Deloitte.

Responding to Cyber Escalation Proactively
Cyber Breach and Attack Simulation (BAS)

Safebreach Cyber Validate Conference

April 28, 2022

Shields Up

Organizations, regardless of size, should take an **enhanced security stance, especially considering geopolitical tensions**, as cyber attacks represent a growing threat.

- Dynamic situation and not completely clear yet how increased cyberattacks might overlap—or even directly target—businesses
- Department of Homeland Security US Cybersecurity and Infrastructure Security Agency (CISA), “Shields Up” warning to businesses
- Warning from the White House on potential threats

BAS is an important part of Shields Up

https://www.cisa.gov/shields-up
https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity

Protecting the enterprise

Organizations should take steps to prioritize the **update technical protections**, **communicate elevated risk levels** with employees, and **refresh processes to be ready** in the event of an attack by considering

Priority actions for cybersecurity teams

Security Functions

- 🔵 Increase vigilance and proactively update systems
- 🟢 **Reduce digital footprints**
- 🟢 **Confirm ingress and egress points**
- 🔵 Pay close attention to intel collection from government bodies
- 🔵 Identify relevant local and federal law enforcement to report a cyber incident
- 🔵 Revise Incident Response (IR) playbooks
- 🟢 **Confirm 24/7 security operations coverage/proactive threat hunting**
- 🟢 **Practice your organization’s cyber capabilities**

Breach Attack Simulation

Support across the enterprise

BAS has **cross-functional application to support other teams**

Priority actions for other functions in collaboration with security teams

Operations functions

- Evaluate supply chain impacts associated with sanctions/vendors
- Determine supplier and customer interdependencies with organizations
- Prepare crisis command and response teams to be ready

Human Resources/ Talent functions

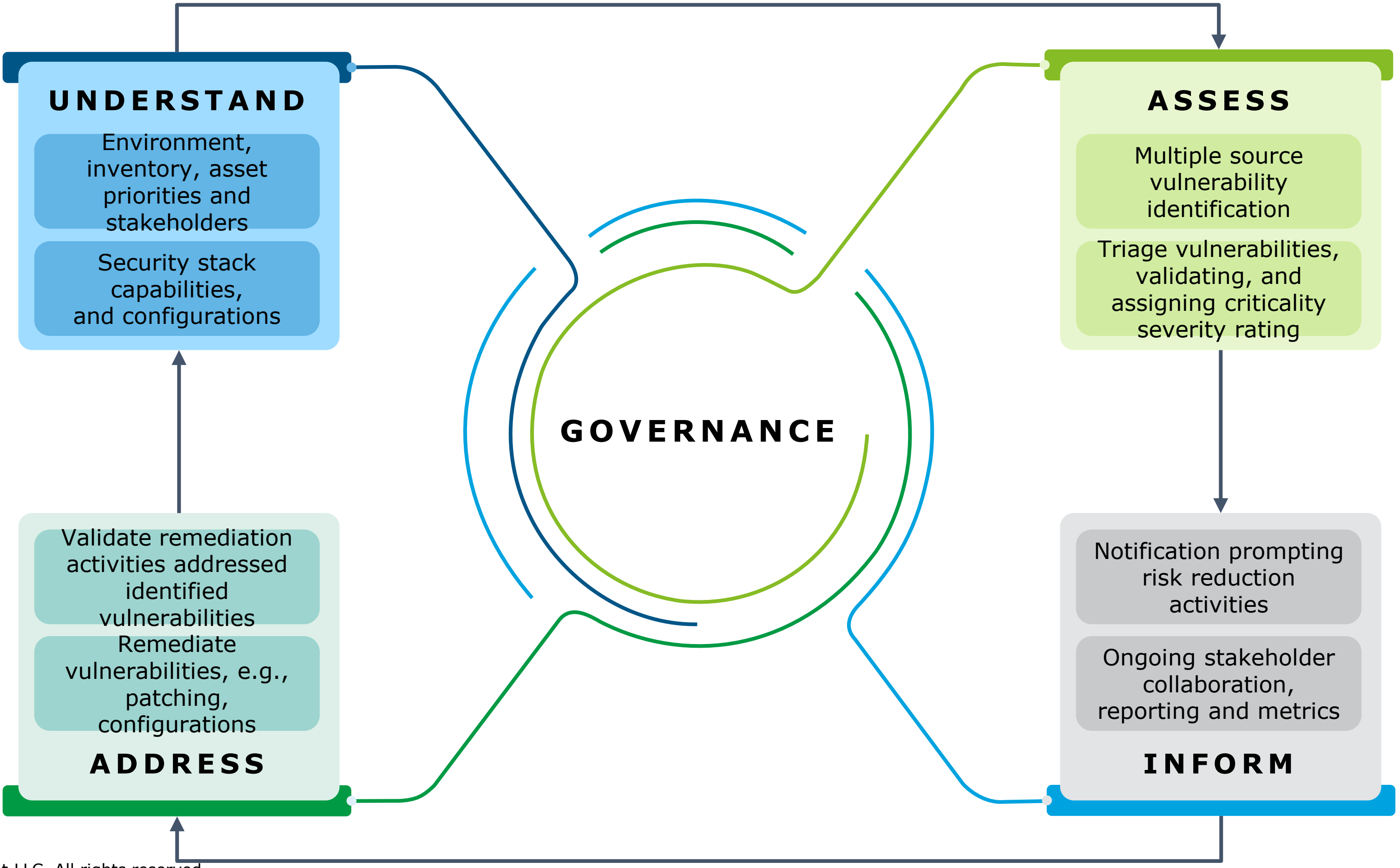
- Cyber mental health.   Evaluate shift schedules of security teams to confirm coverage while avoiding overstrain - security teams are subject to talent shortages, burnout, and higher turnover
- Evaluate security training of security personnel to determine opportunities to expand experiences for active adversary engagement

Boards and Executive Leadership teams

- Review a security dashboard of current communication, crisis, risk management, reporting, and IR plans **and practice response with table-top exercises to test technical controls**; process; governance; and executive, board, and external reporting

Overall attack surface management lifecycle

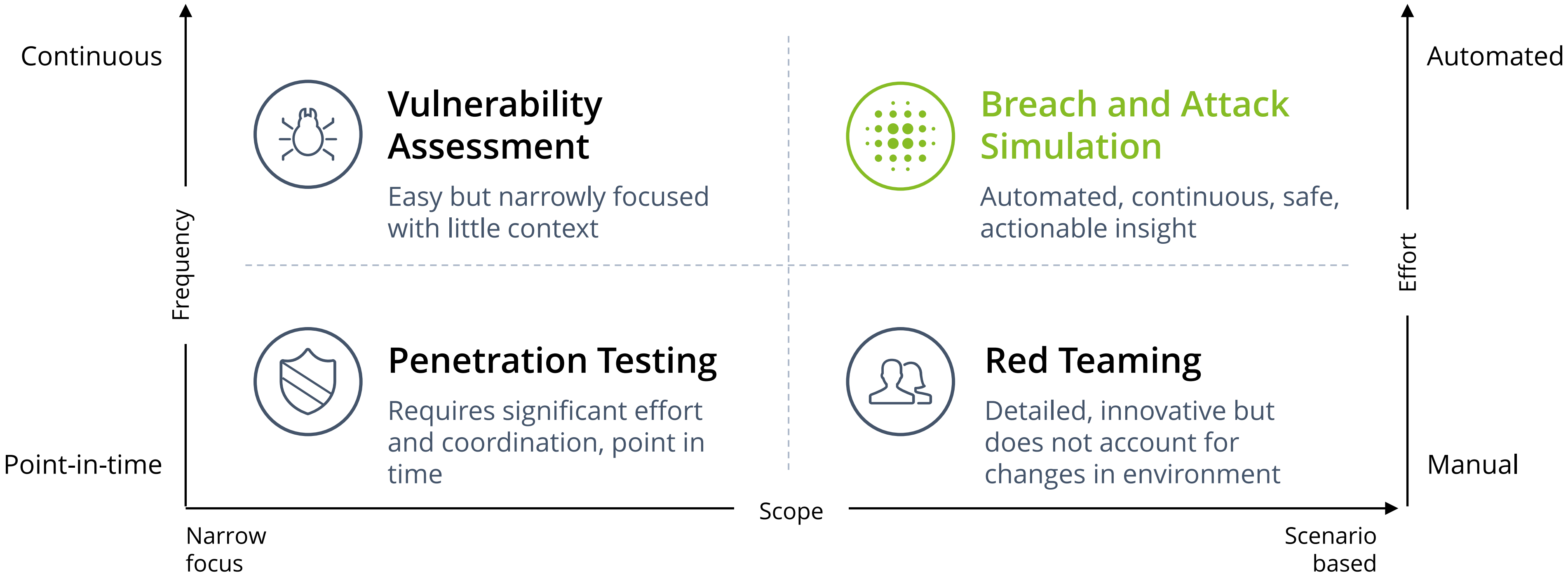
Attack Surface Management (ASM) examines how effective organizational cybersecurity defenses are at protecting operations, assets, users, and proprietary and client information, and BAS is an important capability within this



UNDERSTAND
Environment, inventory, asset priorities and stakeholders
Security stack capabilities, and configurations
ASSESS
Multiple source vulnerability identification
Triage vulnerabilities, validating, and assigning criticality severity rating
GOVERNANCE
Notification prompting risk reduction activities
Ongoing stakeholder collaboration, reporting and metrics
INFORM
Validate remediation activities addressed identified vulnerabilities
Remediate vulnerabilities, e.g., patching, configurations
ADDRESS

Part of the offensive security toolkit

BAS services complement traditional testing efforts by providing a broader view of potential breach scenarios from beginning to end.



Vulnerability Assessment

Easy but narrowly focused with little context

Breach and Attack Simulation

Automated, continuous, safe, actionable insight

Penetration Testing

Requires significant effort and coordination, point in time

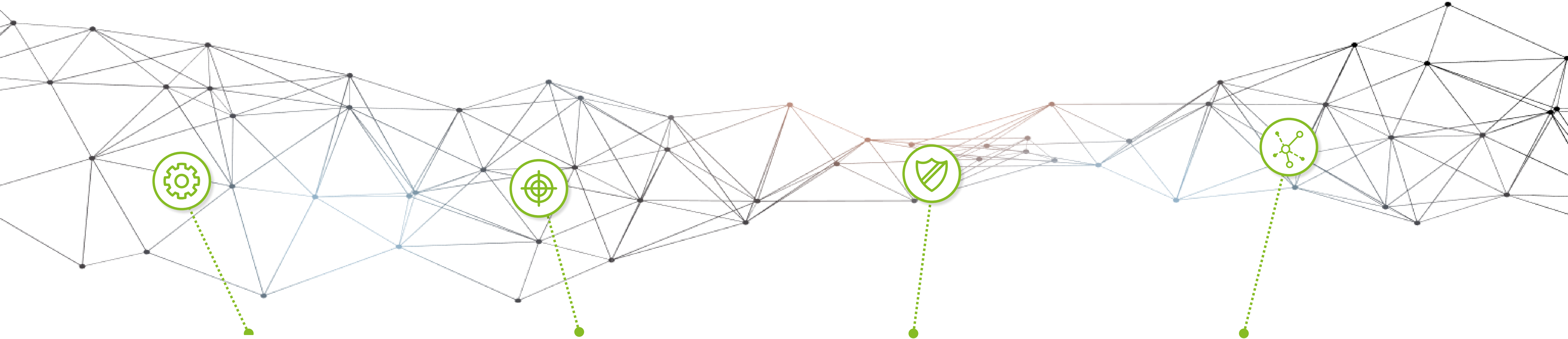
Red Teaming

Detailed, innovative but does not account for changes in environment

Overall goal: If your organization was breached tomorrow, how could that occur and how do you stop it?

Providing a measurable return on investment

Cost of a BAS initiative may be offset by realized risk reduction and potential bottom line savings



Decommission Ineffective or Duplicative Controls

Highlight security controls with less than effective value relative to the cost / threat reduction allowing organizations to make **data- driven security investment decisions.**

Reduce Time to Discovery of Threats

Help prioritize threat hunting activities and inform intelligence requirements based on the TTP’s that are demonstrated to be exploitable within an organization’s environment. **Helps reduce risk exposure** by prioritizing meaningful remediation activities.

Streamline Red Teaming, Penetration Tests, and Tabletop Exercises

A semi-automated and repeatable testing approach **allows traditional testing methods and tabletop exercises to be more streamlined and targeted**

Make Better Use of Data and Analytics

Make better use of data, **increase analytics capabilities, and orchestrate security controls** based on the weaknesses of current controls, ultimately reducing the attack surface and potential for future breaches.

Potential cost savings and return on investments are illustrative

Accelerating benefits when addressing Cyber escalation

Understand risks and impacts to the business, make smart security investments, and enhance the impact of your security controls

Risk and business impact

1 Improve your security posture with better information

Communicate security strategy with clear KPIs that show the cyber program's effectiveness in reducing business risk in a systematic way.

2 Prioritize threats to the business that are actually exploitable.

High risk exists where your security controls fail. Prioritize what matters first.

3 Align security strategy with business growth.

Quantify risk based on potential loss to the business/ cost of avoidance.

4 Know your exposure and get ahead

Measure your exposure to threats, understand which environments and business units are at risk and know what liabilities you are acquiring.

Invest Smart and Protect More

5 Build the right security stack

Structure the right security stack and invest in the stack you need.

6 Justify and prioritize new investments to the board

Accurately identify security gaps that are not covered and advocate where additional investment is needed.

7 Extend the value of your team

Automate activities and get more value from the people you have.

8 Reduce compliance costs

Don't spend time on expensive point-in-time services. Automate continuous compliance testing to communicate with hard metrics.

Enhance Security Control Impact

9 Get the most out of the security controls you have

Often times, the biggest reason why security controls fail is they are not properly configured

10 Ensure your controls accomplish the outcome you bought them for

Verify that your security controls are protecting your critical business assets/outcomes

11 Hold vendors accountable

Run standardized assessments of your security vendors and have them show you they met the threshold of risk that was established in the contract.

Deloitte BAS approach

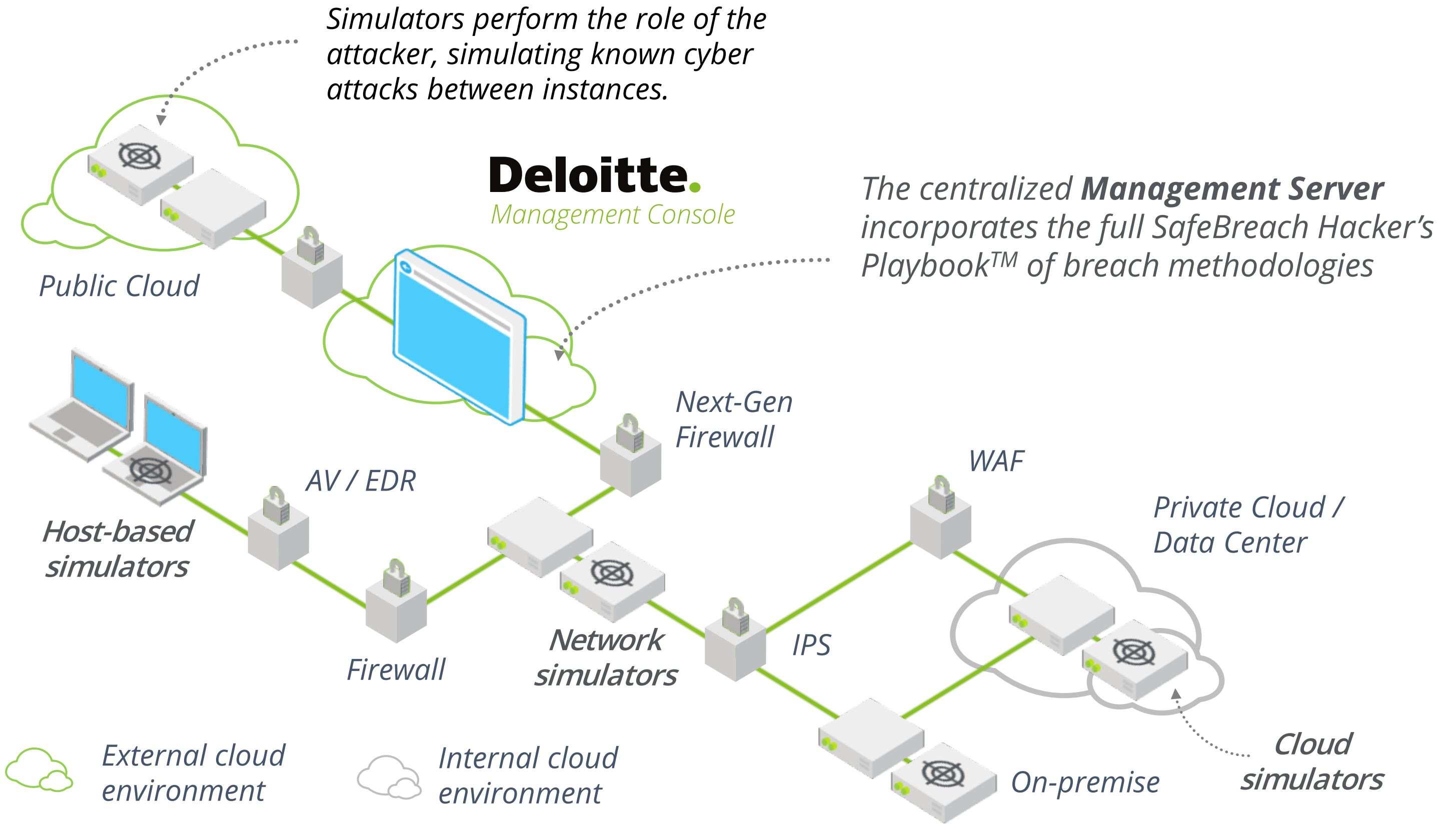
Deloitte's typical BAS engagement consists of three phases: **(1) threat model and plan to better understand the environment and threat landscape; (2) simulate real attacks in a safe environment;** and **(3) report findings/recommendations**

1 THREAT MODEL AND PLAN

Deloitte works with organizations to create a customized threat profile through a threat modeling exercise to identify the latest adversarial tactics, techniques, and procedures (TTPs).

This threat-driven approach will **inform the configuration of a custom playbook of breach simulation use cases.** Customized BAS playbooks will consider which risks are likely to have significant impact to the organization.

It also facilitates the configuration and placement of BAS simulators *(e.g., cloud, network, endpoint)* and the type(s) of sensitive data to simulate *(credit cards, personally identifiable information - PII, source code,*



Simulators perform the role of the attacker, simulating known cyber attacks between instances.

*The centralized **Management Server** incorporates the full SafeBreach Hacker's Playbook™ of breach methodologies*

Deloitte BAS approach (cont.)

2 SIMULATE

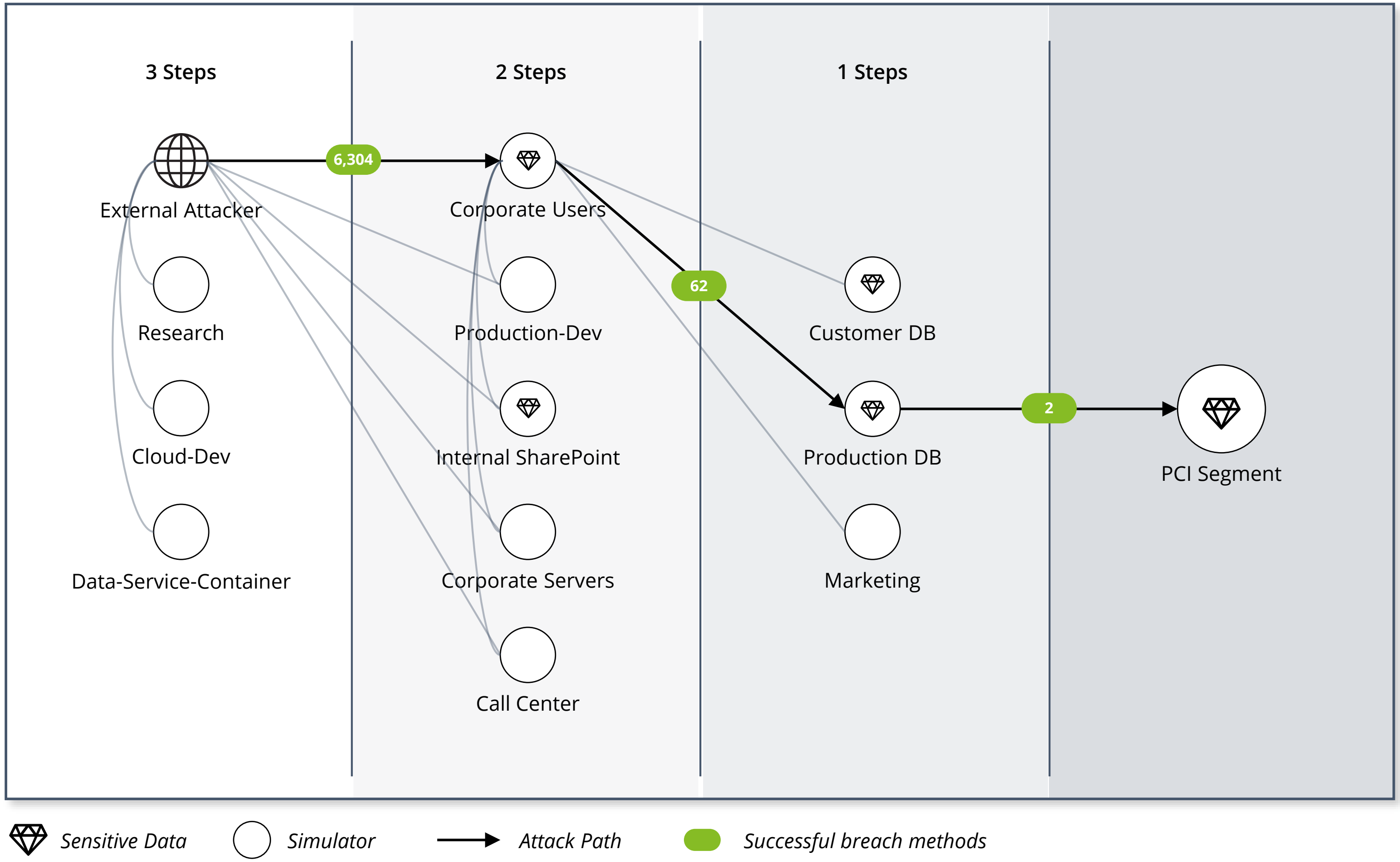
After the simulators and management console have been provisioned, Deloitte will leverage the BAS deployment to safely execute real attacks in the client's production environments.

Simulated TTPs can be stitched together to visualize how an attacker may infiltrate, move laterally, access sensitive data, and exfiltrate within an environment.

BAS simulators execute real attacks solely between simulators in this closed-loop environment using simulated data.

Executing attacks safely in this manner reduces false positives and can help security teams to enhance their situational awareness of control effectiveness without introducing risk to critical systems or actual production data.

Graphic is for illustrative purposes only



Deloitte BAS approach (cont.)

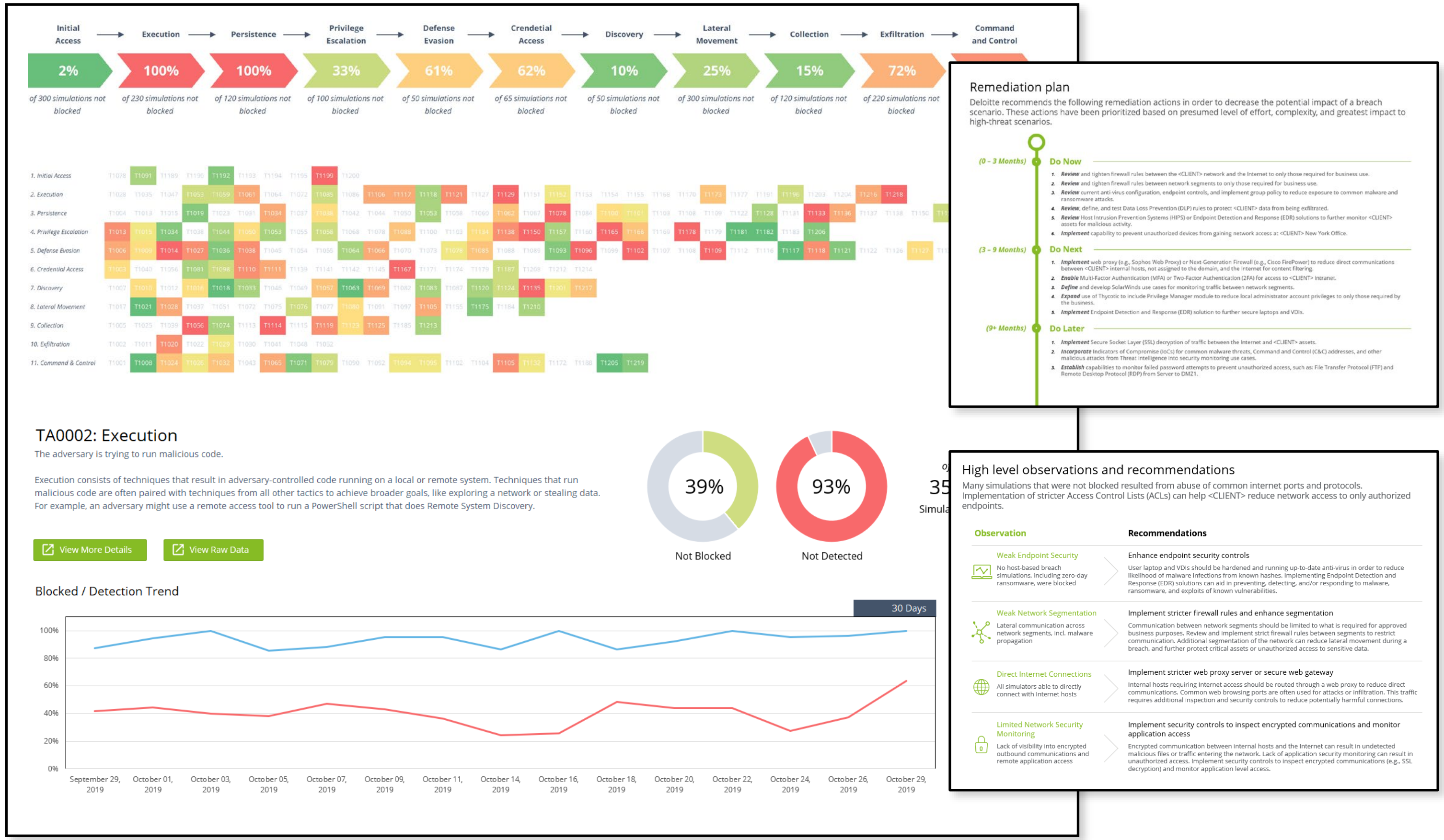
3 REPORT & REPEAT

Deloitte has developed a number of reporting accelerators to **synthesize the significant amount of raw data generated during a BAS exercise against industry-leading views such as the Cyber Kill Chain and MITRE ATT&CK® Framework.**

Develop a roadmap of prioritized remediation activities to help address potential gaps, based on the criticality of findings and the organization's specific threat profile.

Recommendations may include the implementation of new controls and/or tuning of existing controls.

Once the organization's remediation plan has been completed, re-run BAS simulations to identify the efficacy of the newly implemented controls and corresponding gaps.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Crendetial Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
2%	100%	100%	33%	61%	62%	10%	25%	15%	72%	
of 300 simulations not blocked	of 230 simulations not blocked	of 120 simulations not blocked	of 100 simulations not blocked	of 50 simulations not blocked	of 65 simulations not blocked	of 50 simulations not blocked	of 300 simulations not blocked	of 120 simulations not blocked	of 220 simulations not blocked	

1. Initial Access	T1078 T1091 T1189 T1190 T1192 T1193 T1194 T1195 T1199 T1200
2. Execution	T1028 T1035 T1047 T1053 T1059 T1061 T1064 T1072 T1085 T1086 T1106 T1117 T1118 T1121 T1127 T1129 T1151 T1152 T1153 T1154 T1155 T1168 T1170 T1173 T1177 T1191 T1196 T1203 T1204 T1216 T1218
3. Persistence	T1004 T1013 T1015 T1019 T1023 T1031 T1034 T1037 T1038 T1042 T1044 T1050 T1053 T1058 T1060 T1062 T1067 T1078 T1084 T1100 T1101 T1103 T1108 T1109 T1122 T1128 T1131 T1133 T1136 T1137 T1138 T1150
4. Privilege Escalation	T1013 T1015 T1034 T1038 T1044 T1050 T1053 T1055 T1058 T1068 T1078 T1088 T1100 T1103 T1134 T1138 T1150 T1157 T1160 T1165 T1166 T1169 T1178 T1179 T1181 T1182 T1183 T1206
5. Defense Evasion	T1006 T1009 T1014 T1027 T1036 T1038 T1045 T1054 T1055 T1064 T1066 T1070 T1073 T1078 T1085 T1088 T1089 T1093 T1096 T1099 T1102 T1107 T1108 T1109 T1112 T1116 T1117 T1118 T1121 T1122 T1126 T1127
6. Credential Access	T1003 T1040 T1056 T1081 T1098 T1110 T1111 T1139 T1141 T1142 T1145 T1167 T1171 T1174 T1179 T1187 T1208 T1212 T1214
7. Discovery	T1007 T1010 T1012 T1016 T1018 T1033 T1046 T1049 T1057 T1063 T1069 T1082 T1083 T1087 T1120 T1124 T1135 T1201 T1217
8. Lateral Movement	T1017 T1021 T1028 T1037 T1051 T1072 T1075 T1076 T1077 T1080 T1091 T1097 T1105 T1155 T1175 T1184 T1210
9. Collection	T1005 T1025 T1039 T1056 T1074 T1113 T1114 T1115 T1119 T1123 T1125 T1185 T1213
10. Exfiltration	T1002 T1011 T1020 T1022 T1029 T1030 T1041 T1048 T1052
11. Command & Control	T1001 T1008 T1024 T1026 T1032 T1043 T1065 T1071 T1079 T1090 T1092 T1094 T1095 T1102 T1104 T1105 T1132 T1172 T1188 T1205 T1219

TA0002: Execution

The adversary is trying to run malicious code.

Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

Remediation plan

Deloitte recommends the following remediation actions in order to decrease the potential impact of a breach scenario. These actions have been prioritized based on presumed level of effort, complexity, and greatest impact to high-threat scenarios.

(0 – 3 Months) **Do Now**

1. ***Review*** and tighten firewall rules between the <CLIENT> network and the Internet to only those required for business use.
2. ***Review*** and tighten firewall rules between network segments to only those required for business use.
3. ***Review*** current anti-virus configuration, endpoint controls, and implement group policy to reduce exposure to common malware and ransomware attacks.
4. ***Review***, define, and test Data Loss Prevention (DLP) rules to protect <CLIENT> data from being exfiltrated.
5. ***Review*** Host Intrusion Prevention Systems (HIPS) or Endpoint Detection and Response (EDR) solutions to further monitor <CLIENT> assets for malicious activity.
6. ***Implement*** capability to prevent unauthorized devices from gaining network access at <CLIENT> New York Office.

(3 – 9 Months) **Do Next**

1. ***Implement*** web proxy (e.g., Sophos Web Proxy) or Next-Generation Firewall (e.g., Cisco FirePower) to reduce direct communications between <CLIENT> internal hosts, not assigned to the domain, and the Internet for content filtering.
2. ***Enable*** Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) for access to <CLIENT> intranet.
3. ***Define*** and develop SolarWinds use cases for monitoring traffic between network segments.
4. ***Expand*** use of Thycotic to include Privilege Manager module to reduce local administrator account privileges to only those required by the business.
5. ***Implement*** Endpoint Detection and Response (EDR) solution to further secure laptops and VDIs.

(9+ Months) **Do Later**

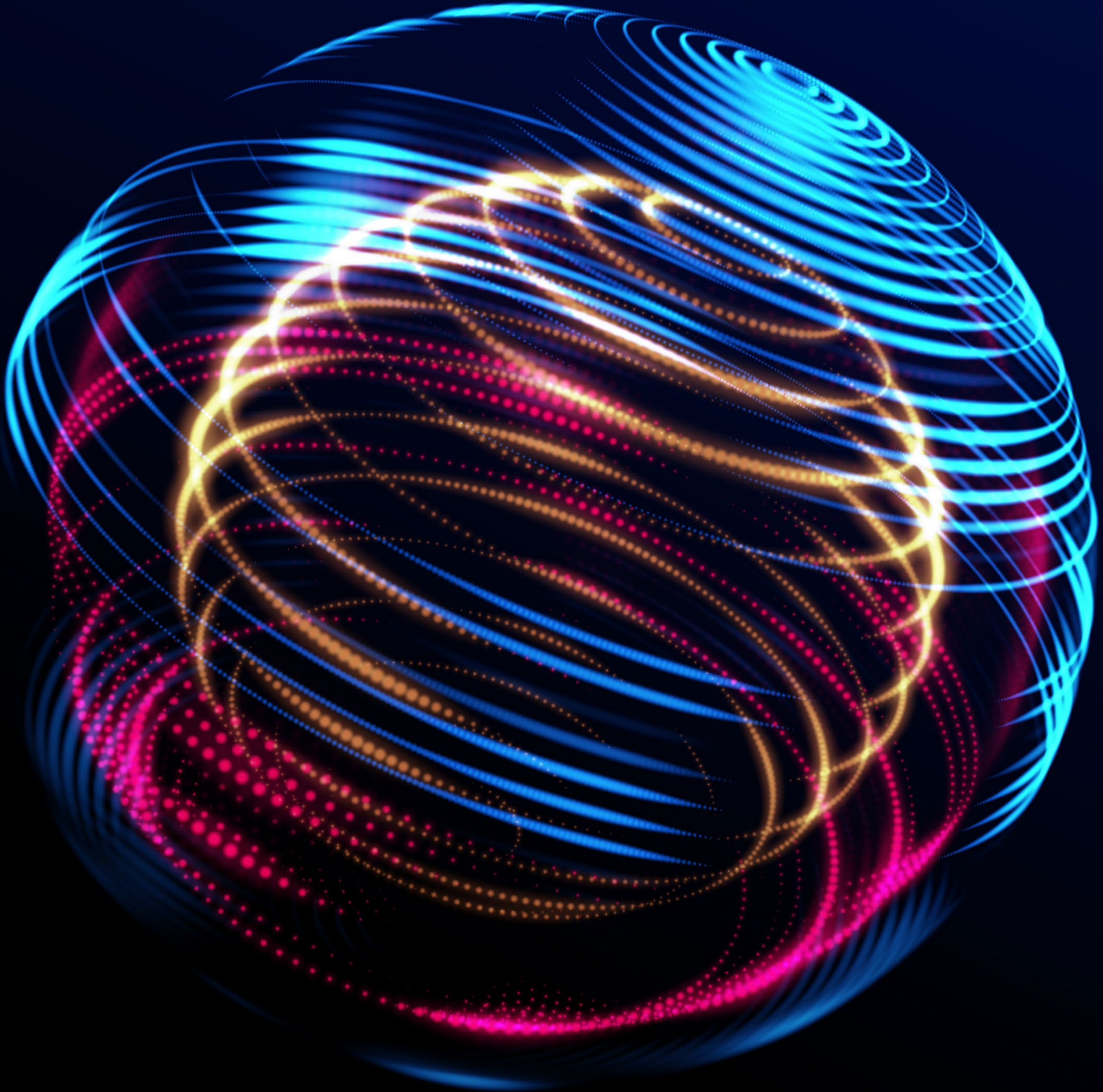
1. ***Implement*** Secure Socket Layer (SSL) decryption of traffic between the Internet and <CLIENT> assets.
2. ***Incorporate*** Indicators of Compromise (IoCs) for common malware threats, Command and Control (C&C) addresses, and other malicious attacks from Threat Intelligence into security monitoring use cases.
3. ***Establish*** capabilities to monitor failed password attempts to prevent unauthorized access, such as: File Transfer Protocol (FTP) and Remote Desktop Protocol (RDP) from Server to DMZ1.

High level observations and recommendations

Many simulations that were not blocked resulted from abuse of common internet ports and protocols. Implementation of stricter Access Control Lists (ACLs) can help <CLIENT> reduce network access to only authorized endpoints.

Observation	Recommendations
Weak Endpoint Security No host-based breach simulations, including zero-day ransomware, were blocked	Enhance endpoint security controls User laptop and VDIs should be hardened and running up-to-date anti-virus in order to reduce likelihood of malware infections from known hashes. Implementing Endpoint Detection and Response (EDR) solutions can aid in preventing, detecting, and/or responding to malware, ransomware, and exploits of known vulnerabilities.
Weak Network Segmentation Lateral communication across network segments, incl. malware propagation	Implement stricter firewall rules and enhance segmentation Communication between network segments should be limited to what is required for approved business purposes. Review and implement strict firewall rules between segments to restrict communication. Additional segmentation of the network can reduce lateral movement during a breach, and further protect critical assets or unauthorized access to sensitive data.
Direct Internet Connections All simulators able to directly connect with Internet hosts	Implement stricter web proxy server or secure web gateway Internal hosts requiring Internet access should be routed through a web proxy to reduce direct communications. Common web browsing ports are often used for attacks or infiltration. This traffic requires additional inspection and security controls to reduce potentially harmful connections.
Limited Network Security Monitoring Lack of visibility into encrypted outbound communications and remote application access	Implement security controls to inspect encrypted communications and monitor application access Encrypted communication between internal hosts and the Internet can result in undetected malicious files or traffic entering the network. Lack of application security monitoring can result in unauthorized access. Implement security controls to inspect encrypted communications (e.g., SSL decryption) and monitor application level access.

Reports are illustrative



MXDR Example

Managed Extended Detection and Response (MXDR) by Deloitte combines an integrated and modular detection and response Software-as-a-Service (SaaS) platform with managed cybersecurity services to provide a military-grade solution—simply put, to provide outcomes for resiliency.

SafeBreach used as part of offensive toolkit to test and analyze MXDR control environment

Integration to accelerate remediation

Integration is a priority for accelerating remediation

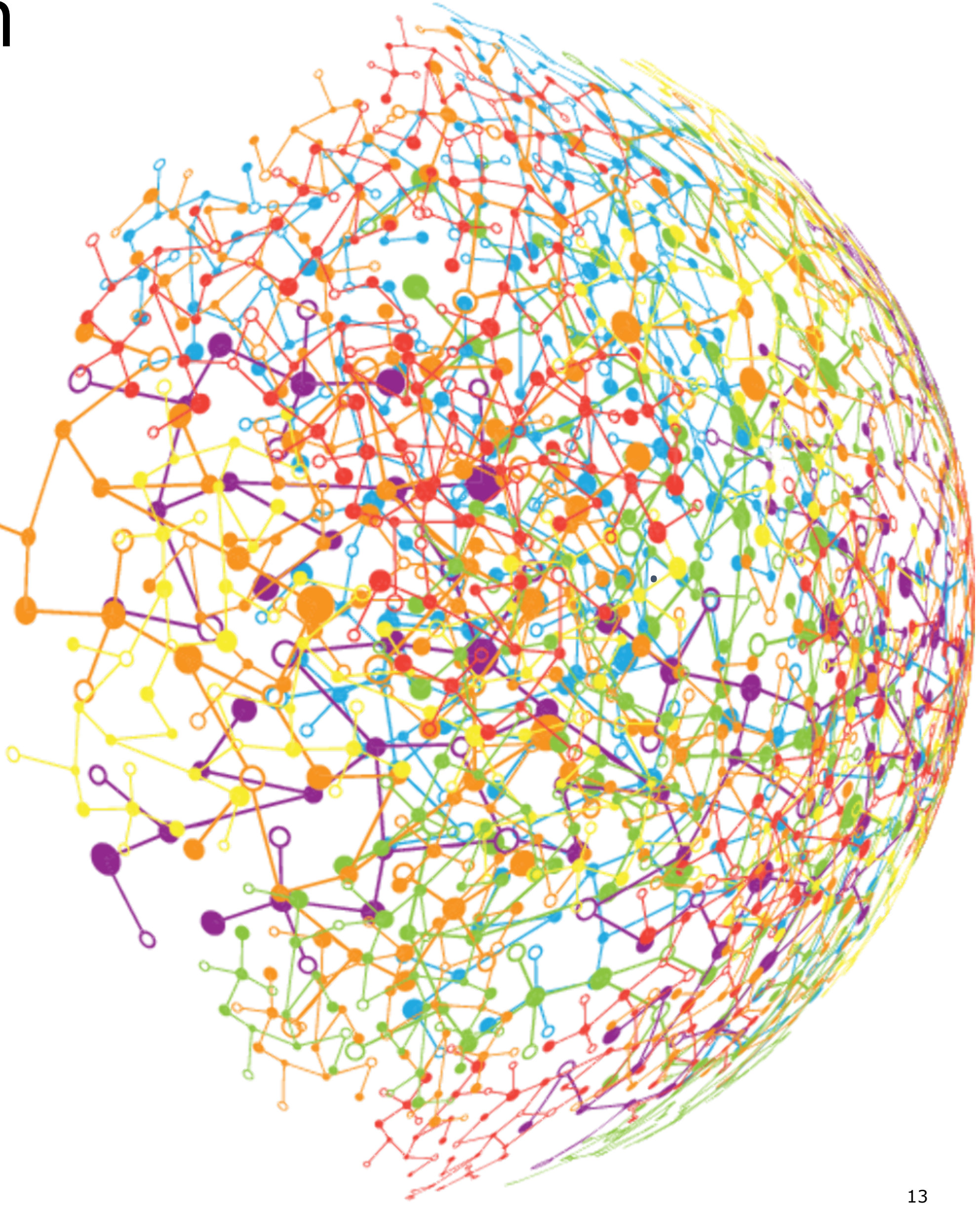
Our experience is:

- Build trust with security operations teams by providing prioritized results in a way that helps them
- Risk-based prioritization is critical
- Inventory available tools and build automation based on quick wins based on:

Security Orchestration, Automation & Response (SOAR)

Case Management

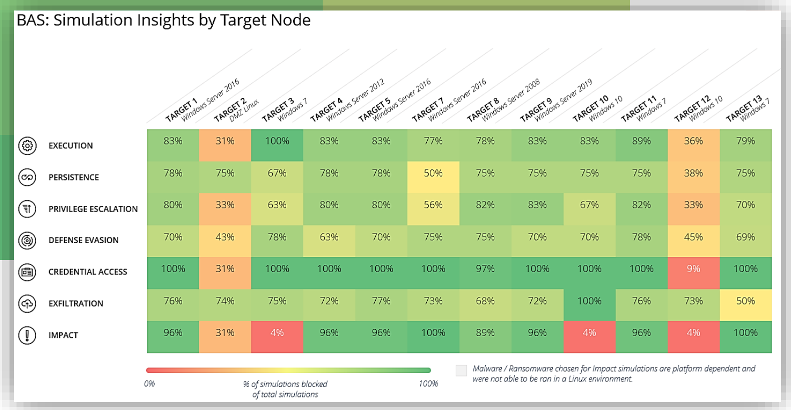
Metrics and Reporting



Simulation Insights by MITRE ATT&CK Tactics and Techniques

EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	EXFILTRATION	IMPACT
Windows Management Instrumentation (100%)	Scheduled Task/Job (50%)	Scheduled Task/Job (50%)	Obfuscated Files or Information (94%)	OS Credential Dumping (89%)	Exfiltration Over C2 Channel (86%)	Data Encrypted for Impact (71%)
Scheduled Task/Job (50%)	Create Account (100%)	Process Injection (50%)	Masquerading (89%)	Unsecured Credentials (91%)		
Command and Scripting Interpreter (57%)	Event Triggered Execution (92%)	Exploitation for Privilege Escalation (65%)	Process Injection (50%)	Steal or Forge Kerberos Tickets (100%)		
Native API (79%)	Boot or Logon Autostart Execution (100%)	Event Triggered Execution (92%)	Deobfuscate / Decode Files or Information (100%)			
	Hijack Execution Flow (0%)	Boot or Logon Autostart Execution (100%)	Signed Binary Proxy Execution (0%)			
		Abuse Elevation Control Mechanism (94%)	Abuse Elevation Control Mechanism (94%)			
		Hijack Execution Flow (0%)	Hijack Execution Flow (0%)			

0% *% of simulations blocked* 100%

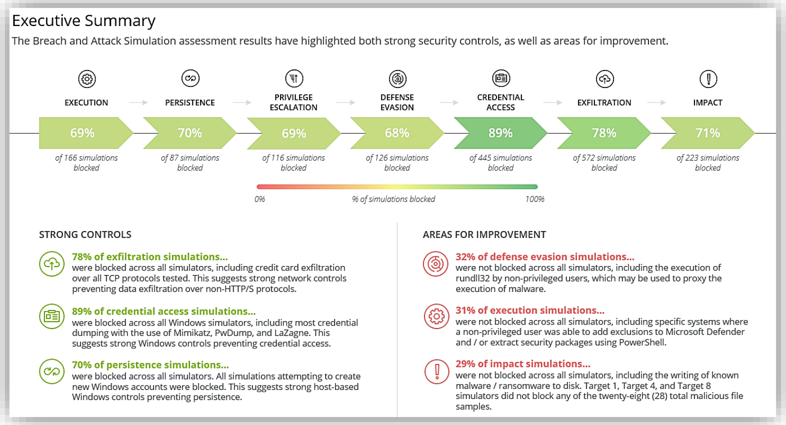


BAS: Simulation Insights by Target Node

	TARGET 1 Windows Server 2016	TARGET 2 DMZ Linux	TARGET 3 Windows 7	TARGET 4 Windows Server 2012	TARGET 5 Windows Server 2016	TARGET 7 Windows Server 2016	TARGET 8 Windows Server 2008	TARGET 9 Windows Server 2019	TARGET 10 Windows 10	TARGET 11 Windows 7	TARGET 12 Windows 10	TARGET 13 Windows 7
EXECUTION	83%	31%	100%	83%	83%	77%	78%	83%	83%	89%	36%	79%
PERSISTENCE	78%	75%	67%	78%	78%	50%	75%	75%	75%	75%	38%	75%
PRIVILEGE ESCALATION	80%	33%	63%	80%	80%	56%	82%	83%	67%	82%	33%	70%
DEFENSE EVASION	70%	43%	78%	63%	70%	75%	75%	70%	70%	78%	45%	69%
CREDENTIAL ACCESS	100%	31%	100%	100%	100%	100%	97%	100%	100%	100%	9%	100%
EXFILTRATION	76%	74%	75%	72%	77%	73%	68%	72%	100%	76%	73%	50%
IMPACT	96%	31%	4%	96%	96%	100%	89%	96%	4%	96%	4%	100%

0% *% of simulations blocked of total simulations* 100%

Malware / Ransomware chosen for Impact simulations are platform dependent and were not able to be ran in a Linux environment.



Executive Summary

The Breach and Attack Simulation assessment results have highlighted both strong security controls, as well as areas for improvement.

EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	EXFILTRATION	IMPACT
69%	70%	69%	68%	89%	78%	71%
of 166 simulations blocked	of 87 simulations blocked	of 116 simulations blocked	of 126 simulations blocked	of 445 simulations blocked	of 572 simulations blocked	of 223 simulations blocked

0% *% of simulations blocked* 100%

STRONG CONTROLS

78% of exfiltration simulations... were blocked across all simulators, including credit card exfiltration over all TCP protocols tested. This suggests strong network controls preventing data exfiltration over non-HTTP/S protocols.

89% of credential access simulations... were blocked across all Windows simulators, including most credential dumping with the use of Mimikatz, PwDump, and LaZagne. This suggests strong Windows controls preventing credential access.

70% of persistence simulations... were blocked across all simulators. All simulations attempting to create new Windows accounts were blocked. This suggests strong host-based Windows controls preventing persistence.

AREAS FOR IMPROVEMENT

32% of defense evasion simulations... were not blocked across all simulators, including the execution of rundll32 by non-privileged users, which may be used to proxy the execution of malware.

31% of execution simulations... were not blocked across all simulators, including specific systems where a non-privileged user was able to add exclusions to Microsoft Defender and / or extract security packages using PowerShell.

29% of impact simulations... were not blocked across all simulators, including the writing of known malware / ransomware to disk. Target 1, Target 4, and Target 8 simulators did not block any of the twenty-eight (28) total malicious file samples.

Final thoughts

- Prepare for cyber escalation now
- Leverage BAS to help multiple teams prepare and be creative in extending use cases
- Consider BAS as a key part of your attack surface management lifecycle
- Force multiply through integration

Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

Product names mentioned in this presentation are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte & Touche LLP is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.