment network observation data for more timely and accurate classification and containment.

Observation starts with detection, but detection is not the problem for most organizations. Typically, multiple detection systems are sending alarms constantly. The issue is knowing what's happening across the network, systems, domains and even the Web in order to connect the dots—in as close to real time as possible—for accurate, effective response.

Monitoring

There are multiple forms of monitoring occurring simultaneously within any organization: Logs are collected from most major applications and OSes, IPS and unified threat management (UTM) systems are watching gateways and endpoint data is being collected via network- or agent-based monitoring.

Honeypots: Old but New Again

Honeypots are a means of contained monitoring and have been around for more than 16 years. They are gaining in popularity among security vendors and organizations with high-value targets and the resources to defend them. Honeypots are decoys designed to appear as legitimate hosts and applications connected to the Internet. Honeynets mimic entire networks, and honeycode mimics tempting targets within applications.

Information from these contained observation environments can prove useful, but they can be detected by attackers, which diminishes their value and creates overhead for the security teams that have to continually update them to prevent attackers from detecting the honey lures.

Network Security Monitoring

For those not using honey technologies, many types of network monitoring tools are already observing and detecting malicious behaviors. VPN systems are monitoring access location, time of day and user information that can also be used in observation and tracking of anomalies (for example, an accounting clerk logs in to a system at 1 a.m.). IDS/IPS and UTM tools, which are constantly updated with new behaviors and signatures, watch for known bad behavior. Their success rate, however, depends on whether they've been kept up to date on known attack signatures, IOCs and patterns of behavior.

The other shortcoming is that these tools are perimeter tools that do not look inward, where malicious activity also takes place. Nor do they look at outbound traffic to detect command and control (C2) activity or outbound sensitive data transfer. Yet outbound traffic can provide a key indicator of compromise that organizations should not miss. Defenders should tune network packet sniffers to look at outbound data transfers, unencrypt headers for further inspection as needed and even unencrypt entire contents so that policies are triggered.

Outside the DMZ

Outside monitoring is equally critical to protect the organization's domains, brand and employees on social media, for example. Organizations typically acquire this type of monitoring, which can be integrated with existing intelligence platforms or services, security information and event management (SIEM) systems, or analytics platforms, as a service through third parties.

Information Sharing

The information drawn from these sources is valuable to all organizations in specific vertical industries.[2] Group efforts always have more resources than a single IT department, so several industries have set up information sharing and analysis centers (ISACs) for industry leaders to share threat information.[3] The financial services ISAC (FS-ISAC) has even automated this information-sharing process through a notification system designed "to speed security alerts to multiple recipients around the globe near simultaneously while providing for user authentication and delivery confirmation."

Intelligence platforms and service providers also correlate and share threat intelligence gathered from multiple sources.

Intelligence

Intelligence (delivered through platforms and services) that looks both inside and outside the organization can help responders drill down to events and systems that need attention while eliminating those they don't need to focus on. Intelligence can include information on known bad IP addresses, known C2 domains, bad file paths and export URLs, for example.

If a device on the network exchanges traffic with a suspicious domain, intelligence can provide additional insight, such as where the domain is registered and other information that would clearly initiate a blocking action against a bad actor—for example, a domain registered to a 10-digit random address at a disreputable email provider that is linked to an IP address with five other suspicious-looking domains. The more visibility you have into relationships pointing to the same conclusion, the more accurate your response.

[2] National Council of ISACs website: www.isaccouncil.org/memberisacs.html

[3] FS-ISAC website: www.fsisac.com/about

Cyberthreat intelligence (CTI) is not just a buzzword. The use of additional intelligence to aid in decision-making is improving visibility, response and blocking, according to the SANS 2015 survey on CTI. See Figure 1.

Please select all the options that describe how the use of CTI has improved your security and response.

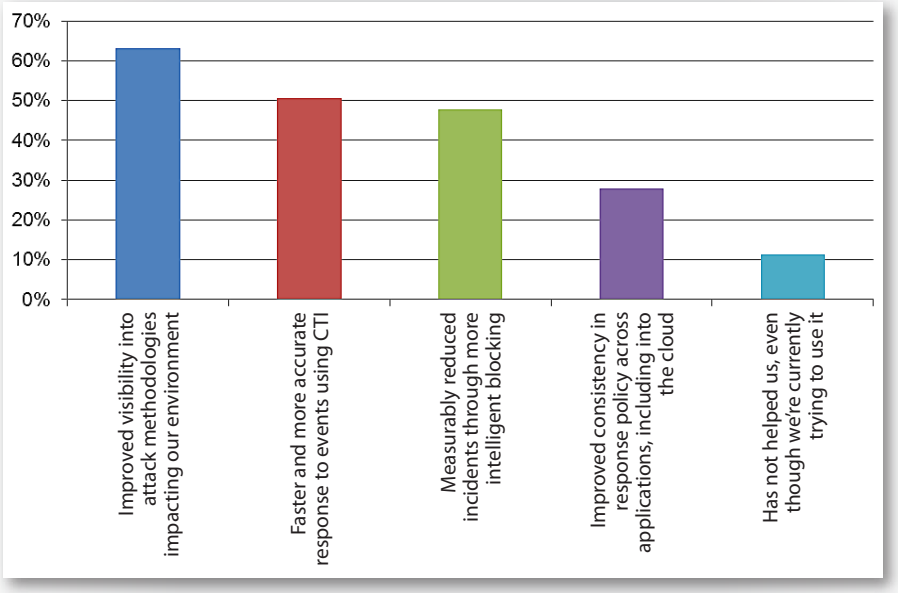


Figure 1. Improvements in Response and Visibility[4]

In the same survey, 75 percent of respondents said that such intelligence would be very useful and be embedded into detection and response over the next five years, while 20 percent said it would be somewhat important.[5]

[4] "Who's Using Cyberthreat Intelligence and How?" February 2015, https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767, p. 14, Figure 8.

[5] "Who's Using Cyberthreat Intelligence and How?" introduction, p. 1.

Just as physical network designs can create defenses in depth using segmentation and other techniques, monitoring is more than just setting some traffic thresholds and waiting for those to trip. Sometimes, organizations need to turn to creative monitoring.

Observe the Targets

Firewalls, IDS/IPS, UTM, server/endpoint monitoring and application monitoring are commonly deployed today, according to multiple SANS surveys. The problem for most organizations is their inability to tie together events reported by these systems, causing them to miss the bigger picture. Analytics and intelligence go only so far without additional observation of the attacker attempting to open files, hide activities and processes, access data and transfer it out.

Many observation practices go beyond the internal network with searches of cloud services, social media, domain registrations and other areas where attackers gather intelligence about their victims. Such services can monitor DNS for changes in the WHOIS registration, administrator contacts and other signs that the DNS infrastructure is under attack. They can also monitor social media platforms for adverse intent or early warnings of attacks.

Domain Registrations

Domains are fair game for attackers who hijack domain registrations to redirect traffic from a legitimate site or tap into traffic. Some will comb publicly available registration data searching for email addresses or other valuable information that can further an attack. In some cases, domain hijackings can last for months before detection because IT groups don't regularly check on the status of registrations.

It's important to know all domains you have registered and in use, as well as their associated IP blocks. You can deploy your own team or a monitoring or intelligence service or platform to search for change attempts or new versions of your company name being issued under new domain registrations. Intelligence and reputation service providers often offer this as part of their service.

ADVICE

Monitor for adversary-created domain registrations or changes, or unauthorized use of your company name. Register similar URLs to prevent impersonation. As well, watch for unauthorized changes in the registration details of your existing domains, including contact information.

[6] "4 Ways to Prevent Domain Name Hijacking," CIO, Feb. 1, 2012, www.cio.com/article/2399853/security0/4-ways-to-prevent-domain-name-hijacking.html

IRC and Other Forums

A complete understanding of targets, methods and vulnerabilities attackers will exploit requires human intelligence gathering via places for underground sharing of attack information, such as IRC and other channels. This is a difficult and risky undertaking for organizations without properly trained staff, so organizations typically use an external service or intelligence platform. Well-resourced IT groups, external research groups, enterprise management services, vulnerability and detection vendors, and intelligence services or platform providers have experts deeply embedded within these criminal underground groups to collect information and use it to develop early detection and defenses.

ADVICE

Engage a service that monitors IRC and other places known to host exploit forums and groups discussing current threat information.

Cloud

Big data applications in the cloud are impossible to ignore. Organizations are adopting cloud-based technologies for their big data implementations, migrating between public and private clouds, but they are finding that they are unable to observe these programs for IOCs and anomalies from internal network monitoring systems. The key is working with cloud providers as well as monitoring and intelligence technologies that will extend visibility into the cloud. The intelligence platform should support this in much the same way it applies intelligence to other enterprise monitoring data.

ADVICE

Work with intelligence platform providers that can track misbehavior in the cloud and unify actionable data across cloud and non-cloud applications involved in the attack.

Social Media

Social media is a rich source of intelligence for both attackers and defenders. In recent years, law enforcement organizations have been collecting intelligence from social media to further their cases.[7] On the other hand, the cadre of underground users who gather social media intelligence for nefarious reasons should concern any organization.

Attackers use social media to mine information about companies (and ultimately access to a company) through their social media pages. Or they can target individual employees. By targeting employees' personal data in social media, attackers can easily find information they can use to reset passwords and break into accounts.

Malware can lurk on social media sites as well, waiting for the unsuspecting user to pick it up. In some cases, attackers may tip off their intentions through insulting posts, or posts about "hacks," "leaks" and "breaches." You can observe and use attacker posts to predict attacks, analyze attacks in progress or find new vulnerabilities.

Augment intelligence collected outside the organization with observations of social media. Disgruntled former employees, hacktivists and others may tip their hands on social media and alert potential target organizations.

ADVICE

Monitor social media for misuse of your brand and URLs, and watch for signs of harmful intent toward your company or users.

Email

Email systems and all their user information are also rich targets for attackers. Email security systems can protect against known bad attachments, links and reputational information based on the sending IP addresses. However, this area also enables better accuracy and response when organizations use additional observation technology with intelligence.

[7] "Developing Policy on Using Social Media for Intelligence and Investigations," The Police Chief, June 2013, www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2951&issue_id=62013

Rich Graves, information security officer at Carleton College and the College of St. Olaf in Minnesota, describes in a recently published paper the use of an observation system to track inappropriate activity on email systems. When a user came into his real email environment with questionable parameters—country of origin or a suspicious token—the user was redirected to a honeypot email system that generated credentials the attacker thought were real. With that, Graves and his team detected 17 logins from Nigeria, as well as 20 sets of fake "honey" credentials attempting access over three months. The discovery deterred the attackers from actually getting to anything important and enabled Graves and his team to use the attackers' IP address information to block them in the future.[8]

ADVICE

Consider all ways to monitor a system. Watch for attempted spamming activities from your email system as well as alterations of email account preferences, servers or administrators, as these can be indicators of compromise. When using web-based email, monitor browser and system information for users accessing the webmail interface to ensure legitimate users are making the access requests.

Endpoints

User endpoints and servers hosting corporate financial data, customer information, employee records and other competitive materials provide rich targets that attackers can monetize with ease on the so-called *darknet*, the private, anonymous, nontrackable underbelly of the Internet where one may share information with impunity. It's not enough to focus on the devices inside your perimeter; user endpoints outside of the protected network should also be included in the observation program.[9] Suspicious processes to observe on the endpoint include (but are not limited to):

- DNS caches
- Open sockets
- Changes to registry keys
- Multiple processes or updates occurring simultaneously that should not be running
- Access requests
- File or system changes

[8] The system also detected 16 logins from Nigeria with real passwords, and those were also directed to the honeypot. "Honeypots and Honey Tokens for Webmail ID/IR," May 2015, www.sans.org/reading-room/whitepapers/email/honeytokens-honeypots-web-id-ih-35962, p. 14.

[9] "Shutting the Backyard Gate – Reducing the Risk to Corporate Data from Employees' Compromised Home Networks," scheduled for publication in September 2015.

This is where a threat intelligence platform can provide shared data to be used to search for endpoint issues.

ADVICE

Provide your technical team with search tools, along with targets of interest, to help them focus on specific issues and compromised endpoints quickly and effectively.

Access and Authentication

Remote access applications are a common target because they offer a way into the network that looks legitimate to security monitoring systems. Remote access credentials are the biggest treasure for attackers because they can use them to log in as a seemingly legitimate user from anywhere.[10] Since 2010, attacks involving credentials have become the top attack methodology, according to the 2015 Verizon DBIR.[11]

Observation of these access points should include user information, IP address and geolocation of the device requesting access, time of day, username/password and other credentials used for access, application requests and other activities occurring inside the network after access is granted.

ADVICE

Monitor endpoints for signs of breach, location, time of day and the systems/applications being requested.

Outbound Communications

Network-focused tools such as packet analyzers are usually set up to watch inbound traffic and traffic between devices on the internal network. However, it's just as critical to monitor outbound connections, particularly over commonly used ports. Specifically, watch the egress points where attackers can exfiltrate sensitive data. Such outbound transmissions can lead investigators to other infected devices or, if the attacker is sloppy, to the attacker's server itself.

[10] They can also enter temporarily through an open session if they have full control of the endpoint during the session.

[11] 2015 Verizon DBIR, www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf, p. 5, Figure 4.

More important, unauthorized outbound activity is one of the most common indicators of compromise occurring at an organization's perimeter. Ports, pathways and connections to external devices can all provide IOCs and valuable observation data when malicious activity is present. Destination and source are critical, as well as the data itself and who is attempting to send it out.

ADVICE

Monitor all outbound communications and connections for to/from information, looking for new data pathways between servers and outbound past the perimeter. Watch for encrypted outbound traffic, time of day and sender information, noting applications from which the data originated.

Integrating Observation and Intelligence

Intelligence comes in many forms—either in a platform model or through services or even security vendors that provide intelligence to their products and clients directly. According to the SANS 2014 Analytics and Intelligence Survey, respondents who reported using specific threat analytics tools overwhelmingly selected "finding new or unknown threats" as their most valuable use case.[12] Finding the unknown is critical to every enterprise: The 2015 Verizon DBIR indicates that 70 to 90 percent of malware samples were "unique to a single organization," so signature-based technologies would have to be aware of and follow all of these in order to provide rules to block them.

Using the Observation Data

Any system an organization selects as an intelligence platform must accumulate, normalize, aggregate and categorize data from a variety of systems, some of which include:

- OS and applications
- Access and authentication
- Network monitoring
- Honey observation systems
- External intelligence sources or platforms
- Information gathered from darknet sources
- Reputational data
- IDS/IPS, firewalls and UTM systems
- Endpoints

This isn't a comprehensive list of data sources; creative thinking in this stage will reward analysts and investigators.

[12] SANS 2014 Analytics and Intelligence Survey, October 2014, www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507, p. 16, Figure 11.

[13] 2015 Verizon DBIR, www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf, p. 22.

Standardizing the Data

The ability to normalize and reuse data collected through observation is now supported through standards being adopted by tool vendors. Standards actively promoted by Mitre and ISAC organizations include:

- **Structured Threat Information eXpression (STIX)—**Language for representing structured threat information, whereby machine-readable formats are applied to sensor readings with the aim of capturing threat indicators[14]
- **Trusted Automated Exchange of Indicator Information (TAXII)—**Transport mechanism for STIX-based threat information, enabling secure sharing of data in real time[15]
- **Common Attack Pattern Enumeration and Classification (CAPEC)—**Dictionary and taxonomy of attacks[16]

Tool vendors using these standards and taxonomies are making it possible to unify the data into strings that indicate compromise, for example.

Analyzing the Data

There are many systems for analyzing observation data, including analytics and intelligence platforms, SIEM systems or a combination of manual and automated processes that may or may not include central collection and visibility. According to the 2014 SANS Analytics and Intelligence Survey, this is typically conducted through a SIEM system.

Edward Pardo, a senior IT security engineer in western New York, used his SIEM system for correlating his observation data for faster response and user policy enforcement. With this information, he was able to detect problems and analyze them within minutes. Benefits included:[17]

1. **Reduced time to alert.** Pardo's organization collected syslog data from more than 6,000 systems to watch for 1,300 different error conditions. Any such error caused the SIEM system to send an SNMP trap to the operations console, automatically creating a service ticket. From event to alert: about 30 seconds.

[14] STIX project website: http://stix.mitre.org

[15] TAXII project website: http://taxii.mitre.org

[16] CAPEC project website: http://capec.mitre.org

[17] Email interview with Edward Pardo.

2. **Enforced account use policies.** By looking for simultaneous logins to multiple PCs, Pardo found a user who was sharing account credentials and access to network shares in violation of policy, and was able to educate the user and change his behavior.
3. **Enforced data retention policies.** An engineer was repeatedly deleting the system logs, trying to make more space available, but the deletions set off alarms. Early discovery of the deletions led to quick remediation without any false positives or extra investigation.
4. **Enforced appropriate use policies.** Pardo analyzed the traffic of a legacy FTP server, finding the majority of its use was non-business. After informing users that activity was monitored, the legacy system's use went to almost zero and the FTP server was retired.

This SIEM-driven data correlation helped Pardo's organization make improvements where needed, while saving time that was previously wasted on false alarms.

What system-based intelligence should you gather? Pretty much everything. To get a full view of what's really happening during an event, you need to monitor activity in every corner of your network.

Detecting Signs of Attack

Of course, the place to start is with critical system logs, especially those from the OS and applications on outward-facing systems. Application logs you should carefully examine include those from DNS, email and web servers, as well as any other software those systems may use. These don't need to be outward-facing to pose a threat, so be sure to scrutinize staging and development systems and other seemingly unimportant systems. Attackers may use "unimportant" vectors as launching pads for a backdoor attack.

Even the logs of internal network hardware, including switches and routers, can yield useful intelligence, especially when you're faced with the possibility of an adversary hopping from one VLAN to the next. Other examples revealing signs of access abuse include authentication and VPN logs.

Finally, and perhaps most obviously, examine the logs from open source or commercial forensic tools designed to perform any of the following:

- Locate and reveal suspicious or anomalous behavior.
- Acquire and analyze contents of memory.
- Acquire and analyze data from either active environments or dead drives.
- Establish "super timelines" for suspicious activities by combining logs from multiple sources covering the same time period to correlate activities and events that may lead to IOCs.

Augmenting IOCs with intelligence provided by a platform or service can highlight the difference between suspicious events and real events. For example, an intelligence provider can correlate outbound connections with broadcast IP addresses, IP addresses known as the source of brute-force SSH attacks and IP addresses used for scanning to determine whether your organization could be breached and provide direction for further investigation.

Examples of Observation Systems

To supplement logs, observe attacker behaviors, including crawling the Web or building honeypots for malicious users. Analysts can then aggregate the data collected from these systems with the data already obtained through other security monitoring systems and additional intelligence services, as discussed previously.

Attracting the Malicious User

Various lures can attract malicious users into a honeypot or honeynet or into honeycode simulating a real application; such lures should appear rich in exploitable (realistic, albeit fake) data, including:

- Source code samples
- Admin passwords
- Embedded contact lists
- DNS, email and other target apps
- Customer or employee data

As security analyst Lenny Zeltser points out, a well-built observation system can do the following:

- Slow down intruders' progress by having them waste time.
- Decrease the rate of false positives that plague IDSes.
- Capture malware samples for analysis.
- Help you understand intruders' intentions by enabling you to observe their interactions.
- Watch your own users to see if they visit malicious websites.

The most challenging aspect of deploying such systems, in Zeltser's estimation, is preventing their use as launching pads for attacks.[18] Monitoring and hygiene of these observation systems is discussed in Critical Security Control 5, Malware Defenses:

> *Security personnel should continuously monitor these [honeypot] tools to determine whether traffic is directed to them and account logins are attempted. When they identify such events, personnel should gather the source address from which this traffic originates and other details associated with the attack for follow-on investigation.*[19]

[18] "Stopping Malware on Its Tracks," Larry Zeltser, March 2008, https://zeltser.com/stopping-malware-on-its-tracks

[19] "The Critical Security Controls for Effective Cyber Defense," Version 5.1, www.counciloncybersecurity.org/bcms-media/Files/Download?id=a52977d7-a0e7-462e-a4c0-a3bd01512144, pp. 34–38.

Web Behavior Analytics

Researchers at the U.S. Naval Research Laboratory observing behavioral patterns of web users determined that they could track and identify people through their online habits:

> *As our interaction with the Web becomes more natural and even mediates our interaction with others, we claim that Web browsing behavior can be rich enough to uniquely characterize who we are through unconscious behavioral patterns and authenticate ourselves with a cognitive fingerprint.*[20]

Both semantic as well as syntactic patterns of the user enter into the equation, including the following parameters:

- Number of page revisits
- Number of pages between revisits
- Burstiness (changes of pause time between page views)
- Statistical studies of arrival time, length of session, day of the week and similar metrics

All of these fall under syntactic patterns that analysts can use to determine signs of malicious intent and attempts at compromise.

Social networks can aid in removing the cloak of anonymity, as well. However, while "individual features of Web browsing behavior are not individually or collectively strong enough to authenticate and distinguish users," methods exist that can "dramatically improve those results,"[21]

Web browser "fingerprinting" can provide a good deal of information about the attacker, or at least the browser the attacker is using, without relying on easily changed User-Agent identifiers. One proof-of-concept project collects statistics from the visitor's browser via the HTML5 Canvas element, providing information based simply on pixel mapping.[22]

[20] "User Authentication from Web Browsing Behavior," August 2013, www.nrl.navy.mil/itd/imda/sites/www.nrl.navy.mil.itd.imda/files/pdfs/UserAuthenticationFLAIRS.pdf, p. 1.

[21] "User Authentication from Web Browsing Behavior," p. 6.

[22] "Client-Side: HTML5 Canvas Fingerprinting," 2014, www.browserleaks.com/canvas

Collaborative and Outside Services

In addition to ISACs, many other outside services provide intelligence that can help with the task of attribution. Public and free sources include:

- **InfraGard—**an FBI-sponsored group for sharing computer intelligence[23]
- **U.S. Department of Homeland Security—**which offers various information sharing resources[24]
- **Government-led computer emergency response teams, or CERTs—**which often act as the primary clearinghouses for officially disseminated threat intelligence[25]
- **Assured Information Sharing Lifecycle (AISL)—**a project involving faculty and students from six universities, with the goal of better understanding—and eliminating or reducing—the barriers that hinder sharing security, privacy and policy information[26]
- **U.S. General Accounting Office (GAO)—**which provides documentation on global cybersecurity[27]

The variety of data sources for threat intelligence may be overwhelming right now, but delivering and normalizing that data becomes easier with each advance in standards and technology. One remaining challenge is figuring out what to do with all the data.

Code of Ethics

Ethics—the study of what people ought or ought not to do—apply to every facet of life, whether they take the form of official statements, as one sees on the SANS or GIAC websites, or just generally accepted practices.[28] Observation and tracking programs will benefit from a code of ethics that provides clear guidance on how much to observe and how far to track bad actors beyond the perimeter.

Many existing ethics codes for IT lack "wiggle room" for the kind of monitoring this paper discusses. This points to a need for further work to define and standardize a code of ethics for such monitoring.

[23] InfraGard website: www.infragard.org

[24] DHS website, www.dhs.gov/topic/cybersecurity-information-sharing

[25] Examples: Australia at www.cert.gov.au/services; United Kingdom at www.cert.gov.uk; U.S. at www.us-cert.gov

[26] AISL project page: http://aisl.umbc.edu/show/page/id/faq/FAQ.html

[27] "United States Faces Challenges in Addressing Global Cybersecurity and Governance," July 2010, www.gao.gov/products/GAO-10-606

[28] SANS' ethics statement: www.sans.org/security-resources/ethics.php; GIAC's ethics statement: www.giac.org/about/ethics/code Also, consider that in the absence of an official policy, an accepted practice fills that role.

Conclusion

Tracking and observation of the behavior of attackers—both inside and outside the network—are critical in today's fast-paced threat environment where numerous breaches have occurred against even organizations with deep security resources.

Properly focused observation and tracking efforts provide intelligence from inside the enterprise by monitoring for indicators of compromise such as odd point-in-time activities on the network, unusual machine-to-machine communications, outbound transfers, connection requests and many other suspicious activities. Security teams can use honeycode, honeypots and honeynets to observe bad actors in a secured environment. Observation beyond the perimeter should include domain registries and services, the darknet, social media and other nontraditional locations for signs of intent, abuse of brand and new threat information.

Most often, these external-facing observation systems are implemented by third-party intelligence platform or service providers, which correlate their clients' observation data against intelligence gathered on bad domains, IP addresses, actions and code. With deeper observation and analytics, responses can be more accurate and timely. Security teams can also use this level of intelligence to improve the network risk posture.

About the Authoring Team

Stephen Northcutt founded the GIAC certification and served as the founding president of the SANS Technology Institute, an accredited graduate school focused on cybersecurity. He maintains the SANS Leadership Laboratory, leads the Management 512 Alumni Forum and is the lead author/instructor for a variety of SANS Institute courses. Stephen is the author/co-author of *Incident Handling Step-by-Step*, *Intrusion Signatures and Analysis*, *Inside Network Perimeter Security (2nd Edition)*, *IT Ethics Handbook*, and *Network Intrusion Detection (3rd Edition)*. He was the original author of the Shadow intrusion detection system before accepting the position of chief for information warfare at the Ballistic Missile Defense Organization.

J. Michael Butler is a SANS analyst and instructor who has also been involved in writing SANS security training courseware, position papers, articles and blogs. He is an information security consultant with a leading provider of technical services for the mortgage industry. His responsibilities have included computer forensics, information security policies (aligned to ISO—the International Organization for Standardization—and addressing federal and state disclosure laws), enterprise security incident management planning, internal auditing of information systems and infrastructure, service delivery and distributed systems support. He holds the GCFA, CISA, GSEC and EnCE certifications.

Sponsor

SANS would like to thank this paper's sponsor:

Last Updated: March 19th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Boston Spring 2018	OnlineMAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced